

Scan Report

May 18, 2016

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone “Coordinated Universal Time”, which is abbreviated “UTC”. The task was “Immediate scan of IP”. The scan started at Fri May 6 15:35:33 2016 UTC and ended at Fri May 6 19:52:53 2016 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1	Result Overview	2
2	Results per Host	2
2.1	xxx.xx.166.251	2
2.1.1	High 80/tcp	2
2.1.2	Medium 80/tcp	5
2.1.3	Medium 82/tcp	6
2.1.4	Medium 8080/tcp	7
2.1.5	Medium 443/tcp	9
2.1.6	Low general/tcp	13
2.1.7	Log 80/tcp	14
2.1.8	Log 82/tcp	16
2.1.9	Log 8080/tcp	18
2.1.10	Log 443/tcp	20
2.1.11	Log general/tcp	23
2.1.12	Log general/CPE-T	25

1 Result Overview

Host	High	Medium	Low	Log	False Positive
xxx.xx.166.251 www.xxxxx.com	2	10	1	26	0
Total: 1	2	10	1	26	0

Vendor security updates are not trusted.

Overrides are on. When a result has an override, this report uses the threat of the override.

Notes are included in the report.

This report might not show details of all issues that were found.

It only lists hosts that produced issues.

Issues with the threat level “Debug” are not shown.

Issues with the threat level “False Positive” are not shown.

This report contains results 1 to 39 of the 1 results selected by the filtering described above.

Before filtering there were 139 results.

2 Results per Host

xxx.xx.166.251

Host scan start Fri May 6 15:36:02 2016 UTC

Host scan end Fri May 6 19:52:53 2016 UTC

Service (Port)	Threat Level
80/tcp	High
80/tcp	Medium
82/tcp	Medium
8080/tcp	Medium
443/tcp	Medium
general/tcp	Low
80/tcp	Log
82/tcp	Log
8080/tcp	Log
443/tcp	Log
general/tcp	Log
general/CPE-T	Log

2.1.1 High 80/tcp

... continues on next page ...

...continued from previous page ...

High (CVSS: 7.5)

NVT: WordPress Webdorado Spider Event Calendar SQL Injection

Product detection result

cpe:/a:wordpress:wordpress:4.3.1

Detected by WordPress Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900182)

Summary

This host is installed with Wordpress Spider Event Calendar and is prone to sql injection vulnerability.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation will allow remote attackers to inject or manipulate SQL queries in the back-end database, allowing for the manipulation or disclosure of arbitrary data.

Impact Level: Application

Solution

Solution type: NoneAvailable

No solution or patch is available as of 13th April, 2015. Information regarding this issue will be updated once the solution details are available. For updates refer to <https://wordpress.org/plugins/spider-event-calendar>

Affected Software/OS

Wordpress Spider Event Calendar Plugin 1.4.9

Vulnerability Insight**Vulnerability Detection Method**

Send a crafted request via HTTP GET and check whether it is able to execute sql query or not.

Details:WordPress Webdorado Spider Event Calendar SQL Injection

OID:1.3.6.1.4.1.25623.1.0.805349

Version used: \$Revision: 1159 \$

Product Detection Result

Product: cpe:/a:wordpress:wordpress:4.3.1

Method: WordPress Version Detection

OID: 1.3.6.1.4.1.25623.1.0.900182)

References

CVE: CVE-2015-2196

...continues on next page ...

...continued from previous page ...
Other: URL: http://osvdb.org/118829 URL: http://www.exploit-db.com/exploits/36061/
High (CVSS: 7.5) NVT: WordPress Business Intelligence Lite SQL Injection Vulnerability
Product detection result cpe:/a:wordpress:wordpress:4.3.1 Detected by WordPress Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900182)
Summary This host is installed with Wordpress Business Intelligence Lite and is prone to sql injection vulnerability.
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Impact Successful exploitation will allow remote attackers to inject or manipulate SQL queries in the back-end database, allowing for the manipulation or disclosure of arbitrary data. Impact Level: Application
Solution Solution type: VendorFix Upgrade to Wordpress Business Intelligence Lite Plugin 1.6.2 or later, For updates refer to https://wordpress.org/plugins/wp-business-intelligence-lite
Affected Software/OS Wordpress Business Intelligence Lite Plugin version 1.6.1, Prior versions may also be affected.
Vulnerability Insight Flaw is due to the 'view.php' script not properly sanitizing user-supplied input to the 't' parameter.
Vulnerability Detection Method Send a crafted request via HTTP GET and check whether it is able to execute sql query or not. Details:WordPress Business Intelligence Lite SQL Injection Vulnerability OID:1.3.6.1.4.1.25623.1.0.805366 Version used: \$Revision: 1186 \$
Product Detection Result Product: cpe:/a:wordpress:wordpress:4.3.1 Method: WordPress Version Detection OID: 1.3.6.1.4.1.25623.1.0.900182)
...continues on next page ...

...continued from previous page ...

References**Other:**URL:<http://osvdb.org/120224>URL:<http://www.exploit-db.com/exploits/36600>[\[return to xxx.xx.166.251\]](#)**2.1.2 Medium 80/tcp**

Medium (CVSS: 5.8)

NVT: http TRACE XSS attack

Summary

Debugging functions are enabled on the remote HTTP server.

The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.

It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when used in conjunction with various weaknesses in browsers.

An attacker may use this flaw to trick your legitimate web users to give him their credentials.

Vulnerability Detection Result**Solution:**

Add the following lines for each virtual host in your configuration file :

```
RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
RewriteRule .* - [F]
```

See also <http://httpd.apache.org/docs/current/de/mod/core.html#traceenable>

Solution

Disable these methods.

Vulnerability Detection Method

Details: http TRACE XSS attack

OID: 1.3.6.1.4.1.25623.1.0.11213

Version used: \$Revision: 922 \$

References

CVE: CVE-2004-2320, CVE-2003-1567

BID: 9506, 9561, 11604

Other:

URL: <http://www.kb.cert.org/vuls/id/867593>

Medium (CVSS: 5.0) NVT: Missing httpOnly Cookie Attribute
Summary The application is missing the 'httpOnly' cookie attribute
Vulnerability Detection Result The cookies: Set-Cookie: PHPSESSID=cjsgvdaai13qm0ic1k439po0c0; path=/ are missing the httpOnly attribute.
Impact Application
Solution Set the 'httpOnly' attribute for any session cookies.
Affected Software/OS Application with session handling in cookies.
Vulnerability Insight The flaw is due to a cookie is not using the 'httpOnly' attribute. This allows a cookie to be accessed by JavaScript which could lead to session hijacking attacks.
Vulnerability Detection Method Check all cookies sent by the application for a missing 'httpOnly' attribute Details:Missing httpOnly Cookie Attribute OID:1.3.6.1.4.1.25623.1.0.105925 Version used: \$Revision: 809 \$
References Other: URL:https://www.owasp.org/index.php/HttpOnly URL:https://www.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-↵002)

[\[return to xxx.xx.166.251\]](#)

2.1.3 Medium 82/tcp

Medium (CVSS: 5.8) NVT: http TRACE XSS attack
Summary Debugging functions are enabled on the remote HTTP server. The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections. ... continues on next page ...

...continued from previous page ...
<p>It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when used in conjunction with various weaknesses in browsers.</p> <p>An attacker may use this flaw to trick your legitimate web users to give him their credentials.</p>
<p>Vulnerability Detection Result</p> <p>Solution:</p> <p>Add the following lines for each virtual host in your configuration file :</p> <pre>RewriteEngine on RewriteCond %{REQUEST_METHOD} ^(TRACE TRACK) RewriteRule .* - [F]</pre> <p>See also http://httpd.apache.org/docs/current/de/mod/core.html#traceenable</p>
<p>Solution</p> <p>Disable these methods.</p>
<p>Vulnerability Detection Method</p> <p>Details:http TRACE XSS attack</p> <p>OID:1.3.6.1.4.1.25623.1.0.11213</p> <p>Version used: \$Revision: 922 \$</p>
<p>References</p> <p>CVE: CVE-2004-2320, CVE-2003-1567</p> <p>BID:9506, 9561, 11604</p> <p>Other:</p> <p>URL:http://www.kb.cert.org/vuls/id/867593</p>

[\[return to xxx.xx.166.251\]](#)

2.1.4 Medium 8080/tcp

<p>Medium (CVSS: 5.8)</p> <p>NVT: http TRACE XSS attack</p>
<p>Summary</p> <p>Debugging functions are enabled on the remote HTTP server.</p> <p>The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.</p> <p>It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when used in conjunction with various weaknesses in browsers.</p> <p>An attacker may use this flaw to trick your legitimate web users to give him their credentials.</p>
<p>Vulnerability Detection Result</p> <p>Solution:</p> <p>Add the following lines for each virtual host in your configuration file :</p> <p>...continues on next page ...</p>

<p>...continued from previous page ...</p> <pre> RewriteEngine on RewriteCond %{REQUEST_METHOD} ^(TRACE TRACK) RewriteRule .* - [F] </pre> <p>See also http://httpd.apache.org/docs/current/de/mod/core.html#traceenable</p>
<p>Solution Disable these methods.</p>
<p>Vulnerability Detection Method Details:http TRACE XSS attack OID:1.3.6.1.4.1.25623.1.0.11213 Version used: \$Revision: 922 \$</p>
<p>References CVE: CVE-2004-2320, CVE-2003-1567 BID:9506, 9561, 11604 Other: URL:http://www.kb.cert.org/vuls/id/867593</p>

<p>Medium (CVSS: 4.3) NVT: Apache Web Server ETag Header Information Disclosure Weakness</p>
<p>Summary A weakness has been discovered in Apache web servers that are configured to use the FileETag directive.</p>
<p>Vulnerability Detection Result Information that was gathered: Inode: 273637 Size: 6</p>
<p>Impact Exploitation of this issue may provide an attacker with information that may be used to launch further attacks against a target network.</p>
<p>Solution OpenBSD has released a patch that addresses this issue. Inode numbers returned from the server are now encoded using a private hash to avoid the release of sensitive information. Novell has released TID10090670 to advise users to apply the available workaround of disabling the directive in the configuration file for Apache releases on NetWare. Please see the attached Technical Information Document for further details.</p>
<p>Vulnerability Detection Method Due to the way in which Apache generates ETag response headers, it may be possible for an attacker to obtain sensitive information regarding server files. Specifically, ETag header fields returned to a client contain the file's inode number. Details:Apache Web Server ETag Header Information Disclosure Weakness</p>
<p>...continues on next page ...</p>

...continued from previous page ...
OID:1.3.6.1.4.1.25623.1.0.103122 Version used: \$Revision: 1218 \$
References CVE: CVE-2003-1418 BID:6939 Other: URL:https://www.securityfocus.com/bid/6939 URL:http://httpd.apache.org/docs/mod/core.html#fileetag URL:http://www.openbsd.org/errata32.html URL:http://support.novell.com/docs/Tids/Solutions/10090670.html

[\[return to xxx.xx.166.251\]](#)

2.1.5 Medium 443/tcp

Medium (CVSS: 5.8) NVT: http TRACE XSS attack
Summary Debugging functions are enabled on the remote HTTP server. The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections. It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when used in conjunction with various weaknesses in browsers. An attacker may use this flaw to trick your legitimate web users to give him their credentials.
Vulnerability Detection Result Solution: Add the following lines for each virtual host in your configuration file : <pre>RewriteEngine on RewriteCond %{REQUEST_METHOD} ^(TRACE TRACK) RewriteRule .* - [F]</pre> See also http://httpd.apache.org/docs/current/de/mod/core.html#traceenable
Solution Disable these methods.
Vulnerability Detection Method Details:http TRACE XSS attack OID:1.3.6.1.4.1.25623.1.0.11213 Version used: \$Revision: 922 \$
References CVE: CVE-2004-2320, CVE-2003-1567
...continues on next page ...

...continued from previous page ...

BID:9506, 9561, 11604

Other:

URL:<http://www.kb.cert.org/vuls/id/867593>

Medium (CVSS: 5.0)

NVT: SSL Certification Expired

Summary

The remote server's SSL certificate has already expired.

Vulnerability Detection Result

Expired Certificates:

The SSL certificate on the remote service expired on 2010-11-11 11:07:41

Certificate details:

subject ...: 1.2.840.113549.1.9.1=#726F6F74406C6F63616C686F73742E6C6F63616C646F6
 ↪D61696E,CN=localhost.localdomain,OU=SomeOrganizationalUnit,O=SomeOrganization,
 ↪L=SomeCity,ST=SomeState,C=--
 issued by ..: 1.2.840.113549.1.9.1=#726F6F74406C6F63616C686F73742E6C6F63616C646F6
 ↪D61696E,CN=localhost.localdomain,OU=SomeOrganizationalUnit,O=SomeOrganization,
 ↪L=SomeCity,ST=SomeState,C=--
 serial: 34D8
 valid from : 2009-11-11 11:07:41 UTC
 valid until: 2010-11-11 11:07:41 UTC
 fingerprint: A17FB3431FF1E1058EA0057ACC7AE5343EB0BAB9

Solution

Replace the SSL certificate by a new one.

Vulnerability Insight

This script checks expiry dates of certificates associated with SSL-enabled services on the target and reports whether any have already expired.

Vulnerability Detection Method

Details:SSL Certification Expired

OID:1.3.6.1.4.1.25623.1.0.103955

Version used: \$Revision: 626 \$

Medium (CVSS: 4.3)

NVT: Check for SSL Weak Ciphers

Summary

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

Vulnerability Detection Result

Weak ciphers offered by this service:

...continues on next page ...

...continued from previous page ...
TLS1_RSA_RC4_128_MD5
Solution The configuration of this services should be changed so that it does not support the listed weak ciphers anymore.
Vulnerability Insight These rules are applied for the evaluation of the cryptographic strength: <ul style="list-style-type: none"> - Any SSL/TLS using no cipher is considered weak. - All SSLv2 ciphers are considered weak due to a design flaw within the SSLv2 protocol. - RC4 is considered to be weak. - Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak. - 1024 bit RSA authentication is considered to be insecure and therefore as weak. - CBC ciphers in TLS ; 1.2 are considered to be vulnerable to the BEAST or Lucky 13 attacks - Any cipher considered to be secure for only the next 10 years is considered as medium - Any other cipher is considered as strong
Vulnerability Detection Method Details:Check for SSL Weak Ciphers OID:1.3.6.1.4.1.25623.1.0.103440 Version used: \$Revision: 733 \$

Medium (CVSS: 4.3) NVT: Deprecated SSLv2 and SSLv3 Protocol Detection
Summary It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.
Vulnerability Detection Result In addition to TLSv1+ the service is also providing the deprecated SSLv3 protocol ↪1 and supports one or more ciphers. Those supported ciphers can be found in th ↪e 'Check SSL Weak Ciphers and Supported Ciphers' NVT.
Impact 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 transfered within the secured connection.
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.
Affected Software/OS All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.
...continues on next page ...

...continued from previous page ...
Vulnerability Insight The SSLv2 and SSLv3 protocols containing known cryptographic flaws.
Vulnerability Detection Method Check the used protocols of the services provided by this system. Details:Deprecated SSLv2 and SSLv3 Protocol Detection OID:1.3.6.1.4.1.25623.1.0.111012 Version used: \$Revision: 1183 \$
References Other: URL: https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report URL: https://bettercrypto.org/
Medium (CVSS: 4.3) NVT: POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability
Summary This host is installed with OpenSSL and is prone to information disclosure vulnerability.
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Impact Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream. Impact Level: Application
Solution Vendor released a patch to address this vulnerabiliy, For updates contact vendor or refer to https://www.openssl.org NOTE: The only correct way to fix POODLE is to disable SSL v3.0
Affected Software/OS OpenSSL through 1.0.1i
Vulnerability Insight The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code
Vulnerability Detection Method Send a SSLv3 request and check the response. Details:POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability OID:1.3.6.1.4.1.25623.1.0.802087
...continues on next page ...

...continued from previous page ...
Version used: \$Revision: 1152 \$
References CVE: CVE-2014-3566 BID: 70574 Other: URL: http://osvdb.com/113251 URL: https://www.openssl.org/~bodo/ssl-poodle.pdf URL: https://www.imperialviolet.org/2014/10/14/poodle.html URL: https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html URL: http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploit-again-ssl-30.html

[\[return to xxx.xx.166.251\]](#)

2.1.6 Low general/tcp

Low (CVSS: 2.6) NVT: TCP timestamps
Summary The remote host implements TCP timestamps and therefore allows to compute the uptime.
Vulnerability Detection Result It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 289743373 Paket 2: 289744426
Impact A side effect of this feature is that the uptime of the remote host can sometimes be computed.
Solution 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
Affected Software/OS TCP/IPv4 implementations that implement RFC1323.
Vulnerability Insight The remote host implements TCP timestamps, as defined by RFC1323.
...continues on next page ...

...continued from previous page ...

Vulnerability Detection Method

Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.

Details:TCP timestamps

OID:1.3.6.1.4.1.25623.1.0.80091

Version used: \$Revision: 787 \$

References

Other:

URL:<http://www.ietf.org/rfc/rfc1323.txt>

[\[return to xxx.xx.166.251\]](#)

2.1.7 Log 80/tcp

Log (CVSS: 0.0)

NVT: HTTP Server type and version

Summary

This detects the HTTP Server's type and version.

Vulnerability Detection Result

The remote web server type is :

Apache/2.2.3 (Red Hat)

Solution : You can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers.

Solution**Log Method**

Details:HTTP Server type and version

OID:1.3.6.1.4.1.25623.1.0.10107

Version used: \$Revision: 229 \$

Log (CVSS: 0.0)

NVT: Services

Summary

This plugin attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 and set the results in the plugins knowledge base.

Vulnerability Detection Result

... continues on next page ...

...continued from previous page ...
A web server is running on this port
Log Method Details:Services OID:1.3.6.1.4.1.25623.1.0.10330 Version used: \$Revision: 69 \$
Log (CVSS: 0.0) NVT: wapiti (NASL wrapper)
Summary This plugin uses wapiti to find web security issues. Make sure to have wapiti 2.x as wapiti 1.x is not supported. See the preferences section for wapiti options. Note that OpenVAS is using limited set of wapiti options. Therefore, for more complete web assessment, you should use standalone wapiti tool for deeper/customized checks.
Vulnerability Detection Result wapiti could not be found in your system path. OpenVAS was unable to execute wapiti and to perform the scan you requested. Please make sure that wapiti is installed and that wapiti is available in the PATH variable defined for your environment.
Log Method Details:wapiti (NASL wrapper) OID:1.3.6.1.4.1.25623.1.0.80110 Version used: \$Revision: 14 \$
Log (CVSS: 0.0) NVT: WordPress Version Detection
Summary Detection of installed version of WordPress/WordPress-Mu. This script sends HTTP GET request and try to get the version from the response, and sets the result in KB.
Vulnerability Detection Result Detected WordPress Version: 4.3.1 Location: / CPE: cpe:/a:wordpress:wordpress:4.3.1 Concluded from version identification result: WordPress 4.3.1
...continues on next page ...

...continued from previous page ...

Log Method

Details:WordPress Version Detection

OID:1.3.6.1.4.1.25623.1.0.900182

Version used: \$Revision: 1072 \$

Log (CVSS: 0.0)

NVT: Apache Web Server Version Detection

Summary

Detection of installed version of Apache Web Server

The script detects the version of Apache HTTP Server on remote host and sets the KB.

Vulnerability Detection Result

Detected Apache

Version: 2.2.3

Location: 80/tcp

CPE: cpe:/a:apache:http_server:2.2.3

Concluded from version identification result:

Server: Apache/2.2.3

Log Method

Details:Apache Web Server Version Detection

OID:1.3.6.1.4.1.25623.1.0.900498

Version used: \$Revision: 1141 \$

[\[return to xxx.xx.166.251\]](#)**2.1.8 Log 82/tcp**

Log (CVSS: 0.0)

NVT: HTTP Server type and version

Summary

This detects the HTTP Server's type and version.

Vulnerability Detection Result

The remote web server type is :

Apache/2.2.3 (Red Hat)

Solution : You can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers.

Solution**Log Method**

... continues on next page ...

...continued from previous page ...

Details:HTTP Server type and version
 OID:1.3.6.1.4.1.25623.1.0.10107
 Version used: \$Revision: 229 \$

Log (CVSS: 0.0)
 NVT: Services

Summary

This plugin attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 and set the results in the plugins knowledge base.

Vulnerability Detection Result

A web server is running on this port

Log Method

Details:Services
 OID:1.3.6.1.4.1.25623.1.0.10330
 Version used: \$Revision: 69 \$

Log (CVSS: 0.0)
 NVT: wapiti (NASL wrapper)

Summary

This plugin uses wapiti to find web security issues.
 Make sure to have wapiti 2.x as wapiti 1.x is not supported.
 See the preferences section for wapiti options.
 Note that OpenVAS is using limited set of wapiti options. Therefore, for more complete web assessment, you should use standalone wapiti tool for deeper/customized checks.

Vulnerability Detection Result

wapiti could not be found in your system path.
 OpenVAS was unable to execute wapiti and to perform the scan you requested.
 Please make sure that wapiti is installed and that wapiti is available in the PATH variable defined for your environment.

Log Method

Details:wapiti (NASL wrapper)
 OID:1.3.6.1.4.1.25623.1.0.80110
 Version used: \$Revision: 14 \$

...continues on next page ...

...continued from previous page ...

Log (CVSS: 0.0) NVT: Apache Web Server Version Detection
Summary Detection of installed version of Apache Web Server The script detects the version of Apache HTTP Server on remote host and sets the KB.
Vulnerability Detection Result Detected Apache Version: 2.2.3 Location: 82/tcp CPE: cpe:/a:apache:http_server:2.2.3 Concluded from version identification result: Server: Apache/2.2.3
Log Method Details:Apache Web Server Version Detection OID:1.3.6.1.4.1.25623.1.0.900498 Version used: \$Revision: 1141 \$

[\[return to xxx.xx.166.251\]](#)**2.1.9 Log 8080/tcp**

Log (CVSS: 0.0) NVT: HTTP Server type and version
Summary This detects the HTTP Server's type and version.
Vulnerability Detection Result The remote web server type is : Apache/2.2.3 (Red Hat) Solution : You can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers.
Solution
Log Method Details:HTTP Server type and version OID:1.3.6.1.4.1.25623.1.0.10107 Version used: \$Revision: 229 \$

Log (CVSS: 0.0) NVT: Services
Summary This plugin attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 and set the results in the plugins knowledge base.
Vulnerability Detection Result A web server is running on this port
Log Method Details:Services OID:1.3.6.1.4.1.25623.1.0.10330 Version used: \$Revision: 69 \$

Log (CVSS: 0.0) NVT: wapiti (NASL wrapper)
Summary This plugin uses wapiti to find web security issues. Make sure to have wapiti 2.x as wapiti 1.x is not supported. See the preferences section for wapiti options. Note that OpenVAS is using limited set of wapiti options. Therefore, for more complete web assessment, you should use standalone wapiti tool for deeper/customized checks.
Vulnerability Detection Result wapiti could not be found in your system path. OpenVAS was unable to execute wapiti and to perform the scan you requested. Please make sure that wapiti is installed and that wapiti is available in the PATH variable defined for your environment.
Log Method Details:wapiti (NASL wrapper) OID:1.3.6.1.4.1.25623.1.0.80110 Version used: \$Revision: 14 \$

Log (CVSS: 0.0) NVT: Apache Web Server Version Detection
Summary Detection of installed version of Apache Web Server The script detects the version of Apache HTTP Server on remote host and sets the KB.
Vulnerability Detection Result ... continues on next page ...

...continued from previous page ...

Detected Apache
 Version: 2.2.3
 Location: 8080/tcp
 CPE: cpe:/a:apache:http_server:2.2.3
 Concluded from version identification result:
 Server: Apache/2.2.3

Log Method

Details:Apache Web Server Version Detection
 OID:1.3.6.1.4.1.25623.1.0.900498
 Version used: \$Revision: 1141 \$

[\[return to xxx.xx.166.251\]](#)
2.1.10 Log 443/tcp

Log (CVSS: 0.0)

NVT: HTTP Server type and version

Summary

This detects the HTTP Server's type and version.

Vulnerability Detection Result

The remote web server type is :

Apache/2.2.3 (Red Hat)

Solution : You can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers.

Solution**Log Method**

Details:HTTP Server type and version
 OID:1.3.6.1.4.1.25623.1.0.10107
 Version used: \$Revision: 229 \$

Log (CVSS: 0.0)

NVT: SSL Certificate - Self-Signed Certificate Detection

Summary

The SSL certificate on this port is self-signed.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

... continues on next page ...

...continued from previous page ...
Log Method Details:SSL Certificate - Self-Signed Certificate Detection OID:1.3.6.1.4.1.25623.1.0.103140 Version used: \$Revision: 651 \$
References Other: URL: http://en.wikipedia.org/wiki/Self-signed_certificate

Log (CVSS: 0.0) NVT: SSL Certificate - Subject Common Name Does Not Match Server FQDN
Summary The SSL certificate contains a common name (CN) that does not match the hostname.
Vulnerability Detection Result Hostname: www.xxxxx.com Common Name: localhost.localdomain
Log Method Details:SSL Certificate - Subject Common Name Does Not Match Server FQDN OID:1.3.6.1.4.1.25623.1.0.103141 Version used: \$Revision: 349 \$

Log (CVSS: 0.0) NVT: Services
Summary This plugin attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 and set the results in the plugins knowledge base.
Vulnerability Detection Result A TLScustom server answered on this port
Log Method Details:Services OID:1.3.6.1.4.1.25623.1.0.10330 Version used: \$Revision: 69 \$

Log (CVSS: 0.0) NVT: Services
Summary ...continues on next page ...

...continued from previous page ...
This plugin attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 and set the results in the plugins knowledge base.
Vulnerability Detection Result A web server is running on this port through SSL
Log Method Details:Services OID:1.3.6.1.4.1.25623.1.0.10330 Version used: \$Revision: 69 \$

Log (CVSS: 0.0) NVT: wapiti (NASL wrapper)
Summary This plugin uses wapiti to find web security issues. Make sure to have wapiti 2.x as wapiti 1.x is not supported. See the preferences section for wapiti options. Note that OpenVAS is using limited set of wapiti options. Therefore, for more complete web assessment, you should use standalone wapiti tool for deeper/customized checks.
Vulnerability Detection Result wapiti could not be found in your system path. OpenVAS was unable to execute wapiti and to perform the scan you requested. Please make sure that wapiti is installed and that wapiti is available in the PATH variable defined for your environment.
Log Method Details:wapiti (NASL wrapper) OID:1.3.6.1.4.1.25623.1.0.80110 Version used: \$Revision: 14 \$

Log (CVSS: 0.0) NVT: Check for SSL Ciphers
Summary This routine search for SSL ciphers offered by a service.
Vulnerability Detection Result Service does not support SSLv2 ciphers. Service does not support SSLv3 ciphers. Service supports TLSv1 ciphers. Service does not support TLSv1.1 ciphers.
...continues on next page ...

...continued from previous page ...
<p>Service does not support TLSv1.2 ciphers. No medium ciphers are supported by this service Weak ciphers offered by this service: TLS1_RSA_RC4_128_MD5 No non-ciphers are supported by this service</p>
<p>Log Method Details:Check for SSL Ciphers OID:1.3.6.1.4.1.25623.1.0.802067 Version used: \$Revision: 312 \$</p>

<p>Log (CVSS: 0.0) NVT: Apache Web Server Version Detection</p>
<p>Summary Detection of installed version of Apache Web Server The script detects the version of Apache HTTP Server on remote host and sets the KB.</p>
<p>Vulnerability Detection Result Detected Apache Version: 2.2.3 Location: 443/tcp CPE: cpe:/a:apache:http_server:2.2.3 Concluded from version identification result: Server: Apache/2.2.3</p>
<p>Log Method Details:Apache Web Server Version Detection OID:1.3.6.1.4.1.25623.1.0.900498 Version used: \$Revision: 1141 \$</p>

[\[return to xxx.xx.166.251\]](#)

2.1.11 Log general/tcp

<p>Log (CVSS: 0.0) NVT: DIRB (NASL wrapper)</p>
<p>Summary This script uses DIRB to find directories and files on web applications via brute forcing.</p>
<p>Vulnerability Detection Result DIRB could not be found in your system path. OpenVAS was unable to execute DIRB and to perform the scan you requested.</p>
<p>...continues on next page ...</p>

...continued from previous page ...
Please make sure that DIRB is installed and is available in the PATH variable defined for your environment.
Log Method Details:DIRB (NASL wrapper) OID:1.3.6.1.4.1.25623.1.0.103079 Version used: \$Revision: 13 \$

Log (CVSS: 0.0) NVT: arachni (NASL wrapper)
Summary This plugin uses arachni ruby command line to find web security issues. See the preferences section for arachni options. Note that OpenVAS is using limited set of arachni options. Therefore, for more complete web assessment, you should use standalone arachni tool for deeper/customized checks.
Vulnerability Detection Result Arachni could not be found in your system path. OpenVAS was unable to execute Arachni and to perform the scan you requested. Please make sure that Arachni is installed and that arachni is available in the PATH variable defined for your environment.
Log Method Details:arachni (NASL wrapper) OID:1.3.6.1.4.1.25623.1.0.110001 Version used: \$Revision: 683 \$

Log (CVSS: 0.0) NVT: Nikto (NASL wrapper)
Summary This plugin uses nikto(1) to find weak CGI scripts and other known issues regarding web server security. See the preferences section for configuration options.
Vulnerability Detection Result Nikto could not be found in your system path. OpenVAS was unable to execute Nikto and to perform the scan you requested. Please make sure that Nikto is installed and that nikto.pl or nikto is available in the PATH variable defined for your environment.
Log Method Details:Nikto (NASL wrapper)
...continues on next page ...

...continued from previous page ...
OID:1.3.6.1.4.1.25623.1.0.14260 Version used: \$Revision: 995 \$

Log (CVSS: 0.0) NVT: Traceroute
Summary A traceroute from the scanning server to the target system was conducted. This traceroute is provided primarily for informational value only. In the vast majority of cases, it does not represent a vulnerability. However, if the displayed traceroute contains any private addresses that should not have been publicly visible, then you have an issue you need to correct.
Vulnerability Detection Result Here is the route from 192.168.29.114 to xxx.xx.166.251: 192.168.29.114 192.168.144.1 80.58.99.57 80.58.106.161 195.95.153.10 213.27.253.25 213.27.253.26 xxx.xx.166.251
Solution Block unwanted packets from escaping your network.
Log Method Details:Traceroute OID:1.3.6.1.4.1.25623.1.0.51662 Version used: \$Revision: 975 \$

[\[return to xxx.xx.166.251\]](#)

2.1.12 Log general/CPE-T

Log (CVSS: 0.0) NVT: CPE Inventory
Summary This routine uses information collected by other routines about CPE identities (http://cpe.mitre.org/) of operating systems, services and applications detected during the scan.
Vulnerability Detection Result xxx.xx.166.251 cpe:/a:wordpress:wordpress:4.3.1 ...continues on next page ...

...continued from previous page ...	
xxx.xx.166.251 cpe:/a:php:php:5.3.3	
xxx.xx.166.251 cpe:/a:apache:http_server:2.2.3	
Log Method Details:CPE Inventory OID:1.3.6.1.4.1.25623.1.0.810002 Version used: \$Revision: 314 \$	

[\[return to xxx.xx.166.251\]](#)

This file was automatically generated.