Scan Report

November 7, 2017

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 10.0.0.2". The scan started at Tue Nov 7 23:28:58 2017 UTC and ended at Tue Nov 7 23:35:09 2017 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

Result Overview

Host	High	Medium	Low	Log	False Positive
10.0.0.2 metasploitable.penetrationtestingstarter_channel	9	15	1	0	0
Total: 1	9	15	1	0	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
Information on overrides is included in the report.
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 "Log" are not shown.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 25 results selected by the filtering described above. Before filtering there were 183 results.

Results per Host

10.0.0.2

Host scan start	Tue Nov 7 23:29:06 2017 UTC
Host scan end	Tue Nov 7 23:35:09 2017 UTC

Service (Port)	Threat Level
80/tcp	High
80/tcp	Medium
general/tcp	Low

High 80/tcp

High (CVSS: 10.0)
NVT: TWiki XSS and Command Execution Vulnerabilities

Product detection result
`cpe:/a:twiki:twiki:01.Feb.2003`
`Detected by TWiki Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800399)`

... continues on next page ...

... continued from previous page ...

Summary
The host is running TWiki and is prone to Cross-Site Scripting (XSS) and Command Execution Vulnerabilities.

Vulnerability Detection Result
`Installed version: 01.Feb.2003`
`Fixed version: 4.2.4`

Impact
Successful exploitation could allow execution of arbitrary script code or commands. This could let attackers steal cookie-based authentication credentials or compromise the affected application.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to version 4.2.4 or later, http://twiki.org/cgi-bin/view/Codev/TWikiRelease04x02x04

Affected Software/OS
TWiki, TWiki version prior to 4.2.4.

Vulnerability Insight
The flaws are due to, - %URLPARAM}}% variable is not properly sanitized which lets attackers conduct cross-site scripting attack. - %SEARCH}}% variable is not properly sanitised before being used in an eval() call which lets the attackers execute perl code through eval injection attack.

Vulnerability Detection Method
Details:`TWiki XSS and Command Execution Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.800320
Version used: `$Revision: 4227 $`

Product Detection Result
Product: `cpe:/a:twiki:twiki:01.Feb.2003`
Method: `TWiki Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.800399)

References
`CVE: CVE-2008-5304, CVE-2008-5305`
`BID:32668, 32669`
`Other:`
`URL:http://twiki.org/cgi-bin/view/Codev.SecurityAlert-CVE-2008-5304`
`URL:http://twiki.org/cgi-bin/view/Codev/SecurityAlert-CVE-2008-5305`

High (CVSS: 7.5)
NVT: phpinfo() output accessible

... continues on next page ...

... continued from previous page ...

Summary
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.

Vulnerability Detection Result
`The following files are calling the function phpinfo() which disclose potentiall`
`↪y sensitive information to the remote attacker:`
`http://metasploitable.penetrationtestingstarter_channel/phpinfo.php`
`http://metasploitable.penetrationtestingstarter_channel/mutillidae/phpinfo.php`

Impact
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.

Solution
Solution type: Workaround
Delete them or restrict access to the listened files.

Vulnerability Detection Method
Details:`phpinfo() output accessible`
OID:1.3.6.1.4.1.25623.1.0.11229
Version used: `$Revision: 6355 $`

High (CVSS: 7.5)
NVT: phpMyAdmin BLOB Streaming Multiple Input Validation Vulnerabilities

Product detection result
`cpe:/a:phpmyadmin:phpmyadmin:3.1.1`
`Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)`

Summary
phpMyAdmin is prone to multiple input-validation vulnerabilities, including an HTTP response-splitting vulnerability and a local file-include vulnerability.
These issues can be leveraged to view or execute arbitrary local scripts, or misrepresent how web content is served, cached, or interpreted. This could aid in various attacks that try to entice client users into a false sense of trust. Other attacks are also possible.
Versions prior to phpMyAdmin 3.1.3.1 are vulnerable.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution

... continues on next page ...

... continued from previous page ...

Vendor updates are available. Please see http://www.phpmyadmin.net for more Information.

Vulnerability Detection Method
Details:phpMyAdmin BLOB Streaming Multiple Input Validation Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.100078
Version used: $Revision: 6704 $

Product Detection Result
Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Method: phpMyAdmin Detection
OID: 1.3.6.1.4.1.25623.1.0.900129)

References
BID:34253
Other:
URL:http://www.securityfocus.com/bid/34253

High (CVSS: 7.5)
NVT: phpMyAdmin Configuration File PHP Code Injection Vulnerability

Product detection result
cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)

Summary
According to its version number, the remote version of phpMyAdmin is prone to a remote PHP code-injection vulnerability.
An attacker can exploit this issue to inject and execute arbitrary malicious PHP code in the context of the webserver process. This may facilitate a compromise of the application and the underlying system other attacks are also possible.
phpMyAdmin 3.x versions prior to 3.1.3.2 are vulnerable.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Vendor updates are available. Please see http://www.phpmyadmin.net for more Information.

Vulnerability Detection Method
Details:phpMyAdmin Configuration File PHP Code Injection Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100144
Version used: $Revision: 6704 $

Product Detection Result

... continues on next page ...

... continued from previous page ...

Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Method: phpMyAdmin Detection
OID: 1.3.6.1.4.1.25623.1.0.900129)

References
CVE: CVE-2009-1285
BID:34526
Other:
URL:http://www.securityfocus.com/bid/34526

High (CVSS: 7.5)
NVT: phpMyAdmin Unspecified SQL Injection and Cross Site Scripting Vulnerabilities

Product detection result
cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)

Summary
phpMyAdmin is prone to SQL-injection and cross-site scripting vulnerabilities because it fails to sufficiently sanitize user- supplied data.
Exploiting these issues could allow an attacker to steal cookie- based authentication credentials, compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database.
Versions prior to phpMyAdmin 2.11.9.6 and 3.2.2.1 are affected.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Vendor updates are available. Please see the references for details.

Vulnerability Detection Method
Details:phpMyAdmin Unspecified SQL Injection and Cross Site Scripting Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.100307
Version used: $Revision: 6948 $

Product Detection Result
Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Method: phpMyAdmin Detection
OID: 1.3.6.1.4.1.25623.1.0.900129)

References
CVE: CVE-2009-3696, CVE-2009-3697
BID:36658

... continues on next page ...

... continued from previous page ...

Other:
URL:http://www.securityfocus.com/bid/36658
URL:http://www.phpmyadmin.net/
URL:http://freshmeat.net/projects/phpmyadmin/releases/306669
URL:http://freshmeat.net/projects/phpmyadmin/releases/306667

High (CVSS: 7.5)
NVT: phpMyAdmin Code Injection and XSS Vulnerability

Product detection result
cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)

Summary
phpMyAdmin is prone to a remote PHP code-injection vulnerability and to a cross-site scripting vulnerability.
An attacker can exploit this issue to inject and execute arbitrary malicious PHP code in the context of the webserver process. This may facilitate a compromise of the application and the underlying system other attacks are also possible.
Versions prior to phpMyAdmin 2.11.9.5 and 3.1.3.1 are vulnerable.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Vendor updates are available. Please see http://www.phpmyadmin.net for more Information.

Vulnerability Detection Method
Details:phpMyAdmin Code Injection and XSS Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100077
Version used: $Revision: 6704 $

Product Detection Result
Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Method: phpMyAdmin Detection
OID: 1.3.6.1.4.1.25623.1.0.900129)

References
CVE: CVE-2009-1151
BID:34236, 34251
Other:
URL:http://www.securityfocus.com/bid/34236
URL:http://www.securityfocus.com/bid/34251

High (CVSS: 7.5)
NVT: Tiki Wiki CMS Groupware < 4.2 Multiple Unspecified Vulnerabilities

Product detection result
cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5
Detected by Tiki Wiki CMS Groupware Version Detection (OID: 1.3.6.1.4.1.25623.1.
↪0.901001)

Summary
Tiki Wiki CMS Groupware is prone to multiple unspecified vulnerabilities, including:
- An unspecified SQL-injection vulnerability - An unspecified authentication-bypass vulnerability
- An unspecified vulnerability

Vulnerability Detection Result
Installed version: 1.9.5
Fixed version: 4.2

Impact
Exploiting these issues could allow an attacker to compromise the application, access or modify data, exploit latent vulnerabilities in the underlying database, and gain unauthorized access to the affected application. Other attacks are also possible.

Solution
Solution type: VendorFix
The vendor has released an advisory and fixes. Please see the references for details.

Affected Software/OS
Versions prior to Tiki Wiki CMS Groupware 4.2 are vulnerable.

Vulnerability Detection Method
Details:Tiki Wiki CMS Groupware < 4.2 Multiple Unspecified Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.100537
Version used: $Revision: 5144 $

Product Detection Result
Product: cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5
Method: Tiki Wiki CMS Groupware Version Detection
OID: 1.3.6.1.4.1.25623.1.0.901001)

References
CVE: CVE-2010-1135, CVE-2010-1134, CVE-2010-1133, CVE-2010-1136
BID:38608
Other:
URL:http://www.securityfocus.com/bid/38608
URL:http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision=247
↪34

. . . continues on next page . . .

... continued from previous page ...

URL:http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision=250
↪46
URL:http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision=254
↪24
URL:http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision=254
↪35
URL:http://info.tikiwiki.org/article86-Tiki-Announces-3-5-and-4-2-Releases
URL:http://info.tikiwiki.org/tiki-index.php?page=homepage

High (CVSS: 7.5)
NVT: PHP-CGI-based setups vulnerability when parsing query string parameters from php files.

Summary
PHP is prone to an information-disclosure vulnerability.

Vulnerability Detection Result
Vulnerable url: http://metasploitable.penetrationtestingstarter_channel/cgi-bin/
↪php

Impact
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.

Solution
Solution type: VendorFix
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.

Vulnerability Insight
When PHP is used in a CGI-based setup (such as Apache's mod_cgid), the php-cgi receives a processed query string parameter as command line arguments which allows command-line switches, such as -s, -d or -c to be passed to the php-cgi binary, which can be exploited to disclose source code and obtain arbitrary code execution.
An example of the -s command, allowing an attacker to view the source code of index.php is below:
http://localhost/index.php?-s

Vulnerability Detection Method
Details:PHP-CGI-based setups vulnerability when parsing query string parameters from ph.
↪..
OID:1.3.6.1.4.1.25623.1.0.103482
Version used: $Revision: 5958 $

References
CVE: CVE-2012-1823, CVE-2012-2311, CVE-2012-2336, CVE-2012-2335
BID:53388

... continues on next page ...

... continued from previous page ...

```
Other:
  URL:http://www.h-online.com/open/news/item/Critical-open-hole-in-PHP-creates-r
↪isks-Update-1567532.html
   URL:http://www.kb.cert.org/vuls/id/520827
   URL:http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/
   URL:https://bugs.php.net/bug.php?id=61910
   URL:http://www.php.net/manual/en/security.cgi-bin.php
   URL:http://www.securityfocus.com/bid/53388
```

High (CVSS: 7.5)
NVT: Test HTTP dangerous methods

Summary
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.

Vulnerability Detection Result

```
We could upload the following files via the PUT method at this web server:
http://metasploitable.penetrationtestingstarter_channel/dav/puttest1945646982.ht
↪ml
We could delete the following files via the DELETE method at this web server:
http://metasploitable.penetrationtestingstarter_channel/dav/puttest1945646982.ht
↪ml
```

Impact
- 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.

Solution
Solution type: Mitigation
Use access restrictions to these dangerous HTTP methods or disable them completely.

Vulnerability Detection Method
Details:`Test HTTP dangerous methods`
OID:1.3.6.1.4.1.25623.1.0.10498
Version used: `$Revision: 4295 $`

References

```
BID:12141
Other:
  OWASP:OWASP-CM-001
```

[return to 10.0.0.2]

Medium 80/tcp

Medium (CVSS: 6.8)
NVT: TWiki Cross-Site Request Forgery Vulnerability - Sep10

Product detection result
`cpe:/a:twiki:twiki:01.Feb.2003`
`Detected by TWiki Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800399)`

Summary
The host is running TWiki and is prone to Cross-Site Request Forgery vulnerability.

Vulnerability Detection Result
`Installed version: 01.Feb.2003`
`Fixed version: 4.3.2`

Impact
Successful exploitation will allow attacker to gain administrative privileges on the target application and can cause CSRF attack.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to TWiki version 4.3.2 or later, For updates refer to http://twiki.org/cgi-bin/view/Codev/DownloadTWiki

Affected Software/OS
TWiki version prior to 4.3.2

Vulnerability Insight
Attack can be done by tricking an authenticated TWiki user into visiting a static HTML page on another side, where a Javascript enabled browser will send an HTTP POST request to TWiki, which in turn will process the request as the TWiki user.

Vulnerability Detection Method
Details:`TWiki Cross-Site Request Forgery Vulnerability - Sep10`
OID:1.3.6.1.4.1.25623.1.0.801281
Version used: `$Revision: 4293 $`

Product Detection Result
Product: `cpe:/a:twiki:twiki:01.Feb.2003`
Method: `TWiki Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.800399)

References
`CVE: CVE-2009-4898`

. . . continues on next page . . .

... continued from previous page ...

Other:
URL:http://www.openwall.com/lists/oss-security/2010/08/03/8
URL:http://www.openwall.com/lists/oss-security/2010/08/02/17
URL:http://twiki.org/cgi-bin/view/Codev/SecurityAuditTokenBasedCsrfFix

Medium (CVSS: 6.5)
NVT: phpMyAdmin Bookmark Security Bypass Vulnerability

Product detection result
cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)

Summary
phpMyAdmin is prone to a security-bypass vulnerability that affects bookmarks.
Successfully exploiting this issue allows a remote attacker to bypass certain security restrictions and perform unauthorized actions.
Versions prior to phpMyAdmin 3.3.9.2 and 2.11.11.3 are vulnerable.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Updates are available. Please see the references for details.

Vulnerability Detection Method
Details:phpMyAdmin Bookmark Security Bypass Vulnerability
OID:1.3.6.1.4.1.25623.1.0.103076
Version used: $Revision: 7006 $

Product Detection Result
Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Method: phpMyAdmin Detection
OID: 1.3.6.1.4.1.25623.1.0.900129)

References
CVE: CVE-2011-0986, CVE-2011-0987
BID:46359
Other:
URL:https://www.securityfocus.com/bid/46359
URL:http://www.phpmyadmin.net/
URL:http://www.phpmyadmin.net/home_page/security/PMASA-2011-2.php

Medium (CVSS: 6.0)
NVT: TWiki Cross-Site Request Forgery Vulnerability

Product detection result
cpe:/a:twiki:twiki:01.Feb.2003
Detected by TWiki Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800399)

Summary
The host is running TWiki and is prone to Cross-Site Request Forgery Vulnerability.

Vulnerability Detection Result
Installed version: 01.Feb.2003
Fixed version: 4.3.1

Impact
Successful exploitation will allow attacker to gain administrative privileges on the target application and can cause CSRF attack.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to version 4.3.1 or later, http://twiki.org/cgi-bin/view/Codev/DownloadTWiki

Affected Software/OS
TWiki version prior to 4.3.1

Vulnerability Insight
Remote authenticated user can create a specially crafted image tag that, when viewed by the target user, will update pages on the target system with the privileges of the target user via HTTP requests.

Vulnerability Detection Method
Details:TWiki Cross-Site Request Forgery Vulnerability
OID:1.3.6.1.4.1.25623.1.0.800400
Version used: $Revision: 4892 $

Product Detection Result
Product: cpe:/a:twiki:twiki:01.Feb.2003
Method: TWiki Version Detection
OID: 1.3.6.1.4.1.25623.1.0.800399)

References
CVE: CVE-2009-1339
Other:
URL:http://secunia.com/advisories/34880
URL:http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=526258

... continues on next page ...

... continued from previous page ...

URL:http://twiki.org/p/pub/Codev/SecurityAlert-CVE-2009-1339/TWiki-4.3.0-c-di
↪ff-cve-2009-1339.txt

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: 6063 $

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: /doc directory browsable

Summary
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.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

Vulnerable url: http://metasploitable.penetrationtestingstarter_channel/doc/

Solution
Solution type: Mitigation
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>

Vulnerability Detection Method
Details:/doc directory browsable
OID:1.3.6.1.4.1.25623.1.0.10056
Version used: $Revision: 4288 $

References
CVE: CVE-1999-0678
BID:318

Medium (CVSS: 5.0)
NVT: Tiki Wiki CMS Groupware 'fixedURLData' Local File Inclusion Vulnerability

Product detection result
cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5
Detected by Tiki Wiki CMS Groupware Version Detection (OID: 1.3.6.1.4.1.25623.1.
↪0.901001)

Summary
The host is installed with Tiki Wiki CMS Groupware and is prone to a local file inclusion vulnerability.

Vulnerability Detection Result
Installed version: 1.9.5
Fixed version: 12.11

Impact
Successful exploitation will allow an user having access to the admin backend to gain access to arbitrary files and to compromise the application.
Impact Level: System/Application

Solution
Solution type: VendorFix
Upgrade to Tiki Wiki CMS Groupware version 12.11 LTS, 15.4 or later. For updates refer to https://tiki.org

Affected Software/OS

... continues on next page ...

... continued from previous page ...

Tiki Wiki CMS Groupware versions:
- below 12.11 LTS
- 13.x, 14.x and 15.x below 15.4

Vulnerability Insight
The Flaw is due to improper sanitization of input passed to the 'fixedURLData' parameter of the 'display_banner.php' script.

Vulnerability Detection Method
Get the installed version with the help of the detect NVT and check the version is vulnerable or not.
Details:`Tiki Wiki CMS Groupware 'fixedURLData' Local File Inclusion Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.108064
Version used: `$Revision: 5144 $`

Product Detection Result
Product: `cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5`
Method: `Tiki Wiki CMS Groupware Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.901001)

References
```
CVE: CVE-2016-10143
Other:
  URL:http://tiki.org/article445-Security-updates-Tiki-16-2-15-4-and-Tiki-12-11-
↪released
   URL:https://sourceforge.net/p/tikiwiki/code/60308/
```

Medium (CVSS: 5.0)
NVT: Tiki Wiki CMS Groupware Input Sanitation Weakness Vulnerability

Product detection result
```
cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5
Detected by Tiki Wiki CMS Groupware Version Detection (OID: 1.3.6.1.4.1.25623.1.
↪0.901001)
```

Summary
The host is installed with Tiki Wiki CMS Groupware and is prone to input sanitation weakness vulnerability.

Vulnerability Detection Result
```
Installed version: 1.9.5
Fixed version:     2.2
```

Impact
Successful exploitation could allow arbitrary code execution in the context of an affected site.

... continues on next page ...

... continued from previous page ...

Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to version 2.2 or latest http://info.tikiwiki.org/tiki-index.php?page=Get+Tiki&bl

Affected Software/OS
Tiki Wiki CMS Groupware version prior to 2.2 on all running platform

Vulnerability Insight
The vulnerability is due to input validation error in tiki-error.php which fails to sanitise before being returned to the user.

Vulnerability Detection Method
Details:`Tiki Wiki CMS Groupware Input Sanitation Weakness Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.800315
Version used: `$Revision: 5144 $`

Product Detection Result
Product: `cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5`
Method: `Tiki Wiki CMS Groupware Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.901001)

References
`CVE: CVE-2008-5318, CVE-2008-5319`
`Other:`
`URL:http://secunia.com/advisories/32341`
`URL:http://info.tikiwiki.org/tiki-read_article.php?articleId=41`

Medium (CVSS: 5.0)
NVT: awiki Multiple Local File Include Vulnerabilities

Summary
awiki is prone to multiple local file-include vulnerabilities because it fails to properly sanitize user-supplied input.

Vulnerability Detection Result
`Vulnerable url: http://metasploitable.penetrationtestingstarter_channel/mutillid`
`↪ae/index.php?page=/etc/passwd`

Impact
An attacker can exploit this vulnerability to obtain potentially sensitive information and execute arbitrary local scripts in the context of the webserver process. This may allow the attacker to compromise the application and the host other attacks are also possible.

... continues on next page ...

... continued from previous page ...

Solution
Solution type: WillNotFix
No solution or patch was made available for at least one year since disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Affected Software/OS
awiki 20100125 is vulnerable other versions may also be affected.

Vulnerability Detection Method
Details:awiki Multiple Local File Include Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.103210
Version used: $Revision: 7577 $

References
BID:49187
Other:
URL:http://www.securityfocus.com/bid/49187
URL:http://www.kobaonline.com/awiki/

Medium (CVSS: 4.3)
NVT: phpMyAdmin SQL bookmark XSS Vulnerability

Product detection result
cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)

Summary
This host is running phpMyAdmin and is prone to Cross Site Scripting vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will let the attacker cause XSS attacks and inject malicious web script or HTML code via a crafted SQL bookmarks.

Solution
Apply the respective patches or upgrade to version 3.2.0.1 http://www.phpmyadmin.net/home_page/downloads.php http://phpmyadmin.svn.sourceforge.net/viewvc/phpmy
*** Note: Ignore the warning if above mentioned patches are applied. *****

Affected Software/OS
phpMyAdmin version 3.0.x to 3.2.0.rc1

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
This flaw arises because the input passed into SQL bookmarks is not adequately sanitised before using it in dynamically generated content.

Vulnerability Detection Method
Details:`phpMyAdmin SQL bookmark XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.800595
Version used: `$Revision: 4869 $`

Product Detection Result
Product: `cpe:/a:phpmyadmin:phpmyadmin:3.1.1`
Method: `phpMyAdmin Detection`
OID: 1.3.6.1.4.1.25623.1.0.900129)

References
`CVE: CVE-2009-2284`
`BID:35543`
`Other:`
`URL:http://secunia.com/advisories/35649`
`URL:http://www.phpmyadmin.net/home_page/security/PMASA-2009-5.php`

Medium (CVSS: 4.3)
NVT: phpMyAdmin Database Search Cross Site Scripting Vulnerability

Product detection result
`cpe:/a:phpmyadmin:phpmyadmin:3.1.1`
`Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)`

Summary
phpMyAdmin is prone to a cross-site scripting vulnerability because it fails to sufficiently sanitize user-supplied data.
An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may allow the attacker to steal cookie-based authentication credentials and to launch other attacks.
Versions prior to phpMyAdmin 3.3.8.1 and 2.11.11.1 are vulnerable.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Vendor updates are available. Please see the references for more information.

Vulnerability Detection Method
Details:`phpMyAdmin Database Search Cross Site Scripting Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.100939

... continues on next page ...

... continued from previous page ...

Version used: $Revision: 6705 $

Product Detection Result
Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Method: phpMyAdmin Detection
OID: 1.3.6.1.4.1.25623.1.0.900129)

References
CVE: CVE-2010-4329
BID:45100
Other:
URL:https://www.securityfocus.com/bid/45100
URL:http://www.phpmyadmin.net/
URL:http://www.phpmyadmin.net/home_page/security/PMASA-2010-8.php

Medium (CVSS: 4.3)
NVT: phpMyAdmin Multiple Cross Site Scripting Vulnerabilities

Product detection result
cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)

Summary
phpMyAdmin is prone to multiple cross-site scripting vulnerabilities because it fails to properly sanitize user-supplied input.
An attacker may leverage these issues to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This can allow the attacker to steal cookie-based authentication credentials and launch other attacks.
The following versions are vulnerable:
phpMyAdmin 2.11.x prior to 2.11.10.1 phpMyAdmin 3.x prior to 3.3.5.1

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Updates are available. Please see the references for details.

Vulnerability Detection Method
Details:phpMyAdmin Multiple Cross Site Scripting Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.100761
Version used: $Revision: 6705 $

Product Detection Result
Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Method: phpMyAdmin Detection

... continues on next page ...

... continued from previous page ...

OID: 1.3.6.1.4.1.25623.1.0.900129)

References
CVE: CVE-2010-3056
BID:42584
Other:
URL:https://www.securityfocus.com/bid/42584
URL:http://www.phpmyadmin.net/
URL:http://www.phpmyadmin.net/home_page/security/PMASA-2010-5.php

Medium (CVSS: 4.3)
NVT: phpMyAdmin Debug Backtrace Cross Site Scripting Vulnerability

Product detection result
cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)

Summary
phpMyAdmin is prone to a cross-site scripting vulnerability because it fails to sufficiently sanitize user-supplied data.
An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may allow the attacker to steal cookie-based authentication credentials and to launch other attacks.
Versions prior to phpMyAdmin 3.3.6 are vulnerable other versions may also be affected.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
Vendor updates are available. Please see the references for more information.

Vulnerability Detection Method
Details:phpMyAdmin Debug Backtrace Cross Site Scripting Vulnerability
OID:1.3.6.1.4.1.25623.1.0.100775
Version used: $Revision: 6705 $

Product Detection Result
Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Method: phpMyAdmin Detection
OID: 1.3.6.1.4.1.25623.1.0.900129)

References
CVE: CVE-2010-2958
BID:42874

... continues on next page ...

... continued from previous page ...

```
Other:
  URL:https://www.securityfocus.com/bid/42874
   URL:http://www.phpmyadmin.net/
   URL:http://www.phpmyadmin.net/home_page/security/PMASA-2010-6.php
   URL:http://www.phpmyadmin.git.sourceforge.net/git/gitweb.cgi?p=phpmyadmin/php
↪myadmin;a=commitdiff;h=133a77fac7d31a38703db2099a90c1b49de62e37
```

Medium (CVSS: 4.3)
NVT: phpMyAdmin Setup Script Request Cross Site Scripting Vulnerability

Product detection result
`cpe:/a:phpmyadmin:phpmyadmin:3.1.1`
`Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)`

Summary
The host is running phpMyAdmin and is prone to Cross-Site Scripting Vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to execute arbitrary web script or HTML in a user's browser session in the context of an affected site. Impact Level: Application

Solution
Upgrade to phpMyAdmin version 3.3.7 or later, For updates refer to http://www.phpmyadmin.net/home_page/downloads.php

Affected Software/OS
phpMyAdmin versions 3.x before 3.3.7

Vulnerability Insight
The flaw is caused by an unspecified input validation error when processing spoofed requests sent to setup script, which could be exploited by attackers to cause arbitrary scripting code to be executed on the user's browser session in the security context of an affected site.

Vulnerability Detection Method
Details:`phpMyAdmin Setup Script Request Cross Site Scripting Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.801286
Version used: `$Revision: 5373 $`

Product Detection Result
Product: `cpe:/a:phpmyadmin:phpmyadmin:3.1.1`
Method: `phpMyAdmin Detection`
OID: 1.3.6.1.4.1.25623.1.0.900129)

... continues on next page ...

... continued from previous page ...

References
CVE: CVE-2010-3263
Other:
URL:http://secunia.com/advisories/41210
URL:http://xforce.iss.net/xforce/xfdb/61675
URL:http://www.phpmyadmin.net/home_page/security/PMASA-2010-7.php

Medium (CVSS: 4.3)
NVT: phpMyAdmin 'error.php' Cross Site Scripting Vulnerability

Product detection result
cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)

Summary
The host is running phpMyAdmin and is prone to Cross-Site Scripting Vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to inject arbitrary HTML code within the error page and conduct phishing attacks.
Impact Level: Application

Solution
Solution type: WillNotFix
No solution or patch was made available for at least one year since disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Affected Software/OS
phpMyAdmin version 3.3.8.1 and prior.

Vulnerability Insight
The flaw is caused by input validation errors in the 'error.php' script when processing crafted BBcode tags containing '@' characters, which could allow attackers to inject arbitrary HTML code within the error page and conduct phishing attacks.

Vulnerability Detection Method
Details:phpMyAdmin 'error.php' Cross Site Scripting Vulnerability
OID:1.3.6.1.4.1.25623.1.0.801660
Version used: $Revision: 5323 $

... continues on next page ...

... continued from previous page ...

Product Detection Result
Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Method: phpMyAdmin Detection
OID: 1.3.6.1.4.1.25623.1.0.900129)

References
CVE: CVE-2010-4480
Other:
URL:http://www.exploit-db.com/exploits/15699/
URL:http://www.vupen.com/english/advisories/2010/3133

Medium (CVSS: 4.3)
NVT: Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability

Summary
This host is running Apache HTTP Server and is prone to cookie information disclosure vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to obtain sensitive information that may aid in further attacks.
Impact Level: Application

Solution
Solution type: VendorFix
Upgrade to Apache HTTP Server version 2.2.22 or later, For updates refer to http://httpd.apache.org/

Affected Software/OS
Apache HTTP Server versions 2.2.0 through 2.2.21

Vulnerability Insight
The flaw is due to an error within the default error response for status code 400 when no custom ErrorDocument is configured, which can be exploited to expose 'httpOnly' cookies.

Vulnerability Detection Method
Details:Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability
OID:1.3.6.1.4.1.25623.1.0.902830
Version used: $Revision: 6720 $

References
CVE: CVE-2012-0053

... continues on next page ...

... continued from previous page ...

```
BID:51706
Other:
  URL:http://secunia.com/advisories/47779
   URL:http://www.exploit-db.com/exploits/18442
   URL:http://rhn.redhat.com/errata/RHSA-2012-0128.html
   URL:http://httpd.apache.org/security/vulnerabilities_22.html
   URL:http://svn.apache.org/viewvc?view=revision&revision=1235454
   URL:http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.htm
↪l
```

[return to 10.0.0.2]

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:
Packet 1: 222961493
Packet 2: 222961762
```

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution
Solution type: Mitigation
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

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: 7277 $`

References
`Other:`
`URL:http://www.ietf.org/rfc/rfc1323.txt`

[return to 10.0.0.2]