Noman Ahmed Project 2

Report generated by Nessus™ Thu, 12 Jan 2023 07:16:07 EST

Vulnerabilities by Host

Vulnerabilities by Host

testphp.vulnweb.com

2	12	16	2	21
CRITICAL	HIGH	MEDIUM	LOW	INFO

Host Information

DNS Name:	testphp.vulnweb.com
IP:	44.228.249.3
OS:	AIX 5.3

Vulnerabilities

58987 - PHP Unsupported Version Detection

Synopsis

The remote host contains an unsupported version of a web application scripting language.

Description

According to its version, the installation of PHP on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

See Also

http://php.net/eol.php

https://wiki.php.net/rfc/releaseprocess

Solution

Upgrade to a version of PHP that is currently supported.

Risk Factor

Critical

CVSS v3.0 Base Score

10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

XREF	IAVA:0001-A-0581

Plugin Information

Published: 2012/05/04, Modified: 2022/12/07

Plugin Output

tcp/80/www

```
Source              : X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Installed version   : 5.6.40-38+ubuntu20.04.1+deb.sury.org+1
End of support date : 2018/12/31
Announcement        : http://php.net/supported-versions.php
Supported versions  : 8.0.x / 8.1.x
```

tcp/80/www

```
Source              : http://testphp.vulnweb.com/secured/phpinfo.php
Installed version   : 5.1.6
End of support date : 2006/08/24
Announcement        : http://php.net/eol.php
Supported versions  : 8.0.x / 8.1.x
```

42479 - CGI Generic SQL Injection (2nd pass)

Synopsis

A web application is potentially vulnerable to SQL injection.

Description

By providing specially crafted parameters to CGIs, Nessus was able to get an error from the underlying database. This error suggests that the CGI is affected by a SQL injection vulnerability.

An attacker may exploit this flaw to bypass authentication, read confidential data, modify the remote database, or even take control of the remote operating system.

See Also

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

http://www.securiteam.com/securityreviews/5DP0N1P76E.html

http://www.nessus.org/u?e5c79f44

http://www.nessus.org/u?11ab1866

Solution

Modify the relevant CGIs so that they properly escape arguments.

Risk Factor

High

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

References

XREF	CWE:20
XREF	CWE:77
XREF	CWE:89
XREF	CWE:713
XREF	CWE:722
XREF	CWE:727
XREF	CWE:751
XREF	CWE:801
XREF	CWE:810
XREF	CWE:928
XREF	CWE:929

Plugin Information

Published: 2009/11/12, Modified: 2021/01/19

Plugin Output

tcp/80/www

```
During testing for cookie manipulation vulnerabilities,
 SQL errors were noticed, suggesting that the scripts / parameters
listed below may also be vulnerable to SQL Injection (SQLi).

-------- request  --------
GET /listproducts.php?cat=<script>document.cookie="testsocd=9059;"</script> HTTP/1.1
Host: testphp.vulnweb.com
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Keep-Alive
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
------------------------

-------- output --------
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
Error: You have an error in your SQL syntax; check the manual that corre
sponds to your MySQL server version for the right syntax to use near '=<
script>document.cookie="testsocd=9059;"</script>' at line 1
Warning: mysql_fetch_array() expects parameter 1 to be resource, b [...]
</div>
------------------------


During testing for uncontrolled redirection vulnerabilities,
 SQL errors were noticed, suggesting that the scripts / parameters
listed below may also be vulnerable to SQL Injection (SQLi).

-------- request  --------
GET /listproducts.php?cat=.example.com HTTP/1.1
Host: testphp.vulnweb.com
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Keep-Alive
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
------------------------

-------- output --------
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
Error: You have an error in your SQL syntax; check the manual that corre
sponds to your MySQL server version for the right syntax to use near '.e
xample.com' at line 1
Warning: mysql_fetch_array() expects parameter 1 to be resource, b [...]
</div>
------------------------


During testing for cross-site scripting (quick test) vulnerabilities,  [...]
```

35043 - PHP 5 < 5.2.7 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP installed on the remote host is prior to 5.2.7. It is, therefore, affected by multiple vulnerabilities :

- There is a buffer overflow flaw in the bundled PCRE library that allows a denial of service attack.

(CVE-2008-2371)

- Multiple directory traversal vulnerabilities exist in functions such as 'posix_access', 'chdir', and 'ftok'

that allow a remote attacker to bypass 'safe_mode'

restrictions. (CVE-2008-2665 and CVE-2008-2666).

- A buffer overflow flaw in 'php_imap.c' may be triggered when processing long message headers due to the use of obsolete API calls. This can be exploited to cause a denial of service or to execute arbitrary code.

(CVE-2008-2829)

- A buffer overflow in the 'imageloadfont' function in 'ext/gd/gd.c' can be triggered when a specially crafted font is given. This can be exploited to cause a denial of service or to execute arbitrary code. (CVE-2008-3658)

- A buffer overflow flaw exists in PHP's internal function 'memnstr' which can be exploited by an attacker using the delimiter argument to the 'explode' function. This can be used to cause a denial of service or to execute arbitrary code. (CVE-2008-3659)

- When PHP is used as a FastCGI module, an attacker by requesting a file whose file name extension is preceded by multiple dots can cause a denial of service.

(CVE-2008-3660)

- A heap-based buffer overflow flaw in the mbstring extension can be triggered via a specially crafted string containing an HTML entity that is not handled during Unicode conversion. This can be exploited to execute arbitrary code.(CVE-2008-5557)

- Improper initialization of global variables 'page_uid'

and 'page_gid' when PHP is used as an Apache module allows the bypassing of security restriction due to SAPI 'php_getuid' function overloading. (CVE-2008-5624)

- PHP does not enforce the correct restrictions when 'safe_mode' is enabled through a 'php_admin_flag'

setting in 'httpd.conf'. This allows an attacker, by placing a specially crafted 'php_value' entry in '.htaccess', to able to write to arbitrary files.

(CVE-2008-5625)

- The 'ZipArchive::extractTo' function in the ZipArchive extension fails to filter directory traversal sequences from file names. An attacker can exploit this to write to arbitrary files. (CVE-2008-5658)

- Under limited circumstances, an attacker can cause a file truncation to occur when calling the 'dba_replace'

function with an invalid argument. (CVE-2008-7068)

- A buffer overflow error exists in the function 'date_from_ISO8601' function within file 'xmlrpc.c' because user-supplied input is improperly validated.
This can be exploited by a remote attacker to cause a denial of service or to execute arbitrary code. (CVE-2014-8626)

See Also

http://cxsecurity.com/issue/WLB-2008110041
http://cxsecurity.com/issue/WLB-2008110058
http://cxsecurity.com/issue/WLB-2008120011
https://seclists.org/fulldisclosure/2008/Jun/237
https://seclists.org/fulldisclosure/2008/Jun/238
https://www.openwall.com/lists/oss-security/2008/08/08/2
https://www.openwall.com/lists/oss-security/2008/08/13/8
https://seclists.org/fulldisclosure/2008/Nov/674
https://seclists.org/fulldisclosure/2008/Dec/90
https://bugs.php.net/bug.php?id=42862
https://bugs.php.net/bug.php?id=45151
https://bugs.php.net/bug.php?id=45722
http://www.php.net/releases/5_2_7.php
http://www.php.net/ChangeLog-5.php#5.2.7

Solution

Upgrade to PHP version 5.2.8 or later.

Note that version 5.2.7 has been removed from distribution because of a regression in that version that results in the 'magic_quotes_gpc'
setting remaining off even if it was set to on.

Risk Factor

High

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	29796
BID	29797
BID	29829
BID	30087
BID	30649
BID	31612
BID	32383
BID	32625
BID	32688
BID	32948
BID	70928
CVE	CVE-2008-2371
CVE	CVE-2008-2665
CVE	CVE-2008-2666
CVE	CVE-2008-2829
CVE	CVE-2008-3658
CVE	CVE-2008-3659
CVE	CVE-2008-3660
CVE	CVE-2008-5557
CVE	CVE-2008-5624
CVE	CVE-2008-5625
CVE	CVE-2008-5658
CVE	CVE-2008-7068
CVE	CVE-2014-8626
XREF	CWE:20
XREF	CWE:22
XREF	CWE:119
XREF	CWE:264

Plugin Information

Published: 2008/12/05, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Version source     : http://testphp.vulnweb.com/secured/phpinfo.php
Installed version  : 5.1.6
Fixed version      : 5.2.7
```

31649 - PHP 5.x < 5.2 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is affected by multiple buffer overflows.

Description

According to its banner, the version of PHP 5.x installed on the remote host is older than 5.2. Such versions may be affected by several buffer overflows.

To exploit these issues, an attacker would need the ability to upload an arbitrary PHP script on the remote server or to manipulate several variables processed by some PHP functions such as 'htmlentities().'

See Also

http://www.hardened-php.net/advisory_092006.133.html

http://www.php.net/releases/5_2_0.php

Solution

Upgrade to PHP version 5.2.0 or later.

Risk Factor

High

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	20349
BID	20879
BID	49634
CVE	CVE-2006-1015
CVE	CVE-2006-1549
CVE	CVE-2006-2660
CVE	CVE-2006-4486
CVE	CVE-2006-4625
CVE	CVE-2006-4812
CVE	CVE-2006-5465

CVE	CVE-2006-5706
CVE	CVE-2006-7205
CVE	CVE-2007-0448
CVE	CVE-2007-1381
CVE	CVE-2007-1584
CVE	CVE-2007-1888
CVE	CVE-2007-2844
CVE	CVE-2007-5424
XREF	CWE:94
XREF	CWE:119
XREF	CWE:399

Plugin Information

Published: 2008/03/25, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Version source     : http://testphp.vulnweb.com/secured/phpinfo.php
Installed version  : 5.1.6
Fixed version      : 5.2
```

17797 - PHP 5.x < 5.2.2 Multiple vulnerabilities

Synopsis

The remote web server uses a version of PHP that is affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP 5.x installed on the remote host is older than 5.2.2. It is, therefore, affected by multiple vulnerabilities:

- A heap-based buffer overflow vulnerability was found in PHP's gd extension. A script that could be forced to process WBMP images from an untrusted source could result in arbitrary code execution. (CVE-2007-1001)

- A vulnerability in the way the mbstring extension setglobal variables was discovered where a script using the mb_parse_str() function to set global variables could be forced to to enable the register_globals configuration option, possibly resulting in global variable injection. (CVE-2007-1583)

- A context-dependent attacker could read portions of heap memory by executing certain scripts with a serialized data input string beginning with 'S:', which did not properly track the number of input bytes being processed. (CVE-2007-1649)

- A vulnerability in how PHP's mail() function processed email messages, truncating potentially important information after the first ASCIIZ (\0) byte.

(CVE-2007-1717)

- A vulnerability in how PHP's mail() function processed header data was discovered. If a script sent mail using a subject header containing a string from an untrusted source, a remote attacker could send bulk email to unintended recipients (CVE-2007-1718).

See Also

http://www.php.net/releases/5_2_2.php

Solution

Upgrade to PHP version 5.2.2 or later.

Risk Factor

High

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

6.7 (CVSS:3.0/E:P/RL:O/RC:C)

CVSS v2.0 Base Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:C/I:N/A:N)

CVSS v2.0 Temporal Score

6.1 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	23105
BID	23357
CVE	CVE-2007-1001
CVE	CVE-2007-1583
CVE	CVE-2007-1649
CVE	CVE-2007-1717
CVE	CVE-2007-1718

Plugin Information

Published: 2012/01/11, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Version source     : http://testphp.vulnweb.com/secured/phpinfo.php
Installed version  : 5.1.6
Fixed version      : 5.2.2
```

24907 - PHP < 5.2.1 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is affected by multiple flaws.

Description

According to its banner, the version of PHP installed on the remote host is older than 5.2.1. Such versions may be affected by several issues, including buffer overflows, format string vulnerabilities, arbitrary code execution, 'safe_mode' and 'open_basedir' bypasses, and clobbering of super-globals.

See Also

http://www.php.net/releases/5_2_1.php

Solution

Upgrade to PHP version 5.2.1 or later.

Risk Factor

High

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	21508
BID	22496
BID	22805
BID	22806
BID	22862
BID	22922
BID	23119
BID	23120
BID	23219
BID	23233
BID	23234
BID	23235
BID	23236

BID	23237
BID	23238
CVE	CVE-2006-6383
CVE	CVE-2007-0905
CVE	CVE-2007-0906
CVE	CVE-2007-0907
CVE	CVE-2007-0908
CVE	CVE-2007-0909
CVE	CVE-2007-0910
CVE	CVE-2007-0988
CVE	CVE-2007-1376
CVE	CVE-2007-1380
CVE	CVE-2007-1383
CVE	CVE-2007-1452
CVE	CVE-2007-1453
CVE	CVE-2007-1454
CVE	CVE-2007-1700
CVE	CVE-2007-1701
CVE	CVE-2007-1824
CVE	CVE-2007-1825
CVE	CVE-2007-1835
CVE	CVE-2007-1884
CVE	CVE-2007-1885
CVE	CVE-2007-1886
CVE	CVE-2007-1887
CVE	CVE-2007-1889
CVE	CVE-2007-1890
CVE	CVE-2007-4441
CVE	CVE-2007-4586
XREF	CWE:20
XREF	CWE:119
XREF	CWE:189
XREF	CWE:399

Plugin Information

Published: 2007/04/02, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
  Version source     : http://testphp.vulnweb.com/secured/phpinfo.php
  Installed version  : 5.1.6
```

```
    Fixed version      : 5.2.1
```

41014 - PHP < 5.2.11 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is affected by multiple flaws.

Description

According to its banner, the version of PHP installed on the remote host is older than 5.2.11. Such versions may be affected by several security issues :

- An unspecified error occurs in certificate validation inside 'php_openssl_apply_verification_policy'.

- An unspecified input validation vulnerability affects the color index in 'imagecolortransparent()'.

- An unspecified input validation vulnerability affects exif processing.

- Calling 'popen()' with an invalid mode can cause a crash under Windows. (Bug #44683)

- An integer overflow in 'xml_utf8_decode()' can make it easier to bypass cross-site scripting and SQL injection protection mechanisms using a specially crafted string with a long UTF-8 encoding. (Bug #49687)

- 'proc_open()' can bypass 'safe_mode_protected_env_vars'.
(Bug #49026)

See Also

http://www.php.net/ChangeLog-5.php#5.2.11

http://www.php.net/releases/5_2_11.php

http://news.php.net/php.internals/45597

http://www.php.net/ChangeLog-5.php#5.2.11

Solution

Upgrade to PHP version 5.2.11 or later.

Risk Factor

High

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	36449
BID	44889
CVE	CVE-2009-3291
CVE	CVE-2009-3292
CVE	CVE-2009-3293
CVE	CVE-2009-3294
CVE	CVE-2009-4018
CVE	CVE-2009-5016
XREF	SECUNIA:36791
XREF	CWE:20
XREF	CWE:134
XREF	CWE:264

Plugin Information

Published: 2009/09/18, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Version source     : http://testphp.vulnweb.com/secured/phpinfo.php
Installed version  : 5.1.6
Fixed version      : 5.2.11
```

25368 - PHP < 5.2.3 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is affected by multiple flaws.

Description

According to its banner, the version of PHP installed on the remote host is older than 5.2.3. It is, therefore, affected by multiple vulnerabilities:

- A buffer overflow in the sqlite_decode_function() in the bundled sqlite library could allow context-dependent attackers to execute arbitrary code. (CVE-2007-1887)

- A CRLF injection vulnerability in the FILTER_VALIDATE_EMAIL filter could allow an attacker to inject arbitrary email headers via a special email address. This only affects Mandriva Linux 2007.1.

(CVE-2007-1900)

- An infinite-loop flaw was discovered in the PHP gd extension. A script that could be forced to process PNG images from an untrusted source could allow a remote attacker to cause a denial of service. (CVE-2007-2756)

- An integer overflow flaw was found in the chunk_split() function that ould possibly execute arbitrary code as the apache user if a remote attacker was able to pass arbitrary data to the third argument of chunk_split() (CVE-2007-2872).

- An open_basedir and safe_mode restriction bypass which could allow context-dependent attackers to determine the existence of arbitrary files. (CVE-2007-3007)

See Also

http://www.php.net/releases/5_2_3.php

Solution

Upgrade to PHP version 5.2.3 or later.

Risk Factor

High

CVSS v3.0 Base Score

7.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L)

CVSS v3.0 Temporal Score

6.6 (CVSS:3.0/E:P/RL:O/RC:C)

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	23235
BID	23359
BID	24089
BID	24259
BID	24261
CVE	CVE-2007-1887
CVE	CVE-2007-1900
CVE	CVE-2007-2756
CVE	CVE-2007-2872
CVE	CVE-2007-3007
XREF	CWE:189
XREF	CWE:264

Plugin Information

Published: 2007/06/02, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Version source     : http://testphp.vulnweb.com/secured/phpinfo.php
Installed version  : 5.1.6
Fixed version      : 5.2.3
```

32123 - PHP < 5.2.6 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is affected by multiple flaws.

Description

According to its banner, the version of PHP installed on the remote host is older than 5.2.6. Such versions may be affected by the following issues :

- A stack-based buffer overflow in FastCGI SAPI.

- An integer overflow in printf().

- An security issue arising from improper calculation of the length of PATH_TRANSLATED in cgi_main.c.

- A safe_mode bypass in cURL.

- Incomplete handling of multibyte chars inside escapeshellcmd().

- Issues in the bundled PCRE fixed by version 7.6.

See Also

https://seclists.org/bugtraq/2008/Mar/285

https://seclists.org/fulldisclosure/2008/May/102

https://seclists.org/fulldisclosure/2008/May/106

http://www.php.net/releases/5_2_6.php

Solution

Upgrade to PHP version 5.2.6 or later.

Risk Factor

High

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	27413

BID	28392
BID	29009
CVE	CVE-2007-4850
CVE	CVE-2007-6039
CVE	CVE-2008-0599
CVE	CVE-2008-1384
CVE	CVE-2008-2050
CVE	CVE-2008-2051
XREF	SECUNIA:30048
XREF	CWE:20
XREF	CWE:119
XREF	CWE:264

Plugin Information

Published: 2008/05/02, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Version source     : http://testphp.vulnweb.com/secured/phpinfo.php
Installed version  : 5.1.6
Fixed version      : 5.2.6
```

35067 - PHP < 5.2.8 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that may be affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP installed on the remote host is earlier than 5.2.8. As such, it is potentially affected by the following vulnerabilities :

- PHP fails to properly sanitize error messages of arbitrary HTML or script code, would code allow for cross-site scripting attacks if PHP's 'display_errors' setting is enabled. (CVE-2008-5814)

- Version 5.2.7 introduced a regression with regard to 'magic_quotes' functionality due to an incorrect fix to the filter extension. As a result, the 'magic_quotes_gpc' setting remains off even if it is set to on. (CVE-2008-5844)

See Also

https://bugs.php.net/bug.php?id=42718

http://www.php.net/releases/5_2_8.php

Solution

Upgrade to PHP version 5.2.8 or later.

Risk Factor

High

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

References

BID	32673
CVE	CVE-2008-5814
CVE	CVE-2008-5844
XREF	CWE:16
XREF	CWE:79

Plugin Information

Published: 2008/12/09, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Version source     : http://testphp.vulnweb.com/secured/phpinfo.php
Installed version  : 5.1.6
Fixed version      : 5.2.8
```

58988 - PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution

Synopsis

The remote web server uses a version of PHP that is affected by a remote code execution vulnerability.

Description

According to its banner, the version of PHP installed on the remote host is earlier than 5.3.12 / 5.4.2, and as such is potentially affected by a remote code execution and information disclosure vulnerability.

An error in the file 'sapi/cgi/cgi_main.c' can allow a remote attacker to obtain PHP source code from the web server or to potentially execute arbitrary code. In vulnerable configurations, PHP treats certain query string parameters as command line arguments including switches such as '-s', '-d', and '-c'.

Note that this vulnerability is exploitable only when PHP is used in CGI-based configurations. Apache with 'mod_php' is not an exploitable configuration.

See Also

http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/

https://bugs.php.net/bug.php?id=61910

http://www.php.net/archive/2012.php#id2012-05-03-1

http://www.php.net/ChangeLog-5.php#5.3.12

http://www.php.net/ChangeLog-5.php#5.4.2

Solution

Upgrade to PHP version 5.3.12 / 5.4.2 or later. A 'mod_rewrite'

workaround is available as well.

Risk Factor

High

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

6.5 (CVSS2#E:H/RL:OF/RC:C)

References

BID	53388
CVE	CVE-2012-1823
XREF	CERT:520827

XREF CISA-KNOWN-EXPLOITED:2022/04/15

Exploitable With

CANVAS (true) Core Impact (true) Metasploit (true)

Plugin Information

Published: 2012/05/04, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Version source     : http://testphp.vulnweb.com/secured/phpinfo.php
Installed version  : 5.1.6
Fixed version      : 5.3.12 / 5.4.2
```

57537 - PHP < 5.3.9 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is affected by multiple flaws.

Description

According to its banner, the version of PHP installed on the remote host is older than 5.3.9. As such, it may be affected by the following security issues :

- The 'is_a()' function in PHP 5.3.7 and 5.3.8 triggers a call to '__autoload()'. (CVE-2011-3379)

- It is possible to create a denial of service condition by sending multiple, specially crafted requests containing parameter values that cause hash collisions when computing the hash values for storage in a hash table. (CVE-2011-4885)

- An integer overflow exists in the exif_process_IFD_TAG function in exif.c that can allow a remote attacker to read arbitrary memory locations or cause a denial of service condition. This vulnerability only affects PHP 5.4.0beta2 on 32-bit platforms. (CVE-2011-4566)

- Calls to libxslt are not restricted via xsltSetSecurityPrefs(), which could allow an attacker to create or overwrite files, resulting in arbitrary code execution. (CVE-2012-0057)

- An error exists in the function 'tidy_diagnose' that can allow an attacker to cause the application to dereference a NULL pointer. This causes the application to crash. (CVE-2012-0781)

- The 'PDORow' implementation contains an error that can cause application crashes when interacting with the session feature. (CVE-2012-0788)

- An error exists in the timezone handling such that repeated calls to the function 'strtotime' can allow a denial of service attack via memory consumption.

(CVE-2012-0789)

See Also

https://www.tenable.com/security/research/tra-2012-01

http://xhe.myxwiki.org/xwiki/bin/view/XSLT/Application_PHP5

http://www.php.net/archive/2012.php#id2012-01-11-1

https://seclists.org/bugtraq/2012/Jan/91

https://bugs.php.net/bug.php?id=55475

https://bugs.php.net/bug.php?id=55776

https://bugs.php.net/bug.php?id=53502

http://www.php.net/ChangeLog-5.php#5.3.9

Solution

Upgrade to PHP version 5.3.9 or later.

Risk Factor

High

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

6.5 (CVSS2#E:H/RL:OF/RC:C)

References

BID	49754
BID	50907
BID	51193
BID	51806
BID	51952
BID	51992
BID	52043
CVE	CVE-2011-3379
CVE	CVE-2011-4566
CVE	CVE-2011-4885
CVE	CVE-2012-0057
CVE	CVE-2012-0781
CVE	CVE-2012-0788
CVE	CVE-2012-0789
XREF	TRA:TRA-2012-01

Exploitable With

Core Impact (true)

Plugin Information

Published: 2012/01/13, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Version source     : http://testphp.vulnweb.com/secured/phpinfo.php
Installed version  : 5.1.6
Fixed version      : 5.3.9
```

142591 - PHP < 7.3.24 Multiple Vulnerabilities

Synopsis

The version of PHP running on the remote web server is affected by multiple vulnerabilities.

Description

According to its self-reported version number, the version of PHP running on the remote web server is prior to 7.3.24. It is, therefore affected by multiple vulnerabilities

See Also

https://www.php.net/ChangeLog-7.php#7.3.24

Solution

Upgrade to PHP version 7.3.24 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

STIG Severity

I

References

XREF	IAVA:2020-A-0510-S

Plugin Information

Published: 2020/11/06, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
  URL               : http://testphp.vulnweb.com/ (5.1.6 under http://testphp.vulnweb.com/secured/
phpinfo.php)
  Installed version : 5.1.6
  Fixed version     : 7.3.24
```

40984 - Browsable Web Directories

Synopsis

Some directories on the remote web server are browsable.

Description

Multiple Nessus plugins identified directories on the web server that are browsable.

See Also

http://www.nessus.org/u?0a35179e

Solution

Make sure that browsable directories do not leak confidential information or give access to sensitive resources. Additionally, use access restrictions or disable directory indexing for any that do.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

Plugin Information

Published: 2009/09/15, Modified: 2021/01/19

Plugin Output

tcp/80/www

```
The following directories are browsable :

http://testphp.vulnweb.com/CVS/
http://testphp.vulnweb.com/Templates/
http://testphp.vulnweb.com/admin/
http://testphp.vulnweb.com/images/
```

44136 - CGI Generic Cookie Injection Scripting

Synopsis

The remote web server is prone to cookie injection attacks.

Description

The remote web server hosts at least one CGI script that fails to adequately sanitize request strings with malicious JavaScript.

By leveraging this issue, an attacker may be able to inject arbitrary cookies. Depending on the structure of the web application, it may be possible to launch a 'session fixation' attack using this mechanism.

Please note that :

- Nessus did not check if the session fixation attack is feasible.

- This is not the only vector of session fixation.

See Also

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

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

http://www.acros.si/papers/session_fixation.pdf

http://projects.webappsec.org/w/page/13246960/Session%20Fixation

Solution

Restrict access to the vulnerable application. Contact the vendor for a patch or upgrade.

Risk Factor

Medium

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

References

XREF	CWE:472
XREF	CWE:642
XREF	CWE:715
XREF	CWE:722

Plugin Information

Published: 2010/01/25, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Using the GET HTTP method, Nessus found that :

+ The following resources may be vulnerable to cookie manipulation :

+ The 'cat' parameter of the /listproducts.php CGI :

/listproducts.php?cat=<script>document.cookie="testsocd=9059;"</script>

-------- output --------
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
Error: You have an error in your SQL syntax; check the manual that corre
sponds to your MySQL server version for the right syntax to use near '=<
script>document.cookie="testsocd=9059;"</script>' at line 1
Warning: mysql_fetch_array() expects parameter 1 to be resource, b [...]
</div>
------------------------

+ The 'pp' parameter of the /hpp/ CGI :

/hpp/?pp=<script>document.cookie="testsocd=9059;"</script>

-------- output --------

<a href="?pp=12">check</a><br/>
<a href="params.php?p=valid&pp=%3Cscript%3Edocument.cookie%3D%22testsocd
%3D9059%3B%22%3C%2Fscript%3E">link1</a><br/><a href="params.php?p=valid&
pp=<script>document.cookie="testsocd=9059;"</script>">link2</a><br/><for
m action="params.php?p=valid&pp=<script>document.cookie="testsocd=9059;"
</script>"><input type=submit name=aaaa/></form><br/>
<hr>
<a href='http://blog.mindedsecurity.com/2009/05/client-side-http-p [...]
------------------------
```

49067 - CGI Generic HTML Injections (quick test)

Synopsis

The remote web server may be prone to HTML injections.

Description

The remote web server hosts CGI scripts that fail to adequately sanitize request strings with malicious JavaScript. By leveraging this issue, an attacker may be able to cause arbitrary HTML to be executed in a user's browser within the security context of the affected site.

The remote web server may be vulnerable to IFRAME injections or cross-site scripting attacks :

- IFRAME injections allow 'virtual defacement' that might scare or anger gullible users. Such injections are sometimes implemented for 'phishing' attacks.

- XSS are extensively tested by four other scripts.

- Some applications (e.g. web forums) authorize a subset of HTML without any ill effect. In this case, ignore this warning.

See Also

http://www.nessus.org/u?602759bc

Solution

Either restrict access to the vulnerable application or contact the vendor for an update.

Risk Factor

Medium

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

References

XREF	CWE:80
XREF	CWE:86

Plugin Information

Published: 2010/09/01, Modified: 2021/01/19

Plugin Output

tcp/80/www

```
Using the GET HTTP method, Nessus found that :

+ The following resources may be vulnerable to HTML injection :

+ The 'cat' parameter of the /listproducts.php CGI :

/listproducts.php?cat=<"mqnlkw%0A>

-------- output --------
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
Error: You have an error in your SQL syntax; check the manual that corre
sponds to your MySQL server version for the right syntax to use near '=<
"mqnlkw
>' at line 1
Warning: mysql_fetch_array() expects parameter 1 to be resource, b [...]
------------------------

+ The 'pp' parameter of the /hpp/ CGI :

/hpp/?pp=<"mqnlkw%0A>

-------- output --------

<a href="?pp=12">check</a><br/>
<a href="params.php?p=valid&pp=%3C%22mqnlkw%0A%3E">link1</a><br/><a href
="params.php?p=valid&pp=<"mqnlkw
>">link2</a><br/><form action="params.php?p=valid&pp=<"mqnlkw
>"><input type=submit name=aaaa/></form><br/>
------------------------

Clicking directly on these URLs should exhibit the issue :
(you will probably need to read the HTML source)

http://testphp.vulnweb.com/listproducts.php?cat=<"mqnlkw%0A>
http://testphp.vulnweb.com/hpp/?pp=<"mqnlkw%0A>
```

39466 - CGI Generic XSS (quick test)

Synopsis

The remote web server is prone to cross-site scripting attacks.

Description

The remote web server hosts CGI scripts that fail to adequately sanitize request strings with malicious JavaScript. By leveraging this issue, an attacker may be able to cause arbitrary HTML and script code to be executed in a user's browser within the security context of the affected site.

These XSS are likely to be 'non persistent' or 'reflected'.

See Also

https://en.wikipedia.org/wiki/Cross_site_scripting#Non-persistent

http://www.nessus.org/u?ea9a0369

http://projects.webappsec.org/w/page/13246920/Cross%20Site%20Scripting

Solution

Restrict access to the vulnerable application. Contact the vendor for a patch or upgrade to address any cross-site scripting vulnerabilities.

Risk Factor

Medium

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

References

XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:80
XREF	CWE:81
XREF	CWE:83
XREF	CWE:86
XREF	CWE:116
XREF	CWE:442
XREF	CWE:692
XREF	CWE:712
XREF	CWE:722

XREF	CWE:725
XREF	CWE:751
XREF	CWE:801
XREF	CWE:811
XREF	CWE:928
XREF	CWE:931

Plugin Information

Published: 2009/06/19, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Using the GET HTTP method, Nessus found that :

+ The following resources may be vulnerable to cross-site scripting (quick test) :

+ The 'cat' parameter of the /listproducts.php CGI :

/listproducts.php?cat=<IMG%20SRC="javascript:alert(104);">

-------- output --------
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
Error: You have an error in your SQL syntax; check the manual that corre
sponds to your MySQL server version for the right syntax to use near '=<
IMG SRC="javascript:alert(104);">' at line 1
Warning: mysql_fetch_array() expects parameter 1 to be resource, b [...]
</div>
------------------------

+ The 'pp' parameter of the /hpp/ CGI :

/hpp/?pp=<IMG%20SRC="javascript:alert(104);">

-------- output --------

<a href="?pp=12">check</a><br/>
<a href="params.php?p=valid&pp=%3CIMG+SRC%3D%22javascript%3Aalert%28104%
29%3B%22%3E">link1</a><br/><a href="params.php?p=valid&pp=<IMG SRC="java
script:alert(104);">">link2</a><br/><form action="params.php?p=valid&pp=
<IMG SRC="javascript:alert(104);">"><input type=submit name=aaaa/></form
><br/>
<hr>
<a href='http://blog.mindedsecurity.com/2009/05/client-side-http-p [...]
------------------------

Clicking directly on these URLs should exhibit the issue :
(you will probably need to read the HTML source)

http://testphp.vulnweb.com/hpp/?pp=<IMG%20SRC="javascript:alert(104);">
```

39480 - PHP < 5.2.10 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP installed on the remote host is older than 5.2.10. Such versions are reportedly affected by multiple vulnerabilities :

- Sufficient checks are not performed on fields reserved for offsets in function 'exif_read_data()'. Successful exploitation of this issue could result in a denial of service condition. (bug 48378)

- Provided 'safe_mode_exec_dir' is not set (not set by default), it may be possible to bypass 'safe_mode' restrictions by preceding a backslash in functions such as 'exec()', 'system()', 'shell_exec()', 'passthru()' and 'popen()' on a system running PHP on Windows. (bug 45997)

See Also

https://bugs.php.net/bug.php?id=45997

https://bugs.php.net/bug.php?id=48378

http://www.php.net/releases/5_2_10.php

http://www.php.net/ChangeLog-5.php#5.2.10

Solution

Upgrade to PHP version 5.2.10 or later.

Risk Factor

Medium

CVSS v2.0 Base Score

5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

3.8 (CVSS2#E:U/RL:OF/RC:C)

References

BID	35435
BID	35440
CVE	CVE-2009-2687
XREF	SECUNIA:35441
XREF	CWE:20

Plugin Information

Published: 2009/06/22, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Version source     : http://testphp.vulnweb.com/secured/phpinfo.php
Installed version  : 5.1.6
Fixed version      : 5.2.10
```

43351 - PHP < 5.2.12 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is affected by multiple flaws.

Description

According to its banner, the version of PHP installed on the remote host is older than 5.2.12. Such versions may be affected by several security issues :

- It is possible to bypass the 'safe_mode' configuration setting using 'tempnam()'. (CVE-2009-3557)

- It is possible to bypass the 'open_basedir' configuration setting using 'posix_mkfifo()'. (CVE-2009-3558)

- Provided file uploading is enabled (it is by default), an attacker can upload files using a POST request with 'multipart/form-data' content even if the target script doesn't actually support file uploads per se. By supplying a large number (15,000+) of files, an attacker could cause the web server to stop responding while it processes the file list. (CVE-2009-4017)

- Missing protection for '$_SESSION' from interrupt corruption and improved 'session.save_path' check. (CVE-2009-4143)

- Insufficient input string validation in the 'htmlspecialchars()' function. (CVE-2009-4142)

See Also

http://www.nessus.org/u?57f2d08f

http://www.php.net/releases/5_2_12.php

http://www.php.net/ChangeLog-5.php#5.2.12

Solution

Upgrade to PHP version 5.2.12 or later.

Risk Factor

Medium

CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.3 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	37389

BID	37390
CVE	CVE-2009-3557
CVE	CVE-2009-3558
CVE	CVE-2009-4017
CVE	CVE-2009-4142
CVE	CVE-2009-4143
XREF	SECUNIA:37821
XREF	CWE:79
XREF	CWE:264

Plugin Information

Published: 2009/12/18, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Version source     : http://testphp.vulnweb.com/secured/phpinfo.php
Installed version  : 5.1.6
Fixed version      : 5.2.12
```

25971 - PHP < 5.2.4 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is affected by multiple flaws.

Description

According to its banner, the version of PHP installed on the remote host is older than 5.2.4. Such versions may be affected by various issues, including but not limited to several overflows.

See Also

http://www.php.net/releases/5_2_4.php

Solution

Upgrade to PHP version 5.2.4 or later.

Risk Factor

Medium

CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.3 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	24261
BID	24661
BID	24922
BID	25498
CVE	CVE-2007-1413
CVE	CVE-2007-2872
CVE	CVE-2007-3294
CVE	CVE-2007-3378
CVE	CVE-2007-3790
CVE	CVE-2007-3799
CVE	CVE-2007-3806
CVE	CVE-2007-4010
CVE	CVE-2007-4033

CVE	CVE-2007-4255
CVE	CVE-2007-4507
CVE	CVE-2007-4652
CVE	CVE-2007-4658
CVE	CVE-2007-4659
CVE	CVE-2007-4660
CVE	CVE-2007-4661
CVE	CVE-2007-4662
CVE	CVE-2007-4663
XREF	CWE:20
XREF	CWE:22
XREF	CWE:119
XREF	CWE:189
XREF	CWE:362
XREF	CWE:399

Plugin Information

Published: 2007/09/03, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Version source     : http://testphp.vulnweb.com/secured/phpinfo.php
Installed version  : 5.1.6
Fixed version      : 5.2.4
```

28181 - PHP < 5.2.5 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is affected by multiple flaws.

Description

According to its banner, the version of PHP installed on the remote host is older than 5.2.5. Such versions may be affected by various issues, including but not limited to several buffer overflows.

See Also

http://www.php.net/releases/5_2_5.php

Solution

Upgrade to PHP version 5.2.5 or later.

Risk Factor

Medium

CVSS v2.0 Base Score

4.4 (CVSS2#AV:L/AC:M/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

3.4 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	26403
BID	69246
CVE	CVE-2007-3996
CVE	CVE-2007-4782
CVE	CVE-2007-4783
CVE	CVE-2007-4784
CVE	CVE-2007-4825
CVE	CVE-2007-4840
CVE	CVE-2007-4887
CVE	CVE-2007-4889
CVE	CVE-2007-5447
CVE	CVE-2007-5653
CVE	CVE-2007-5898

CVE	CVE-2007-5899
CVE	CVE-2007-5900
CVE	CVE-2008-2107
CVE	CVE-2008-2108
CVE	CVE-2008-4107
XREF	CWE:20
XREF	CWE:22
XREF	CWE:78
XREF	CWE:94
XREF	CWE:189
XREF	CWE:200
XREF	CWE:264

Plugin Information

Published: 2007/11/12, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Version source     : http://testphp.vulnweb.com/secured/phpinfo.php
Installed version  : 5.1.6
Fixed version      : 5.2.5
```

35750 - PHP < 5.2.9 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is affected by multiple flaws.

Description

According to its banner, the version of PHP installed on the remote host is older than 5.2.9. Such versions may be affected by several security issues :

- Background color is not correctly validated with a non true color image in function 'imagerotate()'. (CVE-2008-5498)

- A denial of service condition can be triggered by trying to extract zip files that contain files with relative paths in file or directory names.

- Function 'explode()' is affected by an unspecified vulnerability.

- It may be possible to trigger a segfault by passing a specially crafted string to function 'json_decode()'.

- Function 'xml_error_string()' is affected by a flaw which results in messages being off by one.

See Also

http://news.php.net/php.internals/42762

http://www.php.net/releases/5_2_9.php

http://www.php.net/ChangeLog-5.php#5.2.9

Solution

Upgrade to PHP version 5.2.9 or later.

Risk Factor

Medium

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

3.9 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	33002
BID	33927

CVE	CVE-2008-5498
CVE	CVE-2009-1271
CVE	CVE-2009-1272
XREF	SECUNIA:34081
XREF	CWE:20
XREF	CWE:200

Plugin Information

Published: 2009/02/27, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Version source     : http://testphp.vulnweb.com/secured/phpinfo.php
Installed version  : 5.1.6
Fixed version      : 5.2.9
```

58966 - PHP < 5.3.11 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is affected by multiple vulnerabilities.

Description

According to its banner, the version of PHP installed on the remote host is earlier than 5.3.11, and as such is potentially affected by multiple vulnerabilities :

- During the import of environment variables, temporary changes to the 'magic_quotes_gpc' directive are not handled properly. This can lower the difficulty for SQL injection attacks. (CVE-2012-0831)

- The '$_FILES' variable can be corrupted because the names of uploaded files are not properly validated. (CVE-2012-1172)

- The 'open_basedir' directive is not properly handled by the functions 'readline_write_history' and 'readline_read_history'.

- The 'header()' function does not detect multi-line headers with a CR. (Bug #60227 / CVE-2011-1398)

See Also

http://www.nessus.org/u?e81d4026

https://bugs.php.net/bug.php?id=61043

https://bugs.php.net/bug.php?id=54374

https://bugs.php.net/bug.php?id=60227

https://marc.info/?l=oss-security&m=134626481806571&w=2

http://www.php.net/archive/2012.php#id2012-04-26-1

http://www.php.net/ChangeLog-5.php#5.3.11

Solution

Upgrade to PHP version 5.3.11 or later.

Risk Factor

Medium

CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.3 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	51954
BID	53403
BID	55297
CVE	CVE-2011-1398
CVE	CVE-2012-0831
CVE	CVE-2012-1172

Plugin Information

Published: 2012/05/02, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Version source     : http://testphp.vulnweb.com/secured/phpinfo.php
Installed version  : 5.1.6
Fixed version      : 5.3.11
```

44921 - PHP < 5.3.2 / 5.2.13 Multiple Vulnerabilities

Synopsis

The remote web server uses a version of PHP that is affected by multiple flaws.

Description

According to its banner, the version of PHP installed on the remote host is older than 5.3.2 / 5.2.13. Such versions may be affected by several security issues :

- Directory paths not ending with '/' may not be correctly validated inside 'tempnam()' in 'safe_mode' configuration.

- It may be possible to bypass the 'open_basedir'/ 'safe_mode' configuration restrictions due to an error in session extensions.

- An unspecified vulnerability affects the LCG entropy.

See Also

http://securityreason.com/achievement_securityalert/82

http://securityreason.com/securityalert/7008

https://seclists.org/fulldisclosure/2010/Feb/208

http://www.php.net/releases/5_3_2.php

http://www.php.net/ChangeLog-5.php#5.3.2

http://www.php.net/releases/5_2_13.php

http://www.php.net/ChangeLog-5.php#5.2.13

Solution

Upgrade to PHP version 5.3.2 / 5.2.13 or later.

Risk Factor

Medium

CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	38182

BID	38430
BID	38431
CVE	CVE-2010-1128
CVE	CVE-2010-1129
CVE	CVE-2010-1130
XREF	SECUNIA:38708

Plugin Information

Published: 2010/02/26, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Version source     : http://testphp.vulnweb.com/secured/phpinfo.php
Installed version  : 5.1.6
Fixed version      : 5.3.2 / 5.2.13
```

152853 - PHP < 7.3.28 Email Header Injection

Synopsis

The version of PHP running on the remote web server is affected by an email header injection vulnerability.

Description

According to its self-reported version number, the version of PHP running on the remote web server is prior to 7.3.28.

It is, therefore affected by an email header injection vulnerability, due to a failure to properly handle CR-LF sequences in header fields. An unauthenticated, remote attacker can exploit this, by inserting line feed characters into email headers, to gain full control of email header content.

See Also

https://www.php.net/ChangeLog-7.php#7.3.28

Solution

Upgrade to PHP version 7.3.28 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

Plugin Information

Published: 2021/08/26, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
  URL              : http://testphp.vulnweb.com/ (5.1.6 under http://testphp.vulnweb.com/secured/
phpinfo.php)
  Installed version : 5.1.6
  Fixed version     : 7.3.28
```

73289 - PHP PHP_RSHUTDOWN_FUNCTION Security Bypass

Synopsis

The remote web server uses a version of PHP that is potentially affected by a security bypass vulnerability.

Description

According to its banner, the version of PHP 5.x installed on the remote host is 5.x prior to 5.3.11 or 5.4.x prior to 5.4.1 and thus, is potentially affected by a security bypass vulnerability.

An error exists related to the function 'PHP_RSHUTDOWN_FUNCTION' in the libxml extension and the 'stream_close' method that could allow a remote attacker to bypass 'open_basedir' protections and obtain sensitive information.

Note that this plugin has not attempted to exploit this issue, but has instead relied only on PHP's self-reported version number.

See Also

http://www.nessus.org/u?bcc428c2

https://bugs.php.net/bug.php?id=61367

Solution

Upgrade to PHP version 5.3.11 / 5.4.1 or later.

Risk Factor

Medium

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

BID	65673
CVE	CVE-2012-1171

Plugin Information

Published: 2014/04/01, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Version source    : http://testphp.vulnweb.com/secured/phpinfo.php
Installed version : 5.1.6
Fixed version     : 5.3.11 / 5.4.1
```

85582 - Web Application Potentially Vulnerable to Clickjacking

Synopsis

The remote web server may fail to mitigate a class of web application vulnerabilities.

Description

The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy 'frame-ancestors' response header in all content responses. This could potentially expose the site to a clickjacking or UI redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions.

X-Frame-Options has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors.

Content-Security-Policy (CSP) has been proposed by the W3C Web Application Security Working Group, with increasing support among all major browser vendors, as a way to mitigate clickjacking and other attacks. The 'frame-ancestors' policy directive restricts which sources can embed the protected resource.

Note that while the X-Frame-Options and Content-Security-Policy response headers are not the only mitigations for clickjacking, they are currently the most reliable methods that can be detected through automation. Therefore, this plugin may produce false positives if other mitigation strategies (e.g., frame-busting JavaScript) are deployed or if the page does not perform any security-sensitive transactions.

See Also

http://www.nessus.org/u?399b1f56

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

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

Solution

Return the X-Frame-Options or Content-Security-Policy (with the 'frame-ancestors' directive) HTTP header with the page's response.

This prevents the page's content from being rendered by another site when using the frame or iframe HTML tags.

Risk Factor

Medium

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

References

XREF	CWE:693

Plugin Information

Published: 2015/08/22, Modified: 2017/05/16

Plugin Output

tcp/80/www

```
The following pages do not use a clickjacking mitigation response header and contain a clickable
 event :

  - http://testphp.vulnweb.com/
  - http://testphp.vulnweb.com/AJAX/
  - http://testphp.vulnweb.com/AJAX/index.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/.php/.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/.php/.php/.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/.php/.php/showxml.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/.php/showxml.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/.php/showxml.php/.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/.php/showxml.php/showxml.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/showxml.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/showxml.php/.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/showxml.php/.php/.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/showxml.php/.php/showxml.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/showxml.php/showxml.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/showxml.php/showxml.php/.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/showxml.php/showxml.php/showxml.php
  - http://testphp.vulnweb.com/AJAX/index.php/showxml.php
  - http://testphp.vulnweb.com/AJAX/index.php/showxml.php/.php
  - http://testphp.vulnweb.com/AJAX/index.php/showxml.php/.php/.php
  - http://testphp.vulnweb.com/AJAX/index.php/showxml.php/.php/.php/.php
  - http://testphp.vulnweb.com/AJAX/index.php/showxml.php/.php/.php/showxml.php
  - http://testphp.vulnweb.com/AJAX/index.php/showxml.php/.php/showxml.php
  - http://testphp.vulnweb.com/AJAX/index.php/showxml.php/.php/showxml.php/.php
  - http://testphp.vulnweb.com/AJAX/index.php/showxml.php/.php/showxml.php/showxml.php
  - http://testphp.vulnweb.com/AJAX/index.php/showxml.php/showxml.php
  - http://testphp.vulnweb.com/AJAX/index.php/showxml.php/showxml.php/.php
  - http://testphp.vulnweb.com/AJAX/index.ph [...]
```

44670 - Web Application SQL Backend Identification

Synopsis

A web application's SQL backend can be identified.

Description

At least one web application hosted on the remote web server is built on a SQL backend that Nessus was able to identify by looking at error messages.

Leaking this kind of information may help an attacker fine-tune attacks against the application and its backend.

See Also

http://projects.webappsec.org/w/page/13246925/Fingerprinting

Solution

Filter out error messages.

Risk Factor

Medium

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

Plugin Information

Published: 2010/02/19, Modified: 2021/01/19

Plugin Output

tcp/80/www

```
The web application appears to be based on MySQL

This information was leaked by these URLs :
http://testphp.vulnweb.com/
```

11229 - Web Server info.php / phpinfo.php Detection

Synopsis

The remote web server contains a PHP script that is prone to an information disclosure attack.

Description

Many PHP installation tutorials instruct the user to create a PHP file that calls the PHP function 'phpinfo()' for debugging purposes. Various PHP applications may also include such a file. By accessing such a file, a remote attacker can discover a large amount of information about the remote web server, including :

- The username of the user who installed PHP and if they are a SUDO user.

- The IP address of the host.

- The version of the operating system.

- The web server version.

- The root directory of the web server.

- Configuration information about the remote PHP installation.

Solution

Remove the affected file(s).

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

Plugin Information

Published: 2003/02/12, Modified: 2022/06/01

Plugin Output

tcp/80/www

```
Nessus discovered the following URL that calls phpinfo() :
```

```
- http://testphp.vulnweb.com/secured/phpinfo.php
```

42057 - Web Server Allows Password Auto-Completion

Synopsis

The 'autocomplete' attribute is not disabled on password fields.

Description

The remote web server contains at least one HTML form field that has an input of type 'password' where 'autocomplete' is not set to 'off'.

While this does not represent a risk to this web server per se, it does mean that users who use the affected forms may have their credentials saved in their browsers, which could in turn lead to a loss of confidentiality if any of them use a shared host or if their machine is compromised at some point.

Solution

Add the attribute 'autocomplete=off' to these fields to prevent browsers from caching credentials.

Risk Factor

Low

Plugin Information

Published: 2009/10/07, Modified: 2021/11/30

Plugin Output

tcp/80/www

```
Page : /login.php
Destination Page: /userinfo.php

Page : /signup.php
Destination Page: /secured/newuser.php
```

26194 - Web Server Transmits Cleartext Credentials

Synopsis

The remote web server might transmit credentials in cleartext.

Description

The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext.

An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users.

Solution

Make sure that every sensitive form transmits content over HTTPS.

Risk Factor

Low

CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

References

XREF	CWE:522
XREF	CWE:523
XREF	CWE:718
XREF	CWE:724
XREF	CWE:928
XREF	CWE:930

Plugin Information

Published: 2007/09/28, Modified: 2016/11/29

Plugin Output

tcp/80/www

```
Page : /login.php
Destination Page: /userinfo.php

Page : /signup.php
Destination Page: /secured/newuser.php
```

47830 - CGI Generic Injectable Parameter

Synopsis

Some CGIs are candidate for extended injection tests.

Description

Nessus was able to to inject innocuous strings into CGI parameters and read them back in the HTTP response.

The affected parameters are candidates for extended injection tests like cross-site scripting attacks.

This is not a weakness per se, the main purpose of this test is to speed up other scripts. The results may be useful for a human pen-tester.

Solution

n/a

Risk Factor

None

References

XREF CWE:86

Plugin Information

Published: 2010/07/26, Modified: 2021/01/19

Plugin Output

tcp/80/www

```
Using the GET HTTP method, Nessus found that :

+ The following resources may be vulnerable to injectable parameter :

+ The 'cat' parameter of the /listproducts.php CGI :

/listproducts.php?cat=jolpjz

-------- output --------
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
Error: Unknown column 'jolpjz' in 'where clause'
Warning: mysql_fetch_array() expects parameter 1 to be resource, b [...]
</div>
------------------------

+ The 'pp' parameter of the /hpp/ CGI :
```

```
/hpp/?pp=%00jolpjz

-------- output --------

<a href="?pp=12">check</a><br/>
<a href="params.php?p=valid&pp=%00jolpjz">link1</a><br/><a href="params.
php?p=valid&pp=.jolpjz">link2</a><br/><form action="params.php?p=valid&p
p=.jolpjz"><input type=submit name=aaaa/></form><br/>
<hr>
<a href='http://blog.mindedsecurity.com/2009/05/client-side-http-p [...]
------------------------

Clicking directly on these URLs should exhibit the issue :
(you will probably need to read the HTML source)

http://testphp.vulnweb.com/listproducts.php?cat=jolpjz
http://testphp.vulnweb.com/hpp/?pp=%00jolpjz
```

33817 - CGI Generic Tests Load Estimation (all tests)

Synopsis

Load estimation for web application tests.

Description

This script computes the maximum number of requests that would be done by the generic web tests, depending on miscellaneous options. It does not perform any test by itself.

The results can be used to estimate the duration of these tests, or the complexity of additional manual tests.

Note that the script does not try to compute this duration based on external factors such as the network and web servers loads.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/10/26, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Here are the estimated number of requests in miscellaneous modes
for one method only (GET or POST) :
[Single / Some Pairs / All Pairs / Some Combinations / All Combinations]

on site request forgery                  : S=2          SP=2         AP=2         SC=2         AC=2

SQL injection                            : S=1272       SP=1272      AP=2952      SC=864
 AC=31920
unseen parameters                        : S=1855       SP=1855      AP=4305      SC=1260
 AC=46550
local file inclusion                     : S=53         SP=53        AP=123       SC=36
 AC=1330
cookie manipulation                      : S=4          SP=4         AP=4         SC=4         AC=4

web code injection                       : S=53         SP=53        AP=123       SC=36
 AC=1330
XML injection                            : S=53         SP=53        AP=123       SC=36
 AC=1330
format string                            : S=106        SP=106       AP=246       SC=72
 AC=2660
script injection                         : S=2          SP=2         AP=2         SC=2         AC=2
```

```
injectable parameter                     : S=106        SP=106       AP=246       SC=72
 AC=2660
cross-site scripting (comprehensive test): S=212        SP=212       AP=492       SC=144
 AC=5320
cross-site scripting (extended patterns) : S=12         SP=12        AP=12        SC=12        AC=12

directory traversal (write access)       : S=106        SP=106       AP=246       SC=72
 AC=2660
SSI injection                            : S=159        SP=159       AP=369       SC=108
 AC=3990
header injection                         : S=4          SP=4         AP=4         SC=4         AC=4

HTML injection                           : S=10         SP=10        AP=10        SC=10        AC=10

directory traversal                      : S=1325       SP=1325      AP=3075      SC=900
 AC=33250
cross-site scripting (quick test)      [...]
```

39470 - CGI Generic Tests Timeout

Synopsis

Some generic CGI attacks ran out of time.

Description

Some generic CGI tests ran out of time during the scan. The results may be incomplete.

Solution

Consider increasing the 'maximum run time (minutes)' preference for the 'Web Applications Settings' in order to prevent the CGI scanning from timing out. Less ambitious options could also be used, such as :

- Test more that one parameter at a time per form :

'Test all combinations of parameters' is much slower than 'Test random pairs of parameters' or 'Test all pairs of parameters (slow)'.

- 'Stop after one flaw is found per web server (fastest)'

under 'Do not stop after the first flaw is found per web page' is quicker than 'Look for all flaws (slowest)'.

- In the Settings/Advanced menu, try reducing the value for 'Max number of concurrent TCP sessions per host' or 'Max simultaneous checks per host'.

Risk Factor

None

Plugin Information

Published: 2009/06/19, Modified: 2021/01/19

Plugin Output

tcp/80/www

```
The following tests timed out without finding any flaw :
- arbitrary command execution
- blind SQL injection
- XSS (on parameters names)
- SQL injection
- SQL injection (on parameters names)
- unseen parameters
```

49704 - External URLs

Synopsis

Links to external sites were gathered.

Description

Nessus gathered HREF links to external sites by crawling the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/10/04, Modified: 2011/08/19

Plugin Output

tcp/80/www

```
7 external URLs were gathered on this web server :
URL...                                  - Seen on...


http://blog.mindedsecurity.com/2009/05/client-side-http-parameter-pollution.html - /hpp/
http://www.acunetix.com                 - /
http://www.eclectasy.com/Fractal-Explorer/index.html - /
https://www.acunetix.com/               - /
https://www.acunetix.com/blog/articles/prevent-sql-injection-vulnerabilities-in-php-applications/
 - /
https://www.acunetix.com/vulnerability-scanner/ - /
https://www.acunetix.com/vulnerability-scanner/php-security-scanner/ - /
```

43111 - HTTP Methods Allowed (per directory)

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'

in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

See Also

http://www.nessus.org/u?d9c03a9a

http://www.nessus.org/u?b019cbdb

https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/12/10, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Based on tests of each method :

  - HTTP methods ACL BASELINE-CONTROL BCOPY BDELETE BMOVE BPROPFIND
    BPROPPATCH CHECKIN CHECKOUT COPY DEBUG DELETE GET HEAD INDEX
    LABEL LOCK MERGE MKACTIVITY MKCOL MKWORKSPACE MOVE NOTIFY OPTIONS
    ORDERPATCH PATCH POLL POST PROPFIND PROPPATCH PUT REPORT
    RPC_IN_DATA RPC_OUT_DATA SEARCH SUBSCRIBE UNCHECKOUT UNLOCK
    UNSUBSCRIBE UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on :

    /cgi-bin

  - HTTP methods GET HEAD POST are allowed on :

    /
    /AJAX
    /AJAX/index.php
    /AJAX/index.php/.php
    /AJAX/index.php/.php/.php
    /AJAX/index.php/.php/.php/.php
    /AJAX/index.php/.php/.php/showxml.php
    /AJAX/index.php/.php/showxml.php
    /AJAX/index.php/.php/showxml.php/.php
    /AJAX/index.php/.php/showxml.php/showxml.php
    /AJAX/index.php/showxml.php
    /AJAX/index.php/showxml.php/.php
    /AJAX/index.php/showxml.php/.php/.php
    /AJAX/index.php/showxml.php/.php/showxml.php
    /AJAX/index.php/showxml.php/showxml.php
    /AJAX/index.php/showxml.php/showxml.php/.php
    /AJAX/index.php/showxml.php/showxml.php/showxml.php
    /CVS
    /Templates
    /admin
    /images
    /secured

  - Invalid/unknown HTTP methods are allowed on :

    /cgi-bin
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/80/www

```
The remote web server type is :

nginx/1.19.0
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

tcp/80/www

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Server: nginx/1.19.0
  Date: Thu, 12 Jan 2023 11:36:25 GMT
  Content-Type: text/html; charset=UTF-8
  Transfer-Encoding: chunked
  Connection: keep-alive
  X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1

Response Body :

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"
 codeOutsideHTMLIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>Home of Acunetix Art</title>
<!-- InstanceEndEditable -->
```

```
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) {  //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"><img src="images/logo.gif" width="306"
 height="38" border="0" alt="Acunetix website security"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a href="https://www.acunetix.com/vulnerability-
scanner/">Acunetix Web Vulnerability Scanner</a></h6>
  <div id="globalNav">
      <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
<td align="left">
<a href="index.php">home</a> | <a href="categories.php">categories</a> | <a
 href="artists.php">artists
 [...]
```

50344 - Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header

Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description

The remote web server in some responses sets a permissive Content-Security-Policy (CSP) frame-ancestors response header or does not set one at all.

The CSP frame-ancestors header has been proposed by the W3C Web Application Security Working Group as a way to mitigate cross-site scripting and clickjacking attacks.

See Also

http://www.nessus.org/u?55aa8f57

http://www.nessus.org/u?07cc2a06

https://content-security-policy.com/

https://www.w3.org/TR/CSP2/

Solution

Set a non-permissive Content-Security-Policy frame-ancestors header for all requested resources.

Risk Factor

None

Plugin Information

Published: 2010/10/26, Modified: 2021/01/19

Plugin Output

tcp/80/www

```
The following pages do not set a Content-Security-Policy frame-ancestors response header or set a
 permissive policy:

  - http://testphp.vulnweb.com/
  - http://testphp.vulnweb.com/AJAX/
  - http://testphp.vulnweb.com/AJAX/index.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/.php/.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/.php/.php/.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/.php/.php/showxml.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/.php/showxml.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/.php/showxml.php/.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/.php/showxml.php/showxml.php
```

```
  - http://testphp.vulnweb.com/AJAX/index.php/.php/showxml.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/showxml.php/.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/showxml.php/.php/.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/showxml.php/.php/showxml.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/showxml.php/showxml.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/showxml.php/showxml.php/.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/showxml.php/showxml.php/showxml.php
  - http://testphp.vulnweb.com/AJAX/index.php/showxml.php
  - http://testphp.vulnweb.com/AJAX/index.php/showxml.php/.php
  - http://testphp.vulnweb.com/AJAX/index.php/showxml.php/.php/.php
  - http://testphp.vulnweb.com/AJAX/index.php/showxml.php/.php/.php/.php
  - http://testphp.vulnweb.com/AJAX/index.php/showxml.php/.php/.php/showxml.php
  - http://testphp.vulnweb.com/AJAX/index.php/showxml.php/.php/showxml.php
  - http://testphp.vulnweb.com/AJAX/index.php/showxml.php/.php/showxml.php/.php
  - http://testphp.vulnweb.com/AJAX/index.php/showxml.php/.php/showxml.php/showxml.php
  - http://testphp.vulnweb.com/AJAX/index.php/showxml.php/showxml.php
  - http://testphp.vulnweb.com/AJAX/index.php/showxml.php/showxml.php/.php
  - http://testphp.vulnweb.com/A [...]
```

50345 - Missing or Permissive X-Frame-Options HTTP Response Header

Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description

The remote web server in some responses sets a permissive X-Frame-Options response header or does not set one at all.

The X-Frame-Options header has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors

See Also

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

http://www.nessus.org/u?399b1f56

Solution

Set a properly configured X-Frame-Options header for all requested resources.

Risk Factor

None

Plugin Information

Published: 2010/10/26, Modified: 2021/01/19

Plugin Output

tcp/80/www

```
The following pages do not set a X-Frame-Options response header or set a permissive policy:

  - http://testphp.vulnweb.com/
  - http://testphp.vulnweb.com/AJAX/
  - http://testphp.vulnweb.com/AJAX/index.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/.php/.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/.php/.php/.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/.php/.php/showxml.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/.php/showxml.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/.php/showxml.php/.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/.php/showxml.php/showxml.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/showxml.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/showxml.php/.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/showxml.php/.php/.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/showxml.php/.php/showxml.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/showxml.php/showxml.php
```

```
- http://testphp.vulnweb.com/AJAX/index.php/.php/showxml.php/showxml.php/.php
- http://testphp.vulnweb.com/AJAX/index.php/.php/showxml.php/showxml.php/showxml.php
- http://testphp.vulnweb.com/AJAX/index.php/showxml.php
- http://testphp.vulnweb.com/AJAX/index.php/showxml.php/.php
- http://testphp.vulnweb.com/AJAX/index.php/showxml.php/.php/.php
- http://testphp.vulnweb.com/AJAX/index.php/showxml.php/.php/.php/.php
- http://testphp.vulnweb.com/AJAX/index.php/showxml.php/.php/.php/showxml.php
- http://testphp.vulnweb.com/AJAX/index.php/showxml.php/.php/showxml.php
- http://testphp.vulnweb.com/AJAX/index.php/showxml.php/.php/showxml.php/.php
- http://testphp.vulnweb.com/AJAX/index.php/showxml.php/.php/showxml.php/showxml.php
- http://testphp.vulnweb.com/AJAX/index.php/showxml.php/showxml.php
- http://testphp.vulnweb.com/AJAX/index.php/showxml.php/showxml.php/.php
- http://testphp.vulnweb.com/AJAX/index.php/showxml.ph [...]
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2022/11/30

Plugin Output

tcp/80/www

```
Port 80/tcp was found to be open
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2022/06/09

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.4.1
Nessus build : 20091
Plugin feed version : 202301120144
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : debian9-x86-64
Scan type : Normal
Scan name : Noman Ahmed Project 2
```

```
Scan policy used : Web Application Tests
Scanner IP : 10.0.2.15

WARNING : No port scanner was enabled during the scan. This may
lead to incomplete results.

Port range : 1-65535
Ping RTT : 311.423 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : enabled
Web application tests : enabled
Web app tests -  Test mode : single
Web app tests -  Try all HTTP methods : no
Web app tests -  Maximum run time : 5 minutes.
Web app tests -  Stop at first flaw : CGI
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Scan Start Date : 2023/1/12 6:07 EST
Scan duration : 4106 sec
```

48243 - PHP Version Detection

Synopsis

It was possible to obtain the version number of the remote PHP installation.

Description

Nessus was able to determine the version of PHP available on the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0936

Plugin Information

Published: 2010/08/04, Modified: 2022/10/12

Plugin Output

tcp/80/www

```
Nessus was able to identify the following PHP version information :

  Version : 5.1.6
  Source  : http://testphp.vulnweb.com/secured/phpinfo.php

  Version : 5.6.40-38+ubuntu20.04.1+deb.sury.org+1
  Source  : X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
```

66334 - Patch Report

Synopsis

The remote host is missing several patches.

Description

The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.

Note: Because the 'Show missing patches that have been superseded' setting in your scan policy depends on this plugin, it will always run and cannot be disabled.

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information

Published: 2013/07/08, Modified: 2023/01/10

Plugin Output

tcp/0

```
. You need to take the following action :

[ PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution (58988) ]

+ Action to take : Upgrade to PHP version 5.3.12 / 5.4.2 or later.  A 'mod_rewrite' workaround is
 available as well.

+Impact : Taking this action will resolve 110 different vulnerabilities (CVEs).
```

40773 - Web Application Potentially Sensitive CGI Parameter Detection

Synopsis

An application was found that may use CGI parameters to control sensitive information.

Description

According to their names, some CGI parameters may control sensitive data (e.g., ID, privileges, commands, prices, credit card data, etc.). In the course of using an application, these variables may disclose sensitive data or be prone to tampering that could result in privilege escalation. These parameters should be examined to determine what type of data is controlled and if it poses a security risk.

** This plugin only reports information that may be useful for auditors

** or pen-testers, not a real flaw.

Solution

Ensure sensitive data is not disclosed by CGI parameters. In addition, do not use CGI parameters to control access to resources or privileges.

Risk Factor

None

Plugin Information

Published: 2009/08/25, Modified: 2021/01/19

Plugin Output

tcp/80/www

```
Potentially sensitive parameters for CGI /AJAX/index.php/.php/.php :

id : Potential horizontal or vertical privilege escalation

Potentially sensitive parameters for CGI /AJAX/index.php/showxml.php/.php :

id : Potential horizontal or vertical privilege escalation

Potentially sensitive parameters for CGI /AJAX/.php :

id : Potential horizontal or vertical privilege escalation

Potentially sensitive parameters for CGI /AJAX/index.php/.php/.php/.php :

id : Potential horizontal or vertical privilege escalation

Potentially sensitive parameters for CGI /AJAX/index.php/.php/showxml.php/.php/.php :

id : Potential horizontal or vertical privilege escalation

Potentially sensitive parameters for CGI /AJAX/index.php/.php/showxml.php/showxml.php/.php :
```

```
id : Potential horizontal or vertical privilege escalation

Potentially sensitive parameters for CGI /AJAX/index.php/showxml.php/.php/.php/.php :

id : Potential horizontal or vertical privilege escalation

Potentially sensitive parameters for CGI /AJAX/index.php/showxml.php/.php/showxml.php/.php :

id : Potential horizontal or vertical privilege escalation

Potentially sensitive parameters for CGI /AJAX/index.php/showxml.php/showxml.php/.php/.php :

id : Potential horizontal or vertical privilege escalation

Potentially sensitive parameters for CGI /AJAX/index.php/.php/showxml.php/.php/showxml.php/.php :

id : Potential horizontal or vertical privilege escalation

Potentially sensitive parameters for CGI /AJAX/index.php/.php/showxml.php/showxml.php/.php/.php :

id : Potential horizontal or vertical privilege escalation

Potentially sensitive parameters for CGI /AJAX/index.php/.php/showxml.php/showxml.php/
showxml.php/.php :

id : Potential horizontal or vertical privilege escalation

Potentially sensitive parameters for CGI /AJAX/index.php/showxml.php/.php/.php/.php/.php :

id : Potential horizontal or vertical privilege escalation

Potentially sensitive parameters for CGI /AJAX/index.php/showxml.php/.php/.php/showxml.php/.php :

id : Potential horizontal or vertical pr [...]
```

91815 - Web Application Sitemap

Synopsis

The remote web server hosts linkable content that can be crawled by Nessus.

Description

The remote web server contains linkable content that can be used to gather information about a target.

See Also

http://www.nessus.org/u?5496c8d9

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/06/24, Modified: 2016/06/24

Plugin Output

tcp/80/www

```
The following sitemap was created from crawling linkable content on the target host :

  - http://testphp.vulnweb.com/
  - http://testphp.vulnweb.com/AJAX/
  - http://testphp.vulnweb.com/AJAX/index.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/.php/.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/.php/.php/.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/.php/.php/showxml.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/.php/showxml.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/.php/showxml.php/.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/.php/showxml.php/showxml.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/showxml.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/showxml.php/.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/showxml.php/.php/.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/showxml.php/.php/showxml.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/showxml.php/showxml.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/showxml.php/showxml.php/.php
  - http://testphp.vulnweb.com/AJAX/index.php/.php/showxml.php/showxml.php/showxml.php
  - http://testphp.vulnweb.com/AJAX/index.php/showxml.php
  - http://testphp.vulnweb.com/AJAX/index.php/showxml.php/.php
  - http://testphp.vulnweb.com/AJAX/index.php/showxml.php/.php/.php
  - http://testphp.vulnweb.com/AJAX/index.php/showxml.php/.php/.php/.php
```

```
    - http://testphp.vulnweb.com/AJAX/index.php/showxml.php/.php/.php/showxml.php
    - http://testphp.vulnweb.com/AJAX/index.php/showxml.php/.php/showxml.php
    - http://testphp.vulnweb.com/AJAX/index.php/showxml.php/.php/showxml.php/.php
    - http://testphp.vulnweb.com/AJAX/index.php/showxml.php/.php/showxml.php/showxml.php
    - http://testphp.vulnweb.com/AJAX/index.php/showxml.php/showxml.php
    - http://testphp.vulnweb.com/AJAX/index.php/showxml.php/showxml.php/.php
    - http://testphp.vulnweb.com/AJAX/index.php/showxml.php/showx [...]
```

11032 - Web Server Directory Enumeration

Synopsis

It is possible to enumerate directories on the web server.

Description

This plugin attempts to determine the presence of various common directories on the remote web server. By sending a request for a directory, the web server response code indicates if it is a valid directory or not.

See Also

http://projects.webappsec.org/w/page/13246953/Predictable%20Resource%20Location

Solution

n/a

Risk Factor

None

References

XREF	OWASP:OWASP-CM-006

Plugin Information

Published: 2002/06/26, Modified: 2021/08/17

Plugin Output

tcp/80/www

```
The following directories were discovered:
/admin, /cgi-bin, /secured, /CVS, /Templates, /images

While this is not, in and of itself, a bug, you should manually inspect
these directories to ensure that they are in compliance with company
security standards
```

49705 - Web Server Harvested Email Addresses

Synopsis

Email addresses were harvested from the web server.

Description

Nessus harvested HREF mailto: links and extracted email addresses by crawling the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/10/04, Modified: 2018/05/24

Plugin Output

tcp/80/www

```
The following email address has been gathered :

- 'wvs@acunetix.com', referenced from :
   /search.php
   /listproducts.php
   /index.php
   /artists.php
   /categories.php
   /signup.php
   /disclaimer.php
   /
   /Templates/main_dynamic_template.dwt.php
   /cart.php
   /guestbook.php
   /login.php
```

72427 - Web Site Client Access Policy File Detection

Synopsis

The remote web server contains a 'clientaccesspolicy.xml' file.

Description

The remote web server contains a client access policy file. This is a simple XML file used by Microsoft Silverlight to allow access to services that reside outside the exact web domain from which a Silverlight control originated.

See Also

http://www.nessus.org/u?a4eeeaa2

Solution

Review the contents of the policy file carefully. Improper policies, especially an unrestricted one with just '*', could allow for cross- site request forgery or other attacks against the web server.

Risk Factor

None

Plugin Information

Published: 2014/02/11, Modified: 2021/01/19

Plugin Output

tcp/80/www

```
Nessus was able to obtain a client access policy file from the
remote host at the following URL :

  GET /clientaccesspolicy.xml HTTP/1.1
Host: testphp.vulnweb.com
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Keep-Alive
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
```

32318 - Web Site Cross-Domain Policy File Detection

Synopsis

The remote web server contains a 'crossdomain.xml' file.

Description

The remote web server contains a cross-domain policy file. This is a simple XML file used by Adobe's Flash Player to allow access to data that resides outside the exact web domain from which a Flash movie file originated.

See Also

http://www.nessus.org/u?8a58aa76

http://kb2.adobe.com/cps/142/tn_14213.html

http://www.nessus.org/u?74a6a9a5

http://www.nessus.org/u?acb70df2

Solution

Review the contents of the policy file carefully. Improper policies, especially an unrestricted one with just '*', could allow for cross- site request forgery and cross-site scripting attacks against the web server.

Risk Factor

None

Plugin Information

Published: 2008/05/15, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Nessus was able to obtain a cross-domain policy file from the remote
host using the following URL :

  http://testphp.vulnweb.com/crossdomain.xml
```

10662 - Web mirroring

Synopsis

Nessus can crawl the remote website.

Description

This plugin makes a mirror of the remote website(s) and extracts the list of CGIs that are used by the remote host.

It is suggested that you change the number of pages to mirror in the 'Options' section of the client.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/05/04, Modified: 2022/11/30

Plugin Output

tcp/80/www

```
Webmirror performed 174 queries in 156s (1.0115 queries per second)

The following CGIs have been discovered :


+ CGI : /search.php
  Methods : POST
  Argument : goButton
   Value: go
  Argument : searchFor
  Argument : test
   Value: query


+ CGI : /listproducts.php
  Methods : GET
  Argument : cat
   Value: 4


+ CGI : /artists.php
  Methods : GET
  Argument : artist
   Value: 3


+ CGI : /comment.php
```

```
  Methods : GET
  Argument : aid
   Value: 3


+ CGI : /guestbook.php
  Methods : POST
  Argument : name
   Value: anonymous user
  Argument : submit
   Value: add message
  Argument : text


+ CGI : /AJAX/index.php/.php
  Methods : GET
  Argument : id


+ CGI : /userinfo.php
  Methods : POST
  Argument : pass
  Argument : uname


+ CGI : /hpp/
  Methods : GET
  Argument : pp
   Value: 12


+ CGI : /AJAX/index.php/.php/.php
  Methods : GET
  Argument : id


+ CGI : /AJAX/index.php/showxml.php/.php
  Methods : GET
  Argument : id


+ CGI : /AJAX/.php
  Methods : GET
  Argument : id


+ CGI : /secured/newuser.php
  Methods : POST
  Argument : signup
   Value: signup
  Argument : uaddress
  Argument : ucc
  Argument : uemail
  Argument : upass
  Argument : upass2
  Argument : uphone
  Argument : urname
  Argument : uuname


+ CGI : /AJAX/index.php/.php/.php/.php
  Methods : GET
  Argument : id


+ CGI : /AJAX/index.php/.php/showxml.php/.php
  Methods : GET
  Argument : id
```

```
+ CGI : /AJAX/index.php/showxml.php/.php/.php
  Methods : GET
  Argument : id


+ CGI : /AJAX/index.php/showxml.php/showxml.php/.php
  Methods : GET
  Argument : id


+ CGI : /AJAX/index.php/.php/.php/.php/.php
  Methods : GET
  Argument : id


+ CGI : /AJAX/index.php/.php/.php/showxml.php/.php
  Methods : GET
  Argument : id


+ CGI : /AJAX/index.php/.php/showxml.php/.php/.php
  Methods : GET
  Argument : id


+ CGI : /AJAX/index.php/.php/showxml.php/showxml.php/.php
  Methods : GET
  Argument : id


+ CGI : /AJAX/index.php/showxml.php/.php/.php/.php
  Methods : GET
  Argument : id


+ CGI : /AJAX/index.php/showxml.php/.php/showxml.php/.php
  M [...]
```

106375 - nginx HTTP Server Detection

Synopsis

The nginx HTTP server was detected on the remote host.

Description

Nessus was able to detect the nginx HTTP server by looking at the HTTP banner on the remote host.

See Also

https://nginx.org/

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0677

Plugin Information

Published: 2018/01/26, Modified: 2021/04/07

Plugin Output

tcp/80/www

```
URL     : http://testphp.vulnweb.com/
Version : 1.19.0
source  : Server: nginx/1.19.0
```