De-ICE-web

Report generated by Nessus™ Thu, 01 Jun 2023 23:13:26 CEST

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

10.0.2.4

1	1	6	1	48
CRITICAL	HIGH	MEDIUM	LOW	INFO

Host Information

IP:	10.0.2.4
MAC Address:	08:00:27:64:FE:E2
OS:	Linux Kernel 3.0 on Ubuntu 12.04 (precise)

Vulnerabilities

125855 - phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)

Synopsis

The remote web server hosts a PHP application that is affected by SQLi vulnerability.

Description

According to its self-reported version number, the phpMyAdmin application hosted on the remote web server is prior to 4.8.6. It is, therefore, affected by a SQL injection (SQLi) vulnerability that exists in designer feature of phpMyAdmin. An unauthenticated, remote attacker can exploit this to inject or manipulate SQL queries in the back-end database, resulting in the disclosure or manipulation of arbitrary data.

Note that Nessus has not attempted to exploit these issues but has instead relied only on the application's self-reported version number.

See Also

http://www.nessus.org/u?c9d7fc8c

Solution

Upgrade to phpMyAdmin version 4.8.6 or later.

Alternatively, apply the patches referenced in the vendor advisories.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

8.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.9

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	108617
CVE	CVE-2019-11768

Plugin Information

Published: 2019/06/13, Modified: 2022/04/11

Plugin Output

tcp/443/www

```
URL               : https://10.0.2.4/phpmyadmin
Installed version : 3.4.10.1
Fixed version     : 4.8.6
```

42424 - CGI Generic SQL Injection (blind)

Synopsis

A CGI application hosted on the remote web server is potentially prone to SQL injection attack.

Description

By sending specially crafted parameters to one or more CGI scripts hosted on the remote web server, Nessus was able to get a very different response, which suggests that it may have been able to modify the behavior of the application and directly access the underlying database.

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

Note that this script is experimental and may be prone to false positives.

See Also

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

http://www.nessus.org/u?ed792cf5

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

Solution

Modify the affected CGI scripts so that they properly escape arguments.

Risk Factor

High

CVSS v3.0 Base Score

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

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:91
XREF	CWE:203
XREF	CWE:643
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: 2009/11/06, Modified: 2022/10/28

Plugin Output

tcp/443/www

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

+ The following resources may be vulnerable to blind SQL injection :

+ The 'js_frame' parameter of the /phpmyadmin/phpmyadmin.css.php CGI :

/phpmyadmin/phpmyadmin.css.php?token=a2d0c4ff4bf120ea5463c7104e263bc1&no
cache=3988383895&server=1&js_frame=rightzza2d0c4ff4bf120ea5463c7104e263b
c1&nocache=3988383895&server=1&js_frame=rightyy

-------- output --------
.syntax_comment {color: #808000;}
.syntax_comment_mysql {}
.syntax_comment_ansi {}
-------- vs --------
/**********************************************************************
*******/
/* general tags */
html {
------------------------
```

88098 - Apache Server ETag Header Information Disclosure

Synopsis

The remote web server is affected by an information disclosure vulnerability.

Description

The remote web server is affected by an information disclosure vulnerability due to the ETag header providing sensitive information that could aid an attacker, such as the inode number of requested files.

See Also

http://httpd.apache.org/docs/2.2/mod/core.html#FileETag

Solution

Modify the HTTP ETag header of the web server to not include file inodes in the ETag header calculation. Refer to the linked Apache documentation for more information.

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 v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

1.4

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	6939
CVE	CVE-2003-1418

XREF CWE:200

Plugin Information

Published: 2016/01/22, Modified: 2020/04/27

Plugin Output

tcp/80/www

```
Nessus was able to determine that the Apache Server listening on
port 80 leaks the servers inode numbers in the ETag HTTP
Header field :

  Source                : ETag: "2edc-6f6-4da1930e20900"
  Inode number          : 11996
  File size             : 1782 bytes
  File modification time : Apr. 11, 2013 at 17:33:56 GMT
```

88098 - Apache Server ETag Header Information Disclosure

Synopsis

The remote web server is affected by an information disclosure vulnerability.

Description

The remote web server is affected by an information disclosure vulnerability due to the ETag header providing sensitive information that could aid an attacker, such as the inode number of requested files.

See Also

http://httpd.apache.org/docs/2.2/mod/core.html#FileETag

Solution

Modify the HTTP ETag header of the web server to not include file inodes in the ETag header calculation. Refer to the linked Apache documentation for more information.

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 v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

1.4

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	6939
CVE	CVE-2003-1418

XREF CWE:200

Plugin Information

Published: 2016/01/22, Modified: 2020/04/27

Plugin Output

tcp/443/www

```
Nessus was able to determine that the Apache Server listening on
port 443 leaks the servers inode numbers in the ETag HTTP
Header field :

  Source                : ETag: "2edc-6f6-4da1930e20900"
  Inode number          : 11996
  File size             : 1782 bytes
  File modification time : Apr. 11, 2013 at 17:33:56 GMT
```

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://10.0.2.4/forum/themes/
http://10.0.2.4/forum/themes/default/
http://10.0.2.4/forum/themes/default/images/
http://10.0.2.4/forum/themes/default/subtemplates/
```

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/443/www

```
The following directories are browsable :

https://10.0.2.4/forum/themes/
https://10.0.2.4/forum/themes/default/
https://10.0.2.4/forum/themes/default/images/
https://10.0.2.4/forum/themes/default/subtemplates/
```

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://10.0.2.4/forum/
  - http://10.0.2.4/forum/index.php
```

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/443/www

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

  - https://10.0.2.4/forum/
  - https://10.0.2.4/forum/index.php
  - https://10.0.2.4/phpmyadmin/
  - https://10.0.2.4/phpmyadmin/index.php
  - https://10.0.2.4/phpmyadmin/url.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/443/www

```
Page : /phpmyadmin/
Destination Page: /phpmyadmin/index.php

Page : /phpmyadmin/url.php
Destination Page: /phpmyadmin/index.php

Page : /phpmyadmin/index.php
Destination Page: /phpmyadmin/index.php
```

18261 - Apache Banner Linux Distribution Disclosure

Synopsis

The name of the Linux distribution running on the remote host was found in the banner of the web server.

Description

Nessus was able to extract the banner of the Apache web server and determine which Linux distribution the remote host is running.

Solution

If you do not wish to display this information, edit 'httpd.conf' and set the directive 'ServerTokens Prod' and restart Apache.

Risk Factor

None

Plugin Information

Published: 2005/05/15, Modified: 2022/03/21

Plugin Output

tcp/0

```
The Linux distribution detected was :
 - Ubuntu 12.04 (precise)
 - Ubuntu 12.10 (quantal)
 - Ubuntu 13.04 (raring)
```

48204 - Apache HTTP Server Version

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

See Also

https://httpd.apache.org/

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0530

Plugin Information

Published: 2010/07/30, Modified: 2023/05/24

Plugin Output

tcp/80/www

```
URL        : http://10.0.2.4/
Version    : 2.2.99
Source     : Server: Apache/2.2.22 (Ubuntu) mod_ssl/2.2.22 OpenSSL/1.0.1
backported : 1
modules    : mod_ssl/2.2.22 OpenSSL/1.0.1
os         : ConvertedUbuntu
```

48204 - Apache HTTP Server Version

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

See Also

https://httpd.apache.org/

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0530

Plugin Information

Published: 2010/07/30, Modified: 2023/05/24

Plugin Output

tcp/443/www

```
URL        : https://10.0.2.4/
Version    : 2.2.99
Source     : Server: Apache/2.2.22 (Ubuntu) mod_ssl/2.2.22 OpenSSL/1.0.1
backported : 1
modules    : mod_ssl/2.2.22 OpenSSL/1.0.1
os         : ConvertedUbuntu
```

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/443/www

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

+ The following resources may be vulnerable to injectable parameter :

+ The 'db' parameter of the /phpmyadmin/index.php CGI :

/phpmyadmin/index.php?db=sxlkan

-------- output --------
<script src="./js/functions.js?ts=1329568005" type="text/javascrip [...]
<script src="./js/jquery/jquery.qtip-1.0.0.min.js?ts=1329568005" t [...]
<script src="./js/messages.php?lang=en&amp;db=sxlkan&amp;collation_conne
ction=utf8_general_ci&amp;token=b3235e63f6e945faccd19c39ee6c48dc" type="
text/javascript"></script>
<script type="text/javascript">
// <![CDATA[
------------------------
```

```
+ The 'lang' parameter of the /phpmyadmin/index.php CGI :

/phpmyadmin/index.php?lang=sxlkan

-------- output --------
</form>

<div><div class="error">Unknown language: sxlkan.</div><div class="notic
e">Cookies must be enabled past this point.</div></div></div>
</body>
</html>
------------------------

+ The 'table' parameter of the /phpmyadmin/index.php CGI :

/phpmyadmin/index.php?table=sxlkan

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

<form method="post" action="index.php" target="_parent">
<input type="hidden" name="db" value="" /><input type="hidden" name="tab
le" value="sxlkan" /><input type="hidden" name="lang" value="en" /><inpu
t type="hidden" name="collation_connection" value="utf8_general_ci" /><i
nput type="hidden" name="token" value="df2f73dc6b264cecee69e72558165dfa"
 /><fieldset><legend xml:lang="en" dir="ltr">Language</legend>
<select name="lang" onchange="this.form.submit();" xml:lang="en" d [...]
<option value="ar">&#1575;&#1604;&#1593;&#1585;&#1576;&#1610;&#157 [...]
------------------------

+ The 'pma_username' parameter of the /phpmyadmin/index.php CGI :

/phpmyadmin/index.php?pma_username=sxlkan

-------- output --------
<div class="item">
<label for="input_username">Username:</label>
<input type="text" name="pma_username" id="input_username" value="sxlkan
" size="24" class="textfield"/>
</div>
<div class="item">
------------------------

+ The 'db' parameter of the /phpmyadmin/index.php CGI :
 [...]
```

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]

arbitrary command execution (time based) : S=54         SP=54        AP=54        SC=0         AC=54

format string                            : S=18         SP=18        AP=18        SC=0         AC=18

cross-site scripting (comprehensive test): S=153        SP=153       AP=153       SC=0
 AC=153
injectable parameter                     : S=18         SP=18        AP=18        SC=0         AC=18

arbitrary command execution              : S=198        SP=198       AP=198       SC=0
 AC=198
local file inclusion                     : S=36         SP=36        AP=36        SC=0         AC=36

directory traversal                      : S=261        SP=261       AP=261       SC=0
 AC=261
web code injection                       : S=9          SP=9         AP=9         SC=0         AC=9

blind SQL injection (4 requests)         : S=36         SP=36        AP=36        SC=0         AC=36
```

```
persistent XSS                          : S=36        SP=36        AP=36        SC=0         AC=36

directory traversal (write access)      : S=18        SP=18        AP=18        SC=0         AC=18

XML injection                           : S=9         SP=9         AP=9         SC=0         AC=9

blind SQL injection                     : S=108       SP=108       AP=108       SC=0
 AC=108
SQL injection                           : S=252       SP=252       AP=252       SC=0
 AC=252
directory traversal (extended test)     : S=459       SP=459       AP=459       SC=0
 AC=459
SSI injection                           : S=27        SP=27        AP=27        SC=0         AC=27

unseen parameters                       : S=315       SP=315       AP=315       SC=0
 AC=315
SQL injection (2nd order)              [...]
```

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/443/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]

cross-site scripting (comprehensive test): S=374        SP=374       AP=782       SC=0
 AC=1615
persistent XSS                           : S=88         SP=88        AP=184       SC=0
 AC=380
arbitrary command execution              : S=484        SP=484       AP=1012      SC=0
 AC=2090
web code injection                       : S=22         SP=22        AP=46        SC=0         AC=95

script injection                         : S=4          SP=4         AP=13        SC=0         AC=20

HTML injection                           : S=20         SP=20        AP=65        SC=0
 AC=100
arbitrary command execution (time based) : S=132        SP=132       AP=276       SC=0
 AC=570
XML injection                            : S=22         SP=22        AP=46        SC=0         AC=95

unseen parameters                        : S=770        SP=770       AP=1610      SC=0
 AC=3325
```

```
directory traversal (write access)        : S=44          SP=44         AP=92         SC=0
 AC=190
SQL injection (2nd order)                 : S=22          SP=22         AP=46         SC=0          AC=95

on site request forgery                   : S=4           SP=4          AP=13         SC=0          AC=20

blind SQL injection (4 requests)          : S=88          SP=88         AP=184        SC=0
 AC=380
HTTP response splitting                   : S=36          SP=36         AP=117        SC=0
 AC=180
directory traversal (extended test)       : S=1122        SP=1122       AP=2346       SC=0
 AC=4845
header injection                          : S=8           SP=8          AP=26         SC=0          AC=40

injectable parameter                      : S=44          SP=44         AP=92         SC=0
 AC=190
local file inclusion                     [...]
```

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 :
- SQL injection
- cross-site scripting (comprehensive test)
- directory traversal
- arbitrary command execution
```

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/443/www

```
The following tests timed out without finding any flaw :
- SQL injection
- web code injection
- directory traversal (extended test)
- cross-site scripting (comprehensive test)
- SQL injection (2nd order)
- blind SQL injection (time based)
- local file inclusion
- arbitrary command execution
- directory traversal

The following tests were interrupted and did not report all possible flaws :
- injectable parameter
```

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

```
1 external URL was gathered on this web server :
URL...                                  - Seen on...


http://mylittleforum.net/               - /forum/
```

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/443/www

```
1 external URL was gathered on this web server :
URL...                                  - Seen on...


http://mylittleforum.net/               -
```

84502 - HSTS Missing From HTTPS Server

Synopsis

The remote web server is not enforcing HSTS.

Description

The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

See Also

https://tools.ietf.org/html/rfc6797

Solution

Configure the remote web server to use HSTS.

Risk Factor

None

Plugin Information

Published: 2015/07/02, Modified: 2021/05/19

Plugin Output

tcp/443/www

```
The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.
```

69826 - HTTP Cookie 'secure' Property Transport Mismatch

Synopsis

The remote web server sent out a cookie with a secure property that does not match the transport on which it was sent.

Description

The remote web server sends out cookies to clients with a 'secure'

property that does not match the transport, HTTP or HTTPS, over which they were received. This may occur in two forms :

1. The cookie is sent over HTTP, but has the 'secure'

property set, indicating that it should only be sent over a secure, encrypted transport such as HTTPS.

This should not happen.

2. The cookie is sent over HTTPS, but has no 'secure'

property set, indicating that it may be sent over both HTTP and HTTPS transports. This is common, but care should be taken to ensure that the 'secure' property not being set is deliberate.

See Also

https://tools.ietf.org/html/rfc6265

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/09/10, Modified: 2021/12/20

Plugin Output

tcp/80/www

```
The following cookies have the 'secure' property enabled, despite being served over HTTP :

  Domain   :
  Path     : /phpmyadmin/
  Name     : phpMyAdmin
  Value    : g2uqo8n0dmquqbe5t1euftcjjsdseo4j
  Secure   : true
  HttpOnly : true
```

```
Domain   :
Path     : /phpmyadmin/
Name     : pma_collation_connection
Value    : utf8_general_ci
Secure   : true
HttpOnly : true

Domain   :
Path     : /phpmyadmin/
Name     : pma_lang
Value    : en
Secure   : true
HttpOnly : true

Domain   :
Path     : /phpmyadmin/
Name     : pma_mcrypt_iv
Value    : mX2%2F%2B6MOpww%3D
Secure   : true
HttpOnly : true
```

69826 - HTTP Cookie 'secure' Property Transport Mismatch

Synopsis

The remote web server sent out a cookie with a secure property that does not match the transport on which it was sent.

Description

The remote web server sends out cookies to clients with a 'secure'

property that does not match the transport, HTTP or HTTPS, over which they were received. This may occur in two forms :

1. The cookie is sent over HTTP, but has the 'secure'

property set, indicating that it should only be sent over a secure, encrypted transport such as HTTPS.

This should not happen.

2. The cookie is sent over HTTPS, but has no 'secure'

property set, indicating that it may be sent over both HTTP and HTTPS transports. This is common, but care should be taken to ensure that the 'secure' property not being set is deliberate.

See Also

https://tools.ietf.org/html/rfc6265

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/09/10, Modified: 2021/12/20

Plugin Output

tcp/443/www

```
The following cookies do not have the 'secure' property enabled, despite being served over HTTPS :

  Domain   :
  Path     : /
  Name     : PHPSESSID
  Value    : afuj2b7eu4v95sr0kigo8ncr97
  Secure   : false
  HttpOnly : false
```

```
Domain   :
Path     : /
Name     : mlf2_last_visit
Value    : 1685651195.1685651195
Secure   : false
HttpOnly : false

Domain   :
Path     : /
Name     : mlf2_usersettings
Value    : 0.0.1.0.0
Secure   : false
HttpOnly : false
```

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 the response to an OPTIONS request :

  - HTTP methods GET HEAD OPTIONS POST are allowed on :

    /
    /forum/themes
    /forum/themes/default
    /forum/themes/default/images
    /forum/themes/default/subtemplates
    /icons


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 OPTIONS POST are allowed on :

    /
    /forum
    /forum/themes
    /forum/themes/default
    /forum/themes/default/images
    /forum/themes/default/subtemplates
    /icons

  - Invalid/unknown HTTP methods are allowed on :

    /cgi-bin
```

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/443/www

```
Based on the response to an OPTIONS request :

  - HTTP methods GET HEAD OPTIONS POST are allowed on :

    /
    /forum/themes
    /forum/themes/default
    /forum/themes/default/images
    /forum/themes/default/subtemplates
    /icons
    /phpmyadmin/themes
    /phpmyadmin/themes/pmahomme
    /phpmyadmin/themes/pmahomme/jquery


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 OPTIONS POST are allowed on :

    /
    /forum
    /forum/themes
    /forum/themes/default
    /forum/themes/default/images
    /forum/themes/default/subtemplates
    /icons
    /phpmyadmin
    /phpmyadmin/themes
    /phpmyadmin/themes/pmahomme
    /phpmyadmin/themes/pmahomme/jquery

  - 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 :

Apache/2.2.22 (Ubuntu) mod_ssl/2.2.22 OpenSSL/1.0.1
```

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/443/www

```
The remote web server type is :

Apache/2.2.22 (Ubuntu) mod_ssl/2.2.22 OpenSSL/1.0.1
```

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 : yes
Options allowed : (Not implemented)
Headers :

  Date: Thu, 01 Jun 2023 20:27:41 GMT
  Server: Apache/2.2.22 (Ubuntu) mod_ssl/2.2.22 OpenSSL/1.0.1
  Last-Modified: Thu, 11 Apr 2013 17:33:56 GMT
  ETag: "2edc-6f6-4da1930e20900"
  Accept-Ranges: bytes
  Content-Length: 1782
  Vary: Accept-Encoding
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html

Response Body :

<html>
<title>Lazy Admin Corp.</title>
<style type="text/css">
table {
border-width: 1px;
border-spacing: 10px;
```

```
border-style: dashed;
border-color: gray;
border-collapse: separate;
background-color: #0d0d0d;
}
font {
font-family: Verdana;
color: #aaaaaa;
}
font.hidden {
font-family: Verdana;
color: #0d0d0d;
}
font.credit {
font-family: Arial;
color: #303030;
font-size: small;
}
</style>
<body bgcolor=#202020><br><br><center><table><td><br>
<font><center><big><b>Welcome to<br>
<big><big>Lazy Admin Corp.<br></big>
HackingLab!</b></big></big></h1></center><br><br><br>
You are employed by the management of LazyAdmin corp. to PenTest their Network.<br>
At this point you have managed to successfully break into the network.<br>
The goal is now to find and extract sensitive information.<br>
<br>
<br>
<div align=right>"I choose a lazy person to do a hard job.<br>
Because a lazy person will find an easy way to do it."<br>
~ <i>Bill Gates</i></div>
<br>
<br>
Below you can find some hints how to get the sensitive information<br>
(just mark the lines to see the hints):<br>
<br><br></font>
```

```
<font class="hidden">
1. Have you seen our new cool forum yet?<br><br>
2. Do not post sensitive information to public!<br><br>
3. Different passwords for different services. What is that for?!<br><br>
4. What if you are able to break out of your cell and manage to enter another one?<br><br>
5. Some things change from time to time, others don't.<br><br>
6. Sor [...]
```

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/443/www

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

  Date: Thu, 01 Jun 2023 20:27:41 GMT
  Server: Apache/2.2.22 (Ubuntu) mod_ssl/2.2.22 OpenSSL/1.0.1
  Last-Modified: Thu, 11 Apr 2013 17:33:56 GMT
  ETag: "2edc-6f6-4da1930e20900"
  Accept-Ranges: bytes
  Content-Length: 1782
  Vary: Accept-Encoding
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html

Response Body :

<html>
<title>Lazy Admin Corp.</title>
<style type="text/css">
table {
border-width: 1px;
border-spacing: 10px;
```

```
border-style: dashed;
border-color: gray;
border-collapse: separate;
background-color: #0d0d0d;
}
font {
font-family: Verdana;
color: #aaaaaa;
}
font.hidden {
font-family: Verdana;
color: #0d0d0d;
}
font.credit {
font-family: Arial;
color: #303030;
font-size: small;
}
</style>
<body bgcolor=#202020><br><br><center><table><td><br>
<font><center><big><b>Welcome to<br>
<big><big>Lazy Admin Corp.<br></big>
HackingLab!</b></big></big></h1></center><br><br><br>
You are employed by the management of LazyAdmin corp. to PenTest their Network.<br>
At this point you have managed to successfully break into the network.<br>
The goal is now to find and extract sensitive information.<br>
<br>
<br>
<div align=right>"I choose a lazy person to do a hard job.<br>
Because a lazy person will find an easy way to do it."<br>
~ <i>Bill Gates</i></div>
<br>
<br>
Below you can find some hints how to get the sensitive information<br>
(just mark the lines to see the hints):<br>
<br><br></font>
```

```
<font class="hidden">
1. Have you seen our new cool forum yet?<br><br>
2. Do not post sensitive information to public!<br><br>
3. Different passwords for different services. What is that for?!<br><br>
4. What if you are able to break out of your cell and manage to enter another one?<br><br>
5. Some things change from time to time, others don't.<br><br>
6. So [...]
```

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://10.0.2.4/
  - http://10.0.2.4/forum/
  - http://10.0.2.4/forum/index.php
  - http://10.0.2.4/forum/themes/
  - http://10.0.2.4/forum/themes/default/
  - http://10.0.2.4/forum/themes/default/images/
  - http://10.0.2.4/forum/themes/default/subtemplates/
```

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/443/www

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

  - https://10.0.2.4/
  - https://10.0.2.4/forum/
  - https://10.0.2.4/forum/index.php
  - https://10.0.2.4/forum/themes/
  - https://10.0.2.4/forum/themes/default/
  - https://10.0.2.4/forum/themes/default/images/
  - https://10.0.2.4/forum/themes/default/subtemplates/
  - https://10.0.2.4/phpmyadmin/
  - https://10.0.2.4/phpmyadmin/index.php
  - https://10.0.2.4/phpmyadmin/url.php
```

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://10.0.2.4/
  - http://10.0.2.4/forum/
  - http://10.0.2.4/forum/index.php
  - http://10.0.2.4/forum/themes/
  - http://10.0.2.4/forum/themes/default/
  - http://10.0.2.4/forum/themes/default/images/
  - http://10.0.2.4/forum/themes/default/subtemplates/
```

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/443/www

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

  - https://10.0.2.4/
  - https://10.0.2.4/forum/
  - https://10.0.2.4/forum/index.php
  - https://10.0.2.4/forum/themes/
  - https://10.0.2.4/forum/themes/default/
  - https://10.0.2.4/forum/themes/default/images/
  - https://10.0.2.4/forum/themes/default/subtemplates/
  - https://10.0.2.4/phpmyadmin/
  - https://10.0.2.4/phpmyadmin/index.php
  - https://10.0.2.4/phpmyadmin/url.php
```

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: 2023/05/31

Plugin Output

tcp/21/ftp

```
Port 21/tcp was found to be open
```

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: 2023/05/31

Plugin Output

tcp/22/ssh

```
Port 22/tcp was found to be open
```

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: 2023/05/31

Plugin Output

tcp/80/www

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

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: 2023/05/31

Plugin Output

tcp/443/www

```
Port 443/tcp was found to be open
```

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: 2023/05/31

Plugin Output

tcp/993/imap

```
Port 993/tcp was found to be open
```

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: 2023/05/31

Plugin Output

tcp/995/pop3

```
Port 995/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: 2023/04/27

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.5.2
Nessus build : 20009
Plugin feed version : 202306011619
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : ubuntu1404-x86-64
Scan type : Normal
Scan name : De-ICE-web
```

```
Scan policy used : Web Application Tests
Scanner IP : 10.0.2.15
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Ping RTT : 276.878 ms
Thorough tests : yes
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 : all_pairs
Web app tests -  Try all HTTP methods : yes
Web app tests -  Maximum run time : 10 minutes.
Web app tests -  Stop at first flaw : param
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : Detected
Allow post-scan editing : Yes
Scan Start Date : 2023/6/1 22:25 CEST
Scan duration : 2859 sec
Scan for malware : no
```

57323 - OpenSSL Version Detection

Synopsis

Nessus was able to detect the OpenSSL version.

Description

Nessus was able to extract the OpenSSL version from the web server's banner. Note that security patches in many cases are backported and the displayed version number does not show the patch level. Using it to identify vulnerable software is likely to lead to false detections.

See Also

https://www.openssl.org/

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0682

Plugin Information

Published: 2011/12/16, Modified: 2023/03/27

Plugin Output

tcp/80/www

```
Source             : Apache/2.2.22 (Ubuntu) mod_ssl/2.2.22 OpenSSL/1.0.1
Reported version   : 1.0.1
Backported version : 1.0.1
```

57323 - OpenSSL Version Detection

Synopsis

Nessus was able to detect the OpenSSL version.

Description

Nessus was able to extract the OpenSSL version from the web server's banner. Note that security patches in many cases are backported and the displayed version number does not show the patch level. Using it to identify vulnerable software is likely to lead to false detections.

See Also

https://www.openssl.org/

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0682

Plugin Information

Published: 2011/12/16, Modified: 2023/03/27

Plugin Output

tcp/443/www

```
Source             : Apache/2.2.22 (Ubuntu) mod_ssl/2.2.22 OpenSSL/1.0.1
Reported version   : 1.0.1
Backported version : 1.0.1
```

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: 2023/05/31

Plugin Output

tcp/0

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

[ phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3) (125855) ]

+ Action to take : Upgrade to phpMyAdmin version 4.8.6 or later.
Alternatively, apply the patches referenced in the vendor advisories.
```

73787 - Postfix Admin Detection

Synopsis

A domain, alias, and mailbox manager are running on the remote host.

Description

The web interface for Postfix Admin was detected on the remote host.
Postfix Admin is a web-based application for managing mailboxes, domains, and aliases.

See Also

http://postfixadmin.sourceforge.net/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2014/04/30, Modified: 2023/05/31

Plugin Output

tcp/443/www

```
The following instance of Postfix Admin was detected on the remote host :

  Version : 2.3.6
  URL     : https://10.0.2.4/postfixadmin/
```

12647 - SquirrelMail Detection

Synopsis

The remote web server contains a webmail application.

Description

The remote host is running SquirrelMail, a PHP-based webmail package that provides access to mail accounts via POP3 or IMAP.

See Also

http://www.squirrelmail.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/07/11, Modified: 2022/06/01

Plugin Output

tcp/443/www

```
The following instance of Squirrelmail was detected on the remote host :

  Version : 1.4.22
  URL     : https://10.0.2.4/webmail/
```

85601 - Web Application Cookies Not Marked HttpOnly

Synopsis

HTTP session cookies might be vulnerable to cross-site scripting attacks.

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, one or more of those cookies are not marked 'HttpOnly', meaning that a malicious client-side script, such as JavaScript, could read them. The HttpOnly flag is a security mechanism to protect against cross-site scripting attacks, which was proposed by Microsoft and initially implemented in Internet Explorer. All modern browsers now support it.

Note that this plugin detects all general cookies missing the HttpOnly cookie flag, whereas plugin 48432 (Web Application Session Cookies Not Marked HttpOnly) will only detect session cookies from an authenticated session missing the HttpOnly cookie flag.

See Also

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

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If possible, add the 'HttpOnly' attribute to all session cookies and any cookies containing sensitive data.

Risk Factor

None

References

XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:442
XREF	CWE:629
XREF	CWE:711
XREF	CWE:712
XREF	CWE:722
XREF	CWE:725
XREF	CWE:750
XREF	CWE:751
XREF	CWE:800
XREF	CWE:801

XREF	CWE:809
XREF	CWE:811
XREF	CWE:864
XREF	CWE:900
XREF	CWE:928
XREF	CWE:931
XREF	CWE:990

Plugin Information

Published: 2015/08/24, Modified: 2015/08/24

Plugin Output

tcp/80/www

```
The following cookies do not set the HttpOnly cookie flag :

Name : mlf2_last_visit
Path : /
Value : 1685651195.1685651195
Domain :
Version : 1
Expires : Sat, 01-Jul-2023 20:26:35 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : mlf2_usersettings
Path : /
Value : 0.0.1.0.0
Domain :
Version : 1
Expires : Sat, 01-Jul-2023 20:26:35 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : PHPSESSID
Path : /
Value : afuj2b7eu4v95sr0kigo8ncr97
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :
```

85601 - Web Application Cookies Not Marked HttpOnly

Synopsis

HTTP session cookies might be vulnerable to cross-site scripting attacks.

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, one or more of those cookies are not marked 'HttpOnly', meaning that a malicious client-side script, such as JavaScript, could read them. The HttpOnly flag is a security mechanism to protect against cross-site scripting attacks, which was proposed by Microsoft and initially implemented in Internet Explorer. All modern browsers now support it.

Note that this plugin detects all general cookies missing the HttpOnly cookie flag, whereas plugin 48432 (Web Application Session Cookies Not Marked HttpOnly) will only detect session cookies from an authenticated session missing the HttpOnly cookie flag.

See Also

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

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If possible, add the 'HttpOnly' attribute to all session cookies and any cookies containing sensitive data.

Risk Factor

None

References

XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:442
XREF	CWE:629
XREF	CWE:711
XREF	CWE:712
XREF	CWE:722
XREF	CWE:725
XREF	CWE:750
XREF	CWE:751
XREF	CWE:800
XREF	CWE:801

XREF	CWE:809
XREF	CWE:811
XREF	CWE:864
XREF	CWE:900
XREF	CWE:928
XREF	CWE:931
XREF	CWE:990

Plugin Information

Published: 2015/08/24, Modified: 2015/08/24

Plugin Output

tcp/443/www

```
The following cookies do not set the HttpOnly cookie flag :

Name : mlf2_last_visit
Path : /
Value : 1685651195.1685651195
Domain :
Version : 1
Expires : Sat, 01-Jul-2023 20:26:35 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : mlf2_usersettings
Path : /
Value : 0.0.1.0.0
Domain :
Version : 1
Expires : Sat, 01-Jul-2023 20:26:35 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : PHPSESSID
Path : /
Value : afuj2b7eu4v95sr0kigo8ncr97
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :
```

85602 - Web Application Cookies Not Marked Secure

Synopsis

HTTP session cookies might be transmitted in cleartext.

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, there are instances where the application is running over unencrypted HTTP or the cookies are not marked 'secure', meaning the browser could send them back over an unencrypted link under certain circumstances. As a result, it may be possible for a remote attacker to intercept these cookies.

Note that this plugin detects all general cookies missing the 'secure'

cookie flag, whereas plugin 49218 (Web Application Session Cookies Not Marked Secure) will only detect session cookies from an authenticated session missing the secure cookie flag.

See Also

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

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If possible, ensure all communication occurs over an encrypted channel and add the 'secure' attribute to all session cookies or any cookies containing sensitive data.

Risk Factor

None

References

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

Plugin Information

Published: 2015/08/24, Modified: 2015/08/24

Plugin Output

tcp/80/www

```
The following cookies do not set the secure cookie flag :

Name : mlf2_last_visit
Path : /
Value : 1685651195.1685651195
Domain :
Version : 1
Expires : Sat, 01-Jul-2023 20:26:35 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : mlf2_usersettings
Path : /
Value : 0.0.1.0.0
Domain :
Version : 1
Expires : Sat, 01-Jul-2023 20:26:35 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : PHPSESSID
Path : /
Value : afuj2b7eu4v95sr0kigo8ncr97
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :
```

85602 - Web Application Cookies Not Marked Secure

Synopsis

HTTP session cookies might be transmitted in cleartext.

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, there are instances where the application is running over unencrypted HTTP or the cookies are not marked 'secure', meaning the browser could send them back over an unencrypted link under certain circumstances. As a result, it may be possible for a remote attacker to intercept these cookies.

Note that this plugin detects all general cookies missing the 'secure'

cookie flag, whereas plugin 49218 (Web Application Session Cookies Not Marked Secure) will only detect session cookies from an authenticated session missing the secure cookie flag.

See Also

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

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If possible, ensure all communication occurs over an encrypted channel and add the 'secure' attribute to all session cookies or any cookies containing sensitive data.

Risk Factor

None

References

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

Plugin Information

Published: 2015/08/24, Modified: 2015/08/24

Plugin Output

tcp/443/www

```
The following cookies do not set the secure cookie flag :

Name : mlf2_last_visit
Path : /
Value : 1685651195.1685651195
Domain :
Version : 1
Expires : Sat, 01-Jul-2023 20:26:35 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : mlf2_usersettings
Path : /
Value : 0.0.1.0.0
Domain :
Version : 1
Expires : Sat, 01-Jul-2023 20:26:35 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : PHPSESSID
Path : /
Value : afuj2b7eu4v95sr0kigo8ncr97
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :
```

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 /forum/index.php :

id : Potential horizontal or vertical privilege escalation
```

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/443/www

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

id : Potential horizontal or vertical privilege escalation
```

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://10.0.2.4/
  - http://10.0.2.4/forum/
  - http://10.0.2.4/forum/index.php
  - http://10.0.2.4/forum/themes/
  - http://10.0.2.4/forum/themes/default/
  - http://10.0.2.4/forum/themes/default/ajax_preview.tpl
  - http://10.0.2.4/forum/themes/default/avatar.tpl
  - http://10.0.2.4/forum/themes/default/images/
  - http://10.0.2.4/forum/themes/default/images/add.png
  - http://10.0.2.4/forum/themes/default/images/add_page.png
  - http://10.0.2.4/forum/themes/default/images/add_user.png
  - http://10.0.2.4/forum/themes/default/images/ajax_preview.png
  - http://10.0.2.4/forum/themes/default/images/arrow_down.png
  - http://10.0.2.4/forum/themes/default/images/arrow_selected.png
  - http://10.0.2.4/forum/themes/default/images/arrow_up.png
  - http://10.0.2.4/forum/themes/default/images/asc.png
  - http://10.0.2.4/forum/themes/default/images/backup.png
  - http://10.0.2.4/forum/themes/default/images/bg_gradient_x.png
  - http://10.0.2.4/forum/themes/default/images/bg_gradient_y.png
  - http://10.0.2.4/forum/themes/default/images/bg_sprite_1.png
  - http://10.0.2.4/forum/themes/default/images/bg_sprite_2.png
  - http://10.0.2.4/forum/themes/default/images/bg_sprite_3.png
```

```
    - http://10.0.2.4/forum/themes/default/images/bg_sprite_4.png
    - http://10.0.2.4/forum/themes/default/images/bg_sprite_5.png
    - http://10.0.2.4/forum/themes/default/images/canvas_bg.png
    - http://10.0.2.4/forum/themes/default/images/categories.png
    - http://10.0.2.4/forum/themes/default/images/caution.png
    - http://10.0.2.4/forum/themes/default/images/close.png
    - http://10.0.2.4/forum/themes/default/images/complete_thread.png
    - http://10.0.2.4/forum/themes/default/images/delete.png
    - http://10.0.2.4/forum/themes/default/images/delete_entries.png
    - http://10.0.2.4/forum/themes/default/images/delete_posting.png
    - http://10.0.2.4/forum/themes/default/images/delete_user.png
    - http://10.0.2.4/forum/themes/default/images/desc.png
    - http://10.0. [...]
```

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/443/www

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

  - https://10.0.2.4/
  - https://10.0.2.4/forum/
  - https://10.0.2.4/forum/index.php
  - https://10.0.2.4/forum/themes/
  - https://10.0.2.4/forum/themes/default/
  - https://10.0.2.4/forum/themes/default/ajax_preview.tpl
  - https://10.0.2.4/forum/themes/default/avatar.tpl
  - https://10.0.2.4/forum/themes/default/images/
  - https://10.0.2.4/forum/themes/default/images/add.png
  - https://10.0.2.4/forum/themes/default/images/add_page.png
  - https://10.0.2.4/forum/themes/default/images/add_user.png
  - https://10.0.2.4/forum/themes/default/images/ajax_preview.png
  - https://10.0.2.4/forum/themes/default/images/arrow_down.png
  - https://10.0.2.4/forum/themes/default/images/arrow_selected.png
  - https://10.0.2.4/forum/themes/default/images/arrow_up.png
  - https://10.0.2.4/forum/themes/default/images/asc.png
  - https://10.0.2.4/forum/themes/default/images/backup.png
  - https://10.0.2.4/forum/themes/default/images/bg_gradient_x.png
  - https://10.0.2.4/forum/themes/default/images/bg_gradient_y.png
  - https://10.0.2.4/forum/themes/default/images/bg_sprite_1.png
  - https://10.0.2.4/forum/themes/default/images/bg_sprite_2.png
  - https://10.0.2.4/forum/themes/default/images/bg_sprite_3.png
```

```
  - https://10.0.2.4/forum/themes/default/images/bg_sprite_4.png
  - https://10.0.2.4/forum/themes/default/images/bg_sprite_5.png
  - https://10.0.2.4/forum/themes/default/images/canvas_bg.png
  - https://10.0.2.4/forum/themes/default/images/categories.png
  - https://10.0.2.4/forum/themes/default/images/caution.png
  - https://10.0.2.4/forum/themes/default/images/close.png
  - https://10.0.2.4/forum/themes/default/images/complete_thread.png
  - https://10.0.2.4/forum/themes/default/images/delete.png
  - https://10.0.2.4/forum/themes/default/images/delete_entries.png
  - https://10.0.2.4/forum/themes/default/images/delete_posting.png
  - https://10.0.2.4/forum/themes/default/images/delete_user.png
  - https://10.0.2.4/forum/themes/defaul [...]
```

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:
/cgi-bin, /forum, /icons

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
```

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/443/www

```
The following directories were discovered:
/cgi-bin, /forum, /icons, /phpmyadmin

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
```

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: 2023/05/31

Plugin Output

tcp/80/www

```
Webmirror performed 114 queries in 3s (38.000 queries per second)

The following CGIs have been discovered :


+ CGI : /forum/index.php
  Methods : GET
  Argument : category
   Value: 0
  Argument : fold_threads
   Value: true
  Argument : id
   Value: 7
  Argument : items
   Value: thread_starts
  Argument : mode
   Value: contact
  Argument : refresh
   Value: 1
  Argument : search
   Value: Search...
  Argument : thread_order
   Value: 1
  Argument : toggle_view
   Value: true

Directory index found at /forum/themes/default/
```

```
Directory index found at /forum/themes/
Directory index found at /forum/themes/default/images/
Directory index found at /forum/themes/default/subtemplates/
```

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: 2023/05/31

Plugin Output

tcp/443/www

```
Webmirror performed 129 queries in 4s (32.0250 queries per second)

The following CGIs have been discovered :


+ CGI : /forum/index.php
  Methods : GET
  Argument : category
   Value: 0
  Argument : fold_threads
   Value: true
  Argument : id
   Value: 7
  Argument : items
   Value: thread_starts
  Argument : mode
   Value: contact
  Argument : refresh
   Value: 1
  Argument : search
   Value: Search...
  Argument : thread_order
   Value: 1
  Argument : toggle_view
   Value: true
```

```
+ CGI : /phpmyadmin/phpmyadmin.css.php
  Methods : GET
  Argument : js_frame
   Value: right
  Argument : nocache
   Value: 3988383895
  Argument : server
   Value: 1
  Argument : token
   Value: a7c93871f4cc865eba6cab0ede0d4824


+ CGI : /phpmyadmin/url.php
  Methods : GET
  Argument : token
   Value: a7c93871f4cc865eba6cab0ede0d4824
  Argument : url
   Value: http%3A%2F%2Fwww.phpmyadmin.net%2F


+ CGI : /phpmyadmin/index.php
  Methods : POST
  Argument : db
  Argument : lang
  Argument : pma_password
  Argument : pma_username
  Argument : server
   Value: 1
  Argument : table
  Argument : token
   Value: a7c93871f4cc865eba6cab0ede0d4824

Directory index found at /forum/themes/default/
Directory index found at /forum/themes/
Directory index found at /forum/themes/default/images/
Directory index found at /forum/themes/default/subtemplates/
```

17219 - phpMyAdmin Detection

Synopsis

The remote web server hosts a database management application written in PHP.

Description

The remote host is running phpMyAdmin, a web-based MySQL administration tool written in PHP.

See Also

https://www.phpmyadmin.net/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/02/25, Modified: 2022/06/01

Plugin Output

tcp/443/www

```
The following instance of phpMyAdmin was detected on the remote host :

  Version : 3.4.10.1
  URL     : https://10.0.2.4/phpmyadmin/
```