



dvwa :Conduct application vulnerability scan

Report generated by Nessus™

Sat, 12 Aug 2023 19:27:27 EDT

TABLE OF CONTENTS

Vulnerabilities by Host

- 172.17.0.2..... 4

Nessus Essentials

Vulnerabilities by Host

172.17.0.2



Scan Information

Start time: Sat Aug 12 19:15:09 2023
End time: Sat Aug 12 19:27:27 2023

Host Information

IP: 172.17.0.2
MAC Address: 02:42:AC:11:00:02
OS: Linux Kernel 3.16 on Debian 8.0 (jessie)

Vulnerabilities

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://172.17.0.2/config/
http://172.17.0.2/docs/
http://172.17.0.2/dvwa/
http://172.17.0.2/dvwa/css/
http://172.17.0.2/dvwa/images/
http://172.17.0.2/dvwa/includes/
http://172.17.0.2/dvwa/includes/DBMS/
http://172.17.0.2/dvwa/js/
http://172.17.0.2/external/
http://172.17.0.2/external/phpids/
http://172.17.0.2/external/phpids/0.6/
http://172.17.0.2/external/phpids/0.6/docs/
http://172.17.0.2/external/phpids/0.6/docs/examples/
http://172.17.0.2/external/phpids/0.6/lib/
http://172.17.0.2/external/phpids/0.6/lib/IDS/
http://172.17.0.2/external/phpids/0.6/tests/
http://172.17.0.2/external/phpids/0.6/tests/IDS/
http://172.17.0.2/external/recaptcha/
```

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://172.17.0.2/login.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: /login.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 :  
- Debian 8.0 (jessie)
```

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: 2023/07/31

Plugin Output

tcp/80/www

```
URL      : http://172.17.0.2/
Version  : 2.4.99
Source   : Server: Apache/2.4.10 (Debian)
backported : 1
os       : ConvertedDebian
```

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=30          SP=30          AP=66          SC=6          AC=78
format string                            : S=10          SP=10          AP=22          SC=2          AC=26
cross-site scripting (comprehensive test): S=20          SP=20          AP=44          SC=4          AC=52
injectable parameter                     : S=10          SP=10          AP=22          SC=2          AC=26
arbitrary command execution              : S=80          SP=80          AP=176         SC=16
AC=208
local file inclusion                     : S=5           SP=5           AP=11          SC=1          AC=13
directory traversal                       : S=125         SP=125         AP=275         SC=25
AC=325
web code injection                       : S=5           SP=5           AP=11          SC=1          AC=13
blind SQL injection (4 requests)         : S=20          SP=20          AP=44          SC=4          AC=52
```

| | | | | | |
|---|---------|--------|--------|-------|-------|
| persistent XSS | : S=20 | SP=20 | AP=44 | SC=4 | AC=52 |
| directory traversal (write access) | : S=10 | SP=10 | AP=22 | SC=2 | AC=26 |
| XML injection | : S=5 | SP=5 | AP=11 | SC=1 | AC=13 |
| blind SQL injection AC=156 | : S=60 | SP=60 | AP=132 | SC=12 | |
| SQL injection AC=312 | : S=120 | SP=120 | AP=264 | SC=24 | |
| directory traversal (extended test) AC=663 | : S=255 | SP=255 | AP=561 | SC=51 | |
| SSI injection | : S=15 | SP=15 | AP=33 | SC=3 | AC=39 |
| unseen parameters AC=455 | : S=175 | SP=175 | AP=385 | SC=35 | |
| SQL injection (2nd order) | [...] | | | | |

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

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

http://hiderefer.com/?http://www.dvwa.co.uk/ - /login.php
http://www.phpdoc.org                - /external/phpids/0.6/docs/phpdocumentor/li_PHPIDS.html
http://www.phpunit.de/                - /external/phpids/0.6/tests/coverage/
http://www.xdebug.org/                - /external/phpids/0.6/tests/coverage/
```

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_\(OTG-CONFIG-006\)](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 :

```
/config
/docs
/dvwa
/dvwa/css
/dvwa/images
/dvwa/includes
/dvwa/includes/DBMS
/dvwa/js
/external
/external/phpids
/external/phpids/0.6
/external/phpids/0.6/docs
/external/phpids/0.6/docs/examples
/external/phpids/0.6/docs/phpdocumentor
/external/phpids/0.6/lib
/external/phpids/0.6/lib/IDS
/icons
```

Based on tests of each method :

- HTTP methods GET HEAD OPTIONS POST are allowed on :

```
/
/config
/docs
/dvwa
/dvwa/css
/dvwa/images
/dvwa/includes
/dvwa/includes/DBMS
/dvwa/js
/external
/external/phpids
/external/phpids/0.6
/external/phpids/0.6/docs
/external/phpids/0.6/docs/examples
/external/phpids/0.6/docs/phpdocumentor
/external/phpids/0.6/lib
/external/phpids/0.6/lib/IDS
/icons
```

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/2.4.10 (Debian)
```


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/1.1 302 Found

Protocol version : HTTP/1.1

SSL : no

Keep-Alive : yes

Options allowed : (Not implemented)

Headers :

Date: Sat, 12 Aug 2023 23:16:17 GMT

Server: Apache/2.4.10 (Debian)

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0

Pragma: no-cache

Location: login.php

Content-Length: 0

Keep-Alive: timeout=5, max=100

Connection: Keep-Alive

Content-Type: text/html; charset=UTF-8

Response Body :

91634 - HyperText Transfer Protocol (HTTP) Redirect Information

Synopsis

The remote web server redirects requests to the root directory.

Description

The remote web server issues an HTTP redirect when requesting the root directory of the web server.

This plugin is informational only and does not denote a security problem.

Solution

Analyze the redirect(s) to verify that this is valid operation for your web server and/or application.

Risk Factor

None

Plugin Information

Published: 2016/06/16, Modified: 2017/10/12

Plugin Output

tcp/80/www

```
Request       : http://172.17.0.2/
HTTP response : HTTP/1.1 302 Found
Redirect to   : http://172.17.0.2/login.php
Redirect type  : 30x redirect

Final page    : http://172.17.0.2/login.php
HTTP response : HTTP/1.1 200 OK
```

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://172.17.0.2/config/>
- <http://172.17.0.2/config/config.inc.php>
- <http://172.17.0.2/docs/>
- <http://172.17.0.2/docs/pdf.html>
- <http://172.17.0.2/dvwa/>
- <http://172.17.0.2/dvwa/css/>
- <http://172.17.0.2/dvwa/images/>
- <http://172.17.0.2/dvwa/includes/>
- <http://172.17.0.2/dvwa/includes/DBMS/>
- <http://172.17.0.2/dvwa/includes/dvwaPage.inc.php>
- <http://172.17.0.2/dvwa/includes/dvwaPhpIds.inc.php>

```
- http://172.17.0.2/dvwa/js/
- http://172.17.0.2/external/
- http://172.17.0.2/external/phpids/
- http://172.17.0.2/external/phpids/0.6/
- http://172.17.0.2/external/phpids/0.6/docs/
- http://172.17.0.2/external/phpids/0.6/docs/examples/
- http://172.17.0.2/external/phpids/0.6/docs/examples/example.php
- http://172.17.0.2/external/phpids/0.6/docs/phpdocumentor/
- http://172.17.0.2/external/phpids/0.6/docs/phpdocumentor/blank.html
- http://172.17.0.2/external/phpids/0.6/docs/phpdocumentor/classtrees_PHPIDS.html
- http://172.17.0.2/external/phpids/0.6/docs/phpdocumentor/elementindex.html
- http://172.17.0.2/external/phpids/0.6/docs/phpdocumentor/elementindex_PHPIDS.html
- http://172.17.0.2/external/phpids/0.6/docs/phpdocumentor/li_PHPIDS.html
- http://172.17.0.2/external/phpids/0.6/docs/phpdocumentor/packages.html
- http://172.17.0.2/external/phpids/0.6/lib/
- http://172.17.0.2/external/phpids/0.6/lib/IDS/
- http://172.17.0.2/external/phpids/0.6/lib/IDS/Converter.php
- http://172.17.0.2/external/phpids/0.6/lib/IDS/Event.php
- http://172.17.0.2/external/phpids/0.6/lib/IDS/Filter.php
- http://172.17.0.2/external/phpids/0.6/lib/IDS/Init.php
- http://172.17.0.2/external/phpids/0.6/lib/IDS/Monitor.php
- http://172.17.0.2/external/phpids/0.6/lib/IDS/Report.php
- http://172.17.0.2/external/phpids/0.6/tests/
- http://172.17.0.2/external/phpids/0.6/tests/IDS/
- http://172.17.0.2/external/phpids/0.6/tests/coverage/
- http://172.17.0.2/external/ph [...]
```

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://172.17.0.2/config/>
- <http://172.17.0.2/config/config.inc.php>
- <http://172.17.0.2/docs/>
- <http://172.17.0.2/docs/pdf.html>
- <http://172.17.0.2/dvwa/>
- <http://172.17.0.2/dvwa/css/>
- <http://172.17.0.2/dvwa/images/>
- <http://172.17.0.2/dvwa/includes/>
- <http://172.17.0.2/dvwa/includes/DBMS/>
- <http://172.17.0.2/dvwa/includes/dvwaPage.inc.php>
- <http://172.17.0.2/dvwa/includes/dvwaPhpIds.inc.php>
- <http://172.17.0.2/dvwa/js/>
- <http://172.17.0.2/external/>
- <http://172.17.0.2/external/phpids/>
- <http://172.17.0.2/external/phpids/0.6/>
- <http://172.17.0.2/external/phpids/0.6/docs/>

- <http://172.17.0.2/external/phpids/0.6/docs/examples/>
- <http://172.17.0.2/external/phpids/0.6/docs/examples/example.php>
- <http://172.17.0.2/external/phpids/0.6/docs/phpdocumentor/>
- <http://172.17.0.2/external/phpids/0.6/docs/phpdocumentor/blank.html>
- http://172.17.0.2/external/phpids/0.6/docs/phpdocumentor/classtrees_PHPIDS.html
- <http://172.17.0.2/external/phpids/0.6/docs/phpdocumentor/elementindex.html>
- http://172.17.0.2/external/phpids/0.6/docs/phpdocumentor/elementindex_PHPIDS.html
- http://172.17.0.2/external/phpids/0.6/docs/phpdocumentor/li_PHPIDS.html
- <http://172.17.0.2/external/phpids/0.6/docs/phpdocumentor/packages.html>
- <http://172.17.0.2/external/phpids/0.6/lib/>
- <http://172.17.0.2/external/phpids/0.6/lib/IDS/>
- <http://172.17.0.2/external/phpids/0.6/lib/IDS/Converter.php>
- <http://172.17.0.2/external/phpids/0.6/lib/IDS/Event.php>
- <http://172.17.0.2/external/phpids/0.6/lib/IDS/Filter.php>
- <http://172.17.0.2/external/phpids/0.6/lib/IDS/Init.php>
- <http://172.17.0.2/external/phpids/0.6/lib/IDS/Monitor.php>
- <http://172.17.0.2/external/phpids/0.6/lib/IDS/Report.php>
- <http://172.17.0.2/external/phpids/0.6/tests/>
- <http://172.17.0.2/external/phpids/0.6/tests/IDS/>
- <http://172.17.0.2/external/phpids/0.6/tests/coverage/>
- <http://172.17.0.2/external/phpids/0.6/tests/coverage/> [...]

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: 2023/06/20

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: 2023/07/31

Plugin Output

tcp/0

Information about this scan :

```
Nessus version : 10.5.4
Nessus build : 20013
Plugin feed version : 202308122002
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : debian10-x86-64
Scan type : Normal
Scan name : dvwa :Conduct application vulnerability scan
```



```
Scan policy used : Web Application Tests
Scanner IP : 172.17.0.1
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 121.747 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 : Detected
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2023/8/12 19:15 EDT
Scan duration : 733 sec
Scan for malware : no
```

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 : security
Path : /
Value : impossible
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 1
Port :

Name : PHPSESSID
Path : /
Value : 36v8f04t7c8g8g7v9hoeqa1v74
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 1
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 /login.php :  
password : Possibly a clear or hashed password, vulnerable to sniffing or dictionary attack
```

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://172.17.0.2/config/>
- <http://172.17.0.2/config/config.inc.php>
- <http://172.17.0.2/docs/>
- http://172.17.0.2/docs/DVWA_v1.3.pdf
- <http://172.17.0.2/docs/pdf.html>
- <http://172.17.0.2/dvwa/>
- <http://172.17.0.2/dvwa/css/>
- <http://172.17.0.2/dvwa/css/help.css>
- <http://172.17.0.2/dvwa/css/login.css>
- <http://172.17.0.2/dvwa/css/main.css>
- <http://172.17.0.2/dvwa/css/source.css>
- <http://172.17.0.2/dvwa/images/>
- <http://172.17.0.2/dvwa/images/RandomStorm.png>
- <http://172.17.0.2/dvwa/images/dollar.png>
- <http://172.17.0.2/dvwa/images/lock.png>
- http://172.17.0.2/dvwa/images/login_logo.png
- <http://172.17.0.2/dvwa/images/logo.png>
- <http://172.17.0.2/dvwa/images/spanner.png>
- <http://172.17.0.2/dvwa/images/warning.png>
- <http://172.17.0.2/dvwa/includes/>
- <http://172.17.0.2/dvwa/includes/DBMS/>
- <http://172.17.0.2/dvwa/includes/dvwaPage.inc.php>

```
- http://172.17.0.2/dvwa/includes/dvwaPhpIds.inc.php
- http://172.17.0.2/dvwa/js/
- http://172.17.0.2/dvwa/js/dvwaPage.js
- http://172.17.0.2/external/
- http://172.17.0.2/external/phpids/
- http://172.17.0.2/external/phpids/0.6/
- http://172.17.0.2/external/phpids/0.6/LICENSE
- http://172.17.0.2/external/phpids/0.6/build.xml
- http://172.17.0.2/external/phpids/0.6/docs/
- http://172.17.0.2/external/phpids/0.6/docs/examples/
- http://172.17.0.2/external/phpids/0.6/docs/examples/example.php
- http://172.17.0.2/external/phpids/0.6/docs/phpdocumentor/
- http://172.17.0.2/external/phpids/0.6/docs/phpdocumentor/blank.html
- http://172.17.0.2/external/phpids/0.6/docs/phpdocumentor/classtrees_PHPIDS.html
- http://172.17.0.2/external/phpids/0.6/docs/phpdocumentor/elementindex.html
- http://172.17.0.2/external/phpids/0.6/docs/phpdocumentor/elementindex_PHPIDS.html
- http://172.17.0.2/external/phpids/0.6/docs/phpdocumentor/li_PHPIDS.html
- http://172.17.0.2/external/phpids/0.6/docs/phpdocumentor/packages.html
- http://172.17.0 [...]

```

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:  
/config, /docs, /external, /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
```

Synopsis

The remote web server hosts office-related files.

Description

This plugin connects to the remote web server and attempts to find office-related files such as .doc, .ppt, .xls, .pdf etc.

Solution

Make sure that such files do not contain any confidential or otherwise sensitive information and that they are only accessible to those with valid credentials.

Risk Factor

None

Plugin Information

Published: 2003/03/19, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
The following office-related files are available on the remote server :
```

```
- Adobe Acrobat files (.pdf) :  
  /docs/DVWA_v1.3.pdf
```


Synopsis

The remote web server contains a 'robots.txt' file.

Description

The remote host contains a file named 'robots.txt' that is intended to prevent web 'robots' from visiting certain directories in a website for maintenance or indexing purposes. A malicious user may also be able to use the contents of this file to learn of sensitive documents or directories on the affected site and either retrieve them directly or target them for other attacks.

See Also

<http://www.robotstxt.org/orig.html>

Solution

Review the contents of the site's robots.txt file, use Robots META tags instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive material.

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2018/11/15

Plugin Output

tcp/80/www

```
Contents of robots.txt :
```

```
User-agent: *  
Disallow: /
```

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: 2023/07/17

Plugin Output

tcp/80/www

```
Webmirror performed 108 queries in 43s (2.0511 queries per second)
```

```
The following CGIs have been discovered :
```

```
+ CGI : /login.php
  Methods : POST
  Argument : Login
    Value: Login
  Argument : password
  Argument : user_token
    Value: 2714287d5d622925c3677df342a59891
  Argument : username

+ CGI : /external/phpids/0.6/docs/examples/
  Methods : GET
  Argument : test
    Value: %22><script>eval(window.name)</script>
```

```
Directory index found at /config/
Directory index found at /docs/
Directory index found at /external/
Directory index found at /external/phpids/
Directory index found at /external/recaptcha/
Directory index found at /dvwa/css/
Directory index found at /dvwa/
```

```
Directory index found at /external/phpids/0.6/  
Directory index found at /dvwa/images/  
Directory index found at /dvwa/includes/  
Directory index found at /dvwa/js/  
Directory index found at /external/phpids/0.6/docs/  
Directory index found at /external/phpids/0.6/lib/  
Directory index found at /external/phpids/0.6/tests/  
Directory index found at /dvwa/includes/DBMS/  
Directory index found at /external/phpids/0.6/docs/examples/  
Directory index found at /external/phpids/0.6/lib/IDS/  
Directory index found at /external/phpids/0.6/tests/IDS/
```