Web_App_Scan

Report generated by Nessus™ Wed, 16 Nov 2022 23:46:58 EST

TABLE OF CONTENTS

Vulnerabilities by Host

Compliance 'FAILED'

Compliance 'SKIPPED'

Compliance 'PASSED'

Compliance 'INFO', 'WARNING', 'ERROR'

Remediations

Vulnerabilities by Host

10.10.101.208

0	0	3	1	19
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Wed Nov 16 23:28:19 2022
End time: Wed Nov 16 23:46:58 2022

Host Information

IP: 10.10.101.208
OS: Linux Kernel 2.6

Vulnerabilities

11411 - Backup Files Disclosure

Synopsis

It is possible to retrieve file backups from the remote web server.

Description

By appending various suffixes (ie: .old, .bak, ~, etc...) to the names of various files on the remote host, it seems possible to retrieve their contents, which may result in disclosure of sensitive information.

See Also

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

Solution

Ensure the files do not contain any sensitive information, such as credentials to connect to a database, and delete or protect those files that should not be accessible.

Risk Factor

Medium

CVSS v2.0 Base Score

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

Plugin Information

Published: 2003/03/17, Modified: 2021/01/19

Plugin Output

tcp/80/www

```
It is possible to read the following backup file :

  - File : /config/config.inc.php.bak
    URL  : http://10.10.101.208/config/config.inc.php.bak
```

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://10.10.101.208/config/
http://10.10.101.208/docs/
http://10.10.101.208/dvwa/
http://10.10.101.208/dvwa/css/
http://10.10.101.208/dvwa/images/
http://10.10.101.208/dvwa/includes/
http://10.10.101.208/dvwa/includes/DBMS/
http://10.10.101.208/dvwa/js/
http://10.10.101.208/external/
http://10.10.101.208/external/phpids/
```

```
http://10.10.101.208/external/phpids/0.6/
http://10.10.101.208/external/phpids/0.6/docs/
http://10.10.101.208/external/phpids/0.6/docs/examples/
http://10.10.101.208/external/phpids/0.6/lib/
http://10.10.101.208/external/phpids/0.6/lib/IDS/
http://10.10.101.208/external/phpids/0.6/tests/
http://10.10.101.208/external/phpids/0.6/tests/IDS/
http://10.10.101.208/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://10.10.101.208/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
```

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: 2022/09/08

Plugin Output

tcp/80/www

```
URL        : http://10.10.101.208/
Version    : 2.4.99
Source     : Server: Apache/2.4.25 (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                     : S=60          SP=60          AP=132         SC=12
 AC=156
SQL injection                           : S=120         SP=120         AP=264         SC=24
 AC=312
directory traversal (extended test)     : S=255         SP=255         AP=561         SC=51
 AC=663
SSI injection                           : S=15          SP=15          AP=33          SC=3           AC=39

unseen parameters                       : S=175         SP=175         AP=385         SC=35
 AC=455
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://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)

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 HEAD 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/2.4.25 (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: Thu, 17 Nov 2022 04:35:28 GMT
  Server: Apache/2.4.25 (Debian)
  Expires: Thu, 19 Nov 1981 08:52:00 GMT
  Cache-Control: no-store, no-cache, must-revalidate
  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://10.10.101.208/
HTTP response   : HTTP/1.1 302 Found
Redirect to     : http://10.10.101.208/login.php
Redirect type   : 30x redirect

Final page      : http://10.10.101.208/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://10.10.101.208/config/
  - http://10.10.101.208/config/config.inc.php
  - http://10.10.101.208/docs/
  - http://10.10.101.208/docs/pdf.html
  - http://10.10.101.208/dvwa/
  - http://10.10.101.208/dvwa/css/
  - http://10.10.101.208/dvwa/images/
  - http://10.10.101.208/dvwa/includes/
  - http://10.10.101.208/dvwa/includes/DBMS/
  - http://10.10.101.208/dvwa/includes/dvwaPage.inc.php
  - http://10.10.101.208/dvwa/includes/dvwaPhpIds.inc.php
```

```
- http://10.10.101.208/dvwa/js/
- http://10.10.101.208/external/
- http://10.10.101.208/external/phpids/
- http://10.10.101.208/external/phpids/0.6/
- http://10.10.101.208/external/phpids/0.6/docs/
- http://10.10.101.208/external/phpids/0.6/docs/examples/
- http://10.10.101.208/external/phpids/0.6/docs/examples/example.php
- http://10.10.101.208/external/phpids/0.6/docs/phpdocumentor/
- http://10.10.101.208/external/phpids/0.6/docs/phpdocumentor/blank.html
- http://10.10.101.208/external/phpids/0.6/docs/phpdocumentor/classtrees_PHPIDS.html
- http://10.10.101.208/external/phpids/0.6/docs/phpdocumentor/elementindex.html
- http://10.10.101.208/external/phpids/0.6/docs/phpdocumentor/elementindex_PHPIDS.html
- http://10.10.101.208/external/phpids/0.6/docs/phpdocumentor/li_PHPIDS.html
- http://10.10.101.208/external/phpids/0.6/docs/phpdocumentor/packages.html
- http://10.10.101.208/external/phpids/0.6/lib/
- http://10.10.101.208/external/phpids/0.6/lib/IDS/
- http://10.10.101.208/external/phpids/0.6/lib/IDS/Converter.php
- http://10.10.101.208/external/phpids/0.6/lib/IDS/Event.php
- http://10.10.101.208/external/phpids/0.6/lib/IDS/Filter.php
- http://10.10.101.208/external/phpids/0.6/lib/IDS/Init.php
- http://10.10.101.208/external/phpids/0.6/lib/IDS/Monitor.php
- http://10.10.101.208/external/phpids/0.6/lib/IDS/Report.php
- http://10.10.101.208/external/phpids/0.6/tests/
- http://10.10.101.208/external/phpids/0 [...]
```

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://10.10.101.208/config/
  - http://10.10.101.208/config/config.inc.php
  - http://10.10.101.208/docs/
  - http://10.10.101.208/docs/pdf.html
  - http://10.10.101.208/dvwa/
  - http://10.10.101.208/dvwa/css/
  - http://10.10.101.208/dvwa/images/
  - http://10.10.101.208/dvwa/includes/
  - http://10.10.101.208/dvwa/includes/DBMS/
  - http://10.10.101.208/dvwa/includes/dvwaPage.inc.php
  - http://10.10.101.208/dvwa/includes/dvwaPhpIds.inc.php
  - http://10.10.101.208/dvwa/js/
  - http://10.10.101.208/external/
  - http://10.10.101.208/external/phpids/
  - http://10.10.101.208/external/phpids/0.6/
  - http://10.10.101.208/external/phpids/0.6/docs/
```

```
- http://10.10.101.208/external/phpids/0.6/docs/examples/
- http://10.10.101.208/external/phpids/0.6/docs/examples/example.php
- http://10.10.101.208/external/phpids/0.6/docs/phpdocumentor/
- http://10.10.101.208/external/phpids/0.6/docs/phpdocumentor/blank.html
- http://10.10.101.208/external/phpids/0.6/docs/phpdocumentor/classtrees_PHPIDS.html
- http://10.10.101.208/external/phpids/0.6/docs/phpdocumentor/elementindex.html
- http://10.10.101.208/external/phpids/0.6/docs/phpdocumentor/elementindex_PHPIDS.html
- http://10.10.101.208/external/phpids/0.6/docs/phpdocumentor/li_PHPIDS.html
- http://10.10.101.208/external/phpids/0.6/docs/phpdocumentor/packages.html
- http://10.10.101.208/external/phpids/0.6/lib/
- http://10.10.101.208/external/phpids/0.6/lib/IDS/
- http://10.10.101.208/external/phpids/0.6/lib/IDS/Converter.php
- http://10.10.101.208/external/phpids/0.6/lib/IDS/Event.php
- http://10.10.101.208/external/phpids/0.6/lib/IDS/Filter.php
- http://10.10.101.208/external/phpids/0.6/lib/IDS/Init.php
- http://10.10.101.208/external/phpids/0.6/lib/IDS/Monitor.php
- http://10.10.101.208/external/phpids/0.6/lib/IDS/Report.php
- http://10.10.101.208/external/phpids/0.6/tests/
- http://10.10.101.208/external/phpids/0.6/tests/IDS/
- http:/ [...]
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2022/08/15

Plugin Output

tcp/80/www

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

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.4.1
Nessus build : 20091
Plugin feed version : 202211162347
Scanner edition used : Nessus
Scanner OS : LINUX
Scanner distribution : debian9-x86-64
Scan type : Normal
Scan name : Web_App_Scan
```

```
Scan policy used : Web Application Tests
Scanner IP : 10.9.19.48
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 121.891 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
Scan Start Date : 2022/11/16 23:28 EST
Scan duration : 1118 sec
```

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


Name : PHPSESSID
Path : /
Value : g0m97e9off92n0pav09a1e4rd0
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 : security
Path : /
Value : low
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


Name : PHPSESSID
Path : /
Value : g0m97e9off92n0pav09a1e4rd0
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 /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://10.10.101.208/config/
  - http://10.10.101.208/config/config.inc.php
  - http://10.10.101.208/config/config.inc.php.bak
  - http://10.10.101.208/config/config.inc.php.dist
  - http://10.10.101.208/docs/
  - http://10.10.101.208/docs/DVWA_v1.3.pdf
  - http://10.10.101.208/docs/pdf.html
  - http://10.10.101.208/dvwa/
  - http://10.10.101.208/dvwa/css/
  - http://10.10.101.208/dvwa/css/help.css
  - http://10.10.101.208/dvwa/css/login.css
  - http://10.10.101.208/dvwa/css/main.css
  - http://10.10.101.208/dvwa/css/source.css
  - http://10.10.101.208/dvwa/images/
  - http://10.10.101.208/dvwa/images/RandomStorm.png
  - http://10.10.101.208/dvwa/images/dollar.png
  - http://10.10.101.208/dvwa/images/lock.png
  - http://10.10.101.208/dvwa/images/login_logo.png
  - http://10.10.101.208/dvwa/images/logo.png
  - http://10.10.101.208/dvwa/images/spanner.png
  - http://10.10.101.208/dvwa/images/warning.png
  - http://10.10.101.208/dvwa/includes/
```

```
- http://10.10.101.208/dvwa/includes/DBMS/
- http://10.10.101.208/dvwa/includes/dvwaPage.inc.php
- http://10.10.101.208/dvwa/includes/dvwaPhpIds.inc.php
- http://10.10.101.208/dvwa/js/
- http://10.10.101.208/dvwa/js/add_event_listeners.js
- http://10.10.101.208/dvwa/js/dvwaPage.js
- http://10.10.101.208/external/
- http://10.10.101.208/external/phpids/
- http://10.10.101.208/external/phpids/0.6/
- http://10.10.101.208/external/phpids/0.6/LICENSE
- http://10.10.101.208/external/phpids/0.6/build.xml
- http://10.10.101.208/external/phpids/0.6/docs/
- http://10.10.101.208/external/phpids/0.6/docs/examples/
- http://10.10.101.208/external/phpids/0.6/docs/examples/example.php
- http://10.10.101.208/external/phpids/0.6/docs/phpdocumentor/
- http://10.10.101.208/external/phpids/0.6/docs/phpdocumentor/blank.html
- http://10.10.101.208/external/phpids/0.6/docs/phpdocumentor/classtrees_PHPIDS.html
- http://10.10.101.208/external/phpids/0.6/docs/phpdocumentor/elem [...]
```

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
```

11419 - Web Server Office File Inventory

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
```

10302 - Web Server robots.txt Information Disclosure

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: 2022/08/15

Plugin Output

tcp/80/www

```
Webmirror performed 111 queries in 89s (1.0247 queries per second)

The following CGIs have been discovered :


+ CGI : /login.php
  Methods : POST
  Argument : Login
   Value: Login
  Argument : password
  Argument : user_token
   Value: 50ebb33e8d4cc093aa3be52dc6d2d8e0
  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/
```

Compliance 'FAILED'

Compliance 'SKIPPED'

Compliance 'PASSED'

Compliance 'INFO', 'WARNING', 'ERROR'

Remediations

Suggested Remediations