PCI-DSS-SCAN_2

Report generated by Nessus™ Thu, 17 Nov 2022 20:44:29 EST

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

10.10.26.84

1	2	9	1	34
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Thu Nov 17 20:09:35 2022
End time:	Thu Nov 17 20:44:29 2022

Host Information

IP:	10.10.26.84
OS:	Linux Kernel 2.6

Vulnerabilities

161948 - Apache 2.4.x < 2.4.54 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.54. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.54 advisory.

- Possible request smuggling in mod_proxy_ajp: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions. Acknowledgements: Ricter Z @ 360 Noah Lab (CVE-2022-26377)

- Read beyond bounds in mod_isapi: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module. Acknowledgements: The Apache HTTP Server project would like to thank Ronald Crane (Zippenhop LLC) for reporting this issue (CVE-2022-28330)

- Read beyond bounds via ap_rwrite(): The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Acknowledgements: The Apache HTTP Server project would like to thank Ronald Crane (Zippenhop LLC) for reporting this issue (CVE-2022-28614)

- Read beyond bounds in ap_strcmp_match(): Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected. Acknowledgements: The Apache HTTP Server project would like to thank Ronald Crane (Zippenhop LLC) for reporting this issue (CVE-2022-28615)

- Denial of service in mod_lua r:parsebody: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size. Acknowledgements: The Apache HTTP Server project would like to thank Ronald Crane (Zippenhop LLC) for reporting this issue (CVE-2022-29404)

- Denial of Service mod_sed: If Apache HTTP Server 2.4.53 is configured to do transformations with mod_sed in contexts where the input to mod_sed may be very large, mod_sed may make excessively large memory allocations and trigger an abort. Acknowledgements: This issue was found by Brian Moussalli from the JFrog Security Research team (CVE-2022-30522)

- Information Disclosure in mod_lua with websockets: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.

Acknowledgements: The Apache HTTP Server project would like to thank Ronald Crane (Zippenhop LLC) for reporting this issue (CVE-2022-30556)

- X-Forwarded-For dropped by hop-by-hop mechanism in mod_proxy: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.

Acknowledgements: The Apache HTTP Server project would like to thank Gaetan Ferry (Synacktiv) for reporting this issue (CVE-2022-31813)

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

See Also

https://httpd.apache.org/security/vulnerabilities_24.html

Solution

Upgrade to Apache version 2.4.54 or later.

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)

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)

STIG Severity

I

References

CVE	CVE-2022-26377
CVE	CVE-2022-28330
CVE	CVE-2022-28614
CVE	CVE-2022-28615
CVE	CVE-2022-29404
CVE	CVE-2022-30522
CVE	CVE-2022-30556
CVE	CVE-2022-31813
XREF	IAVA:2022-A-0230

Plugin Information

Published: 2022/06/08, Modified: 2022/06/20

Plugin Output

tcp/80/www

```
  URL               : http://10.10.26.84/
  Installed version : 2.4.25
  Fixed version     : 2.4.54
```

17693 - Apache mod_suexec Multiple Privilege Escalation Vulnerabilities

Synopsis

The remote Apache server is vulnerable to multiple privilege escalation attacks.

Description

The remote host appears to be running Apache and is potentially affected by the following vulnerabilities:

- Multiple race conditions exist in suexec between the validation and usage of directories and files. Under certain conditions local users are able to escalate privileges and execute arbitrary code through the renaming of directories or symlink attacks.

(CVE-2007-1741)

- Apache's suexec module only performs partial comparisons on paths, which could result in privilege escalation. (CVE-2007-1742)

- Apache's suexec module does not properly verify user and group IDs on the command line. When the '/
proc'

filesystem is mounted, a local user can utilize suexec to escalate privileges. (CVE-2007-1743)

Note that this plugin only checks for the presence of Apache, and does not actually check the configuration.

See Also

https://marc.info/?l=apache-httpd-dev&m=117511568709063&w=2

https://marc.info/?l=apache-httpd-dev&m=117511834512138&w=2

Solution

Disable suexec or disallow users from writing to the document root.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	23438
CVE	CVE-2007-1741
CVE	CVE-2007-1742
CVE	CVE-2007-1743

Plugin Information

Published: 2011/11/18, Modified: 2018/11/15

Plugin Output

tcp/80/www

```
Version source    : Server: Apache/2.4.25 (Debian)
Installed version : 2.4.25
```

33929 - PCI DSS compliance

Synopsis

The remote host has been found to be NOT COMPLIANT with the PCI DSS external scanning requirements.

Description

The remote host is vulnerable to one or more conditions that are considered to be 'automatic failures' according to the PCI DSS Approved Scanning Vendors Program Guide (version 3.1). These failures include one or more of the following :

- Vulnerabilities with a CVSS base score greater than or equal to 4.0

- Unsupported operating systems

- Internet reachable database servers (must validate whether cardholder data is stored)

- Presence of built-in or default accounts

- Unrestricted DNS Zone transfers

- Unvalidated parameters leading to SQL injection attacks

- Cross-Site Scripting (XSS) flaws

- Directory traversal vulnerabilities

- HTTP response splitting/header injection

- Detection of backdoor applications (malware, trojan horses, rootkits, backdoors)

- Use of older, insecure SSL/TLS versions (TLS v1.2 is the minimum standard)

- Use of anonymous key exchange protocols (such as anonymous Diffie-Hellman in SSL/TLS)

- Scan Interference

Details of the failed items may be found in the 'Output' section of this plugin result. These vulnerabilities and/or failure conditions will have to be corrected before you are able to submit your scan results for validation by Tenable to meet your quarterly external scanning requirements.

If you are conducting this scan via Tenable.io and either disagree with any of the results, believe there are false-positives, or must rely on compensating controls to mitigate the vulnerability then you may proceed with submitting this report to our PCI-ASV Workbench by clicking on 'Submit for PCI'. You may login to the Tenable PCI-ASV Workbench in Tenable.io and dispute or provide mitigation evidence for each of the residual findings.

See Also

https://www.pcisecuritystandards.org

Risk Factor

High

Plugin Information

Published: 2008/08/07, Modified: 2022/08/15

Plugin Output

tcp/0

```
+ Directory browsing is enabled on some web servers.
  http://10.10.26.84/config/
  http://10.10.26.84/dvwa/
  http://10.10.26.84/external/phpids/0.6/
  http://10.10.26.84/dvwa/images/
  http://10.10.26.84/dvwa/includes/
  http://10.10.26.84/dvwa/js/
  http://10.10.26.84/external/phpids/0.6/tests/IDS/
  http://10.10.26.84/external/phpids/0.6/docs/examples/cakephp/
  http://10.10.26.84/external/phpids/0.6/lib/IDS/Caching/
  http://10.10.26.84/external/phpids/0.6/lib/IDS/Config/
  http://10.10.26.84/external/phpids/0.6/lib/IDS/Filter/
  http://10.10.26.84/external/phpids/0.6/lib/IDS/Log/
  http://10.10.26.84/external/phpids/0.6/docs/phpdocumentor/PHPIDS/
  http://10.10.26.84/external/phpids/0.6/docs/phpdocumentor/media/
  http://10.10.26.84/external/phpids/0.6/lib/IDS/vendors/htmlpurifier/
  http://10.10.26.84/external/phpids/0.6/lib/IDS/vendors/
  http://10.10.26.84/external/phpids/0.6/lib/IDS/tmp/
  http://10.10.26.84/external/phpids/0.6/lib/IDS/
  http://10.10.26.84/external/phpids/0.6/docs/examples/
  http://10.10.26.84/dvwa/includes/DBMS/
  http://10.10.26.84/external/phpids/0.6/tests/
  http://10.10.26.84/external/phpids/0.6/lib/
  http://10.10.26.84/external/phpids/0.6/docs/
  http://10.10.26.84/dvwa/css/
  http://10.10.26.84/external/recaptcha/
  http://10.10.26.84/external/phpids/
  http://10.10.26.84/external/
  http://10.10.26.84/docs/
+ 9 high risk flaws were found. See :
   http://www.nessus.org/plugins/index.php?view=single&id=161948
   http://www.nessus.org/plugins/index.php?view=single&id=153584
   http://www.nessus.org/plugins/index.php?view=single&id=100995
   http://www.nessus.org/plugins/index.php?view=single&id=156255
   http://www.nessus.org/plugins/index.php?view=single&id=139574
   http://www.nessus.org/plugins/index.php?view=single&id=123642
   http://www.nessus.org/plugins/index.php?view=single&id=161454
   http://www.nessus.org/plugins/index.php?view=single&id=158900
   http://www.nessus.org/plugins/index.php?view=single&id=150280
+ 18 medium risk flaws were found. See :
   http://www.ness [...]
```

17695 - Apache Mixed Platform AddType Directive Information Disclosure

Synopsis

The remote Apache server is vulnerable to an information disclosure attack.

Description

The remote host appears to be running Apache. When Apache runs on a Unix host with a document root on a Windows SMB share, remote, unauthenticated attackers could obtain the unprocessed contents of the directory. For example, requesting a PHP file with a trailing backslash could display the file's source instead of executing it.

See Also

http://www.nessus.org/u?eb25db1c

Solution

Ensure that the document root is not located on a Windows SMB share.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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

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

References

BID	26939
CVE	CVE-2007-6514
XREF	CWE:200

Plugin Information

Published: 2011/11/18, Modified: 2018/11/15

Plugin Output

tcp/80/www

```
  Version source    : Server: Apache/2.4.25 (Debian)
  Installed version : 2.4.25
```

106232 - Apache ServerTokens Information Disclosure

Synopsis

The remote web server discloses information via HTTP headers.

Description

The HTTP headers sent by the remote web server disclose information that can aid an attacker, such as the server version, operating system, and module versions.

See Also

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

Solution

Change the Apache ServerTokens configuration value to 'Prod'

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: 2018/01/22, Modified: 2020/04/22

Plugin Output

tcp/80/www

```
The Apache server listening on port 80 contains
sensitive information in the HTTP Server field.

Server: Apache/2.4.25 (Debian)
```

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://10.10.26.84/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://10.10.26.84/config/
http://10.10.26.84/docs/
http://10.10.26.84/dvwa/
http://10.10.26.84/dvwa/css/
http://10.10.26.84/dvwa/images/
http://10.10.26.84/dvwa/includes/
http://10.10.26.84/dvwa/includes/DBMS/
http://10.10.26.84/dvwa/js/
http://10.10.26.84/external/
http://10.10.26.84/external/phpids/
```

```
http://10.10.26.84/external/phpids/0.6/
http://10.10.26.84/external/phpids/0.6/docs/
http://10.10.26.84/external/phpids/0.6/docs/examples/
http://10.10.26.84/external/phpids/0.6/docs/examples/cakephp/
http://10.10.26.84/external/phpids/0.6/docs/phpdocumentor/PHPIDS/
http://10.10.26.84/external/phpids/0.6/docs/phpdocumentor/media/
http://10.10.26.84/external/phpids/0.6/lib/
http://10.10.26.84/external/phpids/0.6/lib/IDS/
http://10.10.26.84/external/phpids/0.6/lib/IDS/Caching/
http://10.10.26.84/external/phpids/0.6/lib/IDS/Config/
http://10.10.26.84/external/phpids/0.6/lib/IDS/Filter/
http://10.10.26.84/external/phpids/0.6/lib/IDS/Log/
http://10.10.26.84/external/phpids/0.6/lib/IDS/tmp/
http://10.10.26.84/external/phpids/0.6/lib/IDS/vendors/
http://10.10.26.84/external/phpids/0.6/lib/IDS/vendors/htmlpurifier/
http://10.10.26.84/external/phpids/0.6/tests/
http://10.10.26.84/external/phpids/0.6/tests/IDS/
http://10.10.26.84/external/recaptcha/
```

56208 - PCI DSS Compliance : Insecure Communication Has Been Detected

Synopsis

An insecure port, protocol, or service has been detected.

Description

Applications that fail to adequately encrypt network traffic using strong cryptography are at increased risk of being compromised and exposing cardholder data. An attacker who is able to exploit weak cryptographic processes can gain control of an application or even gain cleartext access to encrypted data.

Solution

Properly encrypt all authenticated and sensitive communications.

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: 2011/09/15, Modified: 2020/04/22

Plugin Output

tcp/80/www

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

121041 - Sensitive File Disclosure

Synopsis

The web application hosts static files that may be sensitive in nature.

Description

The remote web application hosts documents or office files that may contain sensitive information.

Solution

Static files that are not necessary should be removed from the web root. If documents are required to be in the web root, and are sensitive in nature, they should require authentication.

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: 2019/01/09, Modified: 2022/08/15

Plugin Output

tcp/80/www

```
The following URLs are potentially sensitive documents :

  /docs/DVWA_v1.3.pdf
```

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://10.10.26.84/login.php
```

88490 - Web Server Error Page Information Disclosure

Synopsis

The remote web server discloses information via a default error page.

Description

The default error page sent by the remote web server discloses information that can aid an attacker, such as the server version and languages used by the web server.

Solution

Modify the web server to not disclose detailed information about the underlying web server, or use a custom error page instead.

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: 2016/01/29, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
  Server Type    : Apache
  Server Version : Apache/2.4.25
  Source         : http://10.10.26.84/Pf_py812
```

88099 - Web Server HTTP Header Information Disclosure

Synopsis

The remote web server discloses information via HTTP headers.

Description

The HTTP headers sent by the remote web server disclose information that can aid an attacker, such as the server version and languages used by the web server.

Solution

Modify the HTTP headers of the web server to not disclose detailed information about the underlying web server.

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: 2016/01/22, Modified: 2019/04/30

Plugin Output

tcp/80/www

```
Server type     : Apache
Server version  : 2.4.25
Source          : 2.4.25
```

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
```

111465 - Apache HTTP Server Error Page Detection

Synopsis

The remote web server version can be obtained via a default error page.

Description

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

See Also

https://httpd.apache.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/07/31, Modified: 2022/08/15

Plugin Output

tcp/80/www

```
Version : 2.4.25
Source  : Apache/2.4.25 (Debian)
URL     : http://10.10.26.84/mail/
```

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://10.10.26.84/
  Version    : 2.4.25
  Source     : Server: Apache/2.4.25 (Debian)
  backported : 0
  os         : Debian
```

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=85         SP=85        AP=187       SC=17
 AC=221
injectable parameter                     : S=10         SP=10        AP=22        SC=2         AC=26

arbitrary command execution              : S=110        SP=110       AP=242       SC=22
 AC=286
local file inclusion                     : S=20         SP=20        AP=44        SC=4         AC=52

directory traversal                      : S=145        SP=145       AP=319       SC=29
 AC=377
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=140        SP=140       AP=308       SC=28
 AC=364
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)              [...]
```

45590 - Common Platform Enumeration (CPE)

Synopsis

It was possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/

https://nvd.nist.gov/products/cpe

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2022/11/15

Plugin Output

tcp/0

```

The remote operating system matched the following CPE :

  cpe:/o:linux:linux_kernel -> Linux Kernel

Following application CPE matched on the remote system :

  cpe:/a:apache:http_server:2.4.25 -> Apache Software Foundation Apache HTTP Server
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/05/23, Modified: 2022/09/09

Plugin Output

tcp/0

```
Remote device type : general-purpose
Confidence level : 65
```

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

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


http://php-ids.org/                     - /external/phpids/0.6/docs/phpdocumentor/PHPIDS/
IDS_Caching_Interface.html
http://www.dvwa.co.uk/                  - /login.php
http://www.gnu.org/licenses/lgpl.html   - /external/phpids/0.6/docs/phpdocumentor/PHPIDS/
IDS_Caching_Interface.html
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/examples/cakephp
    /external/phpids/0.6/docs/phpdocumentor
    /external/phpids/0.6/docs/phpdocumentor/PHPIDS
    /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/examples/cakephp
    /external/phpids/0.6/docs/phpdocumentor
    /external/phpids/0.6/docs/phpdocumentor/PHPIDS
    /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: Fri, 18 Nov 2022 01:27:56 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://10.10.26.84/
  HTTP response    : HTTP/1.1 302 Found
  Redirect to      : http://10.10.26.84/login.php
  Redirect type    : 30x redirect

  Final page       : http://10.10.26.84/login.php
  HTTP response    : HTTP/1.1 200 OK
```

10114 - ICMP Timestamp Request Remote Date Disclosure

Synopsis

It is possible to determine the exact time set on the remote host.

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

None

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0524
XREF	CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2019/10/04

Plugin Output

icmp/0

```
The remote clock is synchronized with the local clock.
```

14788 - IP Protocols Scan

Synopsis

This plugin detects the protocols understood by the remote IP stack.

Description

This plugin detects the protocols understood by the remote IP stack.

See Also

http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/09/22, Modified: 2022/08/15

Plugin Output

tcp/0

```
The following IP protocols are accepted on this host:
1ICMP
2IGMP
6TCP
17UDP
41IPv6
58IPv6-ICMP
103PIM
136UDPLite
```

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://10.10.26.84/config/
  - http://10.10.26.84/config/?C=D%3BO=A
  - http://10.10.26.84/config/?C=M%3BO=A
  - http://10.10.26.84/config/?C=N%3BO=D
  - http://10.10.26.84/config/?C=S%3BO=A
  - http://10.10.26.84/config/config.inc.php
  - http://10.10.26.84/docs/
  - http://10.10.26.84/docs/?C=D%3BO=A
  - http://10.10.26.84/docs/?C=M%3BO=A
  - http://10.10.26.84/docs/?C=N%3BO=D
  - http://10.10.26.84/docs/?C=S%3BO=A
```

```
    - http://10.10.26.84/docs/pdf.html
    - http://10.10.26.84/dvwa/
    - http://10.10.26.84/dvwa/?C=D%3BO=A
    - http://10.10.26.84/dvwa/?C=M%3BO=A
    - http://10.10.26.84/dvwa/?C=N%3BO=D
    - http://10.10.26.84/dvwa/?C=S%3BO=A
    - http://10.10.26.84/dvwa/css/
    - http://10.10.26.84/dvwa/css/?C=D%3BO=A
    - http://10.10.26.84/dvwa/css/?C=M%3BO=A
    - http://10.10.26.84/dvwa/css/?C=N%3BO=D
    - http://10.10.26.84/dvwa/css/?C=S%3BO=A
    - http://10.10.26.84/dvwa/images/
    - http://10.10.26.84/dvwa/images/?C=D%3BO=A
    - http://10.10.26.84/dvwa/images/?C=M%3BO=A
    - http://10.10.26.84/dvwa/images/?C=N%3BO=D
    - http://10.10.26.84/dvwa/images/?C=S%3BO=A
    - http://10.10.26.84/dvwa/includes/
    - http://10.10.26.84/dvwa/includes/?C=D%3BO=A
    - http://10.10.26.84/dvwa/includes/?C=M%3BO=A
    - http://10.10.26.84/dvwa/includes/?C=N%3BO=D
    - http://10.10.26.84/dvwa/includes/?C=S%3BO=A
    - http://10.10.26.84/dvwa/includes/DBMS/
    - http://10.10.26.84/dvwa/includes/DBMS/?C=D%3BO=A
    - http://10.10.26.84/dvwa/includes/DBMS/?C=M%3BO=A
    - http://10.10.26.84/dvwa/includes/DBMS/?C=N%3BO=D
    - http://10.10.26.84/dvwa/includes/DBMS/?C=S%3BO=A
    - http://10.10.26.84/dvwa/includes/dvwaPage.inc.php
    - http://10.10.26.84/dvwa/includes/dvwaPhpIds.inc.php
    - http://10.10.26.84/dvwa/js/
    - http://10.10.26.84/dvwa/js/?C=D%3BO=A
    - http://10.10.26.84/dvwa/js/?C=M%3BO=A
    - http://10.10.26.84/dvwa/js/?C=N%3BO=D
    - http://10.10.26.84/dvwa/js/?C=S%3BO=A
    - http://10.10.26.84/external/
    - http://10.10.26.84/externa [...]
```

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://10.10.26.84/config/
  - http://10.10.26.84/config/?C=D%3BO=A
  - http://10.10.26.84/config/?C=M%3BO=A
  - http://10.10.26.84/config/?C=N%3BO=D
  - http://10.10.26.84/config/?C=S%3BO=A
  - http://10.10.26.84/config/config.inc.php
  - http://10.10.26.84/docs/
  - http://10.10.26.84/docs/?C=D%3BO=A
  - http://10.10.26.84/docs/?C=M%3BO=A
  - http://10.10.26.84/docs/?C=N%3BO=D
  - http://10.10.26.84/docs/?C=S%3BO=A
  - http://10.10.26.84/docs/pdf.html
  - http://10.10.26.84/dvwa/
  - http://10.10.26.84/dvwa/?C=D%3BO=A
  - http://10.10.26.84/dvwa/?C=M%3BO=A
  - http://10.10.26.84/dvwa/?C=N%3BO=D
```

```
    - http://10.10.26.84/dvwa/?C=S%3BO=A
    - http://10.10.26.84/dvwa/css/
    - http://10.10.26.84/dvwa/css/?C=D%3BO=A
    - http://10.10.26.84/dvwa/css/?C=M%3BO=A
    - http://10.10.26.84/dvwa/css/?C=N%3BO=D
    - http://10.10.26.84/dvwa/css/?C=S%3BO=A
    - http://10.10.26.84/dvwa/images/
    - http://10.10.26.84/dvwa/images/?C=D%3BO=A
    - http://10.10.26.84/dvwa/images/?C=M%3BO=A
    - http://10.10.26.84/dvwa/images/?C=N%3BO=D
    - http://10.10.26.84/dvwa/images/?C=S%3BO=A
    - http://10.10.26.84/dvwa/includes/
    - http://10.10.26.84/dvwa/includes/?C=D%3BO=A
    - http://10.10.26.84/dvwa/includes/?C=M%3BO=A
    - http://10.10.26.84/dvwa/includes/?C=N%3BO=D
    - http://10.10.26.84/dvwa/includes/?C=S%3BO=A
    - http://10.10.26.84/dvwa/includes/DBMS/
    - http://10.10.26.84/dvwa/includes/DBMS/?C=D%3BO=A
    - http://10.10.26.84/dvwa/includes/DBMS/?C=M%3BO=A
    - http://10.10.26.84/dvwa/includes/DBMS/?C=N%3BO=D
    - http://10.10.26.84/dvwa/includes/DBMS/?C=S%3BO=A
    - http://10.10.26.84/dvwa/includes/dvwaPage.inc.php
    - http://10.10.26.84/dvwa/includes/dvwaPhpIds.inc.php
    - http://10.10.26.84/dvwa/js/
    - http://10.10.26.84/dvwa/js/?C=D%3BO=A
    - http://10.10.26.84/dvwa/js/?C=M%3BO=A
    - http://10.10.26.84/dvwa/js/?C=N%3BO=D
    - http://10.10.26.84/dvwa/js/?C=S%3BO=A
    - http://10.10.26.84/external/
    - http://10.10.26.84/external/?C=D%3BO=A
    - 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 : PCI-DSS-SCAN_2
Scan policy used : PCI Quarterly External Scan
Scanner IP : 10.9.19.48
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Ping RTT : 121.178 ms
Thorough tests : yes
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 2
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : no (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 : 20
Max checks : 4
Recv timeout : 15
Backports : None
Allow post-scan editing : No
Scan Start Date : 2022/11/17 20:09 EST
Scan duration : 2088 sec
```

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2022/03/09

Plugin Output

tcp/0

```

Remote operating system : Linux Kernel 2.6
Confidence level : 65
Method : SinFP


The remote host is running Linux Kernel 2.6
```

124761 - PCI DSS Compliance - Information Leakage

Synopsis

The remote host has been found to be COMPLIANT with the PCI DSS external scanning requirements.

Description

The remote host is vulnerable to one or more conditions that are considered to be 'information leakage' and so are not automatic failures according to the PCI DSS Approved Scanning Vendors Program Guide (version 3.1). These information leakage issues include one or more of the following :

- Detailed application error messages

- Backup script files (for example,home.asp.bak, index.jsp.old, etc.)

- Include file source code disclosure

- Insecure HTTP methods enabled

- WebDAV or FrontPage extensions enabled

- Default web server files

- Testing and diagnostics pages (for example,phpinfo.html, test-cgi, etc.

Details of the failed items may be found in the 'Output' section of this plugin result.

See Also

https://www.pcisecuritystandards.org

Risk Factor

None

Plugin Information

Published: 2019/05/10, Modified: 2022/08/15

Plugin Output

tcp/0

```
+ Backup script files have been found.
+ A web server is vulnerable to insecure http methods enabled
```

124761 - PCI DSS Compliance - Information Leakage

Synopsis

The remote host has been found to be COMPLIANT with the PCI DSS external scanning requirements.

Description

The remote host is vulnerable to one or more conditions that are considered to be 'information leakage' and so are not automatic failures according to the PCI DSS Approved Scanning Vendors Program Guide (version 3.1). These information leakage issues include one or more of the following :

- Detailed application error messages

- Backup script files (for example,home.asp.bak, index.jsp.old, etc.)

- Include file source code disclosure

- Insecure HTTP methods enabled

- WebDAV or FrontPage extensions enabled

- Default web server files

- Testing and diagnostics pages (for example,phpinfo.html, test-cgi, etc.

Details of the failed items may be found in the 'Output' section of this plugin result.

See Also

https://www.pcisecuritystandards.org

Risk Factor

None

Plugin Information

Published: 2019/05/10, Modified: 2022/08/15

Plugin Output

tcp/80/www

```
The remote web server is vulnerable to insecure http methods enabled
```

60020 - PCI DSS Compliance : Handling False Positives

Synopsis

Notes the proper handling of false positives in PCI DSS scans.

Description

Note that per PCI Security Standards Council (PCI SSC) standards, if the version of the remote software is known to contain flaws, a vulnerability scanner must report it as vulnerable. The scanner must still flag it as vulnerable, even in cases where a workaround or mitigating configuration option is in place. This will result in the scanner issuing false positives by PCI SSC design.

It is recommended that any workarounds and mitigating configurations that are in place be documented including technical details, to be presented to a third-party PCI auditor during an audit.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2012/07/18, Modified: 2019/04/04

Plugin Output

tcp/0

40472 - PCI DSS compliance : options settings

Synopsis

Reports options used in a PCI DSS compliance test.

Description

This plugin reports the values of a few important scan settings if PCI DSS compliance checks are enabled. These scan settings are preset based on the scan template you have selected, but in some cases may be overriden.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/08/03, Modified: 2019/06/12

Plugin Output

tcp/0

```
An External PCI scan has been selected.  Local checks will not be performed.

These settings are required to test cross-site scripting and SQL injection flaws:
Web applications tests are enabled.
CGI scanning is enabled.

The timeout for web application tests is 300 seconds.
```

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: 2022/11/08

Plugin Output

tcp/0

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

[ Apache 2.4.x < 2.4.54 Multiple Vulnerabilities (161948) ]

+ Action to take : Upgrade to Apache version 2.4.54 or later.

+Impact : Taking this action will resolve 55 different vulnerabilities (CVEs).
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2022/07/26

Plugin Output

tcp/80/www

```
A web server is running on this port.
```

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

http://www.ietf.org/rfc/rfc1323.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/03/06

Plugin Output

tcp/0

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2020/08/20

Plugin Output

udp/0

```
For your information, here is the traceroute from 10.9.19.48 to 10.10.26.84 :
10.9.19.48
10.9.0.1
?
10.10.26.84

Hop Count: 3
```

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 : 62eub2m2f2mh5ropth4ojqfv52
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 : 62eub2m2f2mh5ropth4ojqfv52
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://10.10.26.84/config/
  - http://10.10.26.84/config/config.inc.php
  - http://10.10.26.84/config/config.inc.php.bak
  - http://10.10.26.84/config/config.inc.php.dist
  - http://10.10.26.84/docs/
  - http://10.10.26.84/docs/DVWA_v1.3.pdf
  - http://10.10.26.84/docs/pdf.html
  - http://10.10.26.84/dvwa/
  - http://10.10.26.84/dvwa/css/
  - http://10.10.26.84/dvwa/css/help.css
  - http://10.10.26.84/dvwa/css/login.css
  - http://10.10.26.84/dvwa/css/main.css
  - http://10.10.26.84/dvwa/css/source.css
  - http://10.10.26.84/dvwa/images/
  - http://10.10.26.84/dvwa/images/RandomStorm.png
  - http://10.10.26.84/dvwa/images/dollar.png
  - http://10.10.26.84/dvwa/images/lock.png
  - http://10.10.26.84/dvwa/images/login_logo.png
  - http://10.10.26.84/dvwa/images/logo.png
  - http://10.10.26.84/dvwa/images/spanner.png
  - http://10.10.26.84/dvwa/images/warning.png
  - http://10.10.26.84/dvwa/includes/
  - http://10.10.26.84/dvwa/includes/DBMS/
  - http://10.10.26.84/dvwa/includes/dvwaPage.inc.php
  - http://10.10.26.84/dvwa/includes/dvwaPhpIds.inc.php
  - http://10.10.26.84/dvwa/js/
  - http://10.10.26.84/dvwa/js/add_event_listeners.js
  - http://10.10.26.84/dvwa/js/dvwaPage.js
  - http://10.10.26.84/external/
  - http://10.10.26.84/external/phpids/
  - http://10.10.26.84/external/phpids/0.6/
  - http://10.10.26.84/external/phpids/0.6/LICENSE
  - http://10.10.26.84/external/phpids/0.6/build.xml
  - http://10.10.26.84/external/phpids/0.6/docs/
  - http://10.10.26.84/external/phpids/0.6/docs/examples/
  - http://10.10.26.84/external/phpids/0.6/docs/examples/?test=%22%3E%3Cscript
%3Eeval(window.name)%3C/script%3E
  - http://10.10.26.84/external/phpids/0.6/docs/examples/cakephp/
  - http://10.10.26.84/external/phpids/0.6/docs/examples/cakephp/README
  - http://10.10.26.84/external/phpids/0.6/docs/examples/example.php
  - http://10.10.26.84/external/phpids/0.6/docs/phpdocumentor/
  - http://10.10.26.84/external/phpids/0.6/docs/phpdoc [...]
```

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
```

49705 - Web Server Harvested Email Addresses

Synopsis

Email addresses were harvested from the web server.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/80/www

```
The following email addresses have been gathered :


- 'ch0012@gmail.com', referenced from :
   /external/phpids/0.6/docs/phpdocumentor/PHPIDS/_Caching---Database.php.html
   /external/phpids/0.6/docs/phpdocumentor/PHPIDS/_Caching---File.php.html
   /external/phpids/0.6/docs/phpdocumentor/PHPIDS/_Log---Interface.php.html
   /external/phpids/0.6/docs/phpdocumentor/PHPIDS/IDS_Monitor.html
   /external/phpids/0.6/docs/phpdocumentor/PHPIDS/IDS_Log_Email.html
   /external/phpids/0.6/docs/phpdocumentor/PHPIDS/IDS_Log_Database.html
   /external/phpids/0.6/docs/phpdocumentor/PHPIDS/_Filter.php.html
   /external/phpids/0.6/docs/phpdocumentor/PHPIDS/_Caching---Memcached.php.html
   /external/phpids/0.6/docs/phpdocumentor/PHPIDS/IDS_Filter_Storage_Abstract.html
   /external/phpids/0.6/docs/phpdocumentor/PHPIDS/IDS_Log_Interface.html
   /external/phpids/0.6/docs/phpdocumentor/PHPIDS/IDS_Filter.html
   /external/phpids/0.6/docs/phpdocumentor/PHPIDS/IDS_Caching_Database.html
   /external/phpids/0.6/docs/phpdocumentor/PHPIDS/_Caching---Interface.php.html
   /external/phpids/0.6/docs/phpdocumentor/PHPIDS/IDS_Caching_Session.html
   /external/phpids/0.6/docs/phpdocumentor/PHPIDS/IDS_Init.html
   /external/phpids/0.6/docs/phpdocumentor/PHPIDS/_Init.php.html
   /external/phpids/0.6/docs/phpdocumentor/PHPIDS/IDS_Report.html
   /external/phpids/0.6/docs/phpdocumentor/PHPIDS/IDS_Caching_File.html
   /external/phpids/0.6/docs/phpdocumentor/PHPIDS/IDS_Caching_Memcached.html
   /external/phpids/0.6/docs/phpdocumentor/PHPIDS/IDS_Event.html
   /external/phpids/0.6/docs/phpdocumentor/PHPIDS/IDS_Log_File.html
   /external/phpids/0.6/docs/phpdocumentor/PHPIDS/_Filter---Storage.php.html
   /external/phpids/0.6/docs/phpdocumentor/PHPIDS/_Log---File.php.html
   /external/phpids/0.6/docs/phpdocumentor/PHPIDS/IDS_Log_Composite.html
   /external/phpids/0.6/docs/phpdocumentor/PHPIDS/_Converter.php.html
   /external/phpids/0.6/docs/phpdocumentor/PHPIDS/_Event.php.html
```

```
    /external/phpids/0.6/docs/phpdocumentor/PHPIDS/_Report.php.html
    /external/ph [...]
```

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 737 queries in 402s (1.0833 queries per second)

The following CGIs have been discovered :


+ CGI : /login.php
  Methods : POST
  Argument : Login
   Value: Login
  Argument : password
  Argument : user_token
   Value: 7c80cd5c4f08792547a709137dfde005
  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/
  Directory index found at /external/phpids/0.6/docs/examples/cakephp/
  Directory index found at /external/phpids/0.6/lib/IDS/Caching/
  Directory index found at /external/phpids/0.6/lib/IDS/Config/
  Directory index found at /external/phpids/0.6/lib/IDS/Filter/
  Directory index found at /external/phpids/0.6/lib/IDS/Log/
  Directory index found at /external/phpids/0.6/lib/IDS/tmp/
  Directory index found at /external/phpids/0.6/lib/IDS/vendors/
  Directory index found at /external/phpids/0.6/lib/IDS/vendors/htmlpurifier/
  Directory index found at /external/phpids/0.6/docs/phpdocumentor/media/
  Directory index found at /external/phpids/0.6/docs/phpdocumentor/PHPIDS/
```