# Web Application Paper Scan

Report generated by Nessus™ Sun, 10 Apr 2022 18:49:16 EDT

TABLE OF CONTENTS

## Vulnerabilities by Host

# Vulnerabilities by Host

# 10.10.11.143

| 0 | 1 | 12 | 4 | 78 |
|---|---|---|---|---|
| CRITICAL | HIGH | MEDIUM | LOW | INFO |

### Scan Information

| | |
|---|---|
| Start time: | Sun Apr 10 17:52:54 2022 |
| End time: | Sun Apr 10 18:49:16 2022 |

### Host Information

| | |
|---|---|
| DNS Name: | office.paper |
| IP: | 10.10.11.143 |
| OS: | Linux Kernel 2.6 |

## Vulnerabilities

### 42423 - CGI Generic SSI Injection (HTTP headers)

#### Synopsis

It may be possible to execute arbitrary code through a CGI script hosted on the remote web server.

#### Description

The remote web server hosts one or more CGI scripts that fail to adequately sanitize request strings and seem to be vulnerable to an 'SSI injection' attack. By leveraging this issue, an attacker may be able to execute arbitrary commands on the remote host.

#### See Also

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

https://www.owasp.org/index.php/Server-Side_Includes_(SSI)_Injection

http://projects.webappsec.org/w/page/13246964/SSI%20Injection

#### Solution

Disable Server Side Includes if you do not use them.

Otherwise, restrict access to the vulnerable application or contact the vendor for a patch / upgrade.

### Risk Factor

High

### CVSS v2.0 Base Score

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

### References

| | |
|---|---|
| XREF | CWE:97 |
| XREF | CWE:96 |
| XREF | CWE:94 |
| XREF | CWE:74 |
| XREF | CWE:727 |
| XREF | CWE:632 |
| XREF | CWE:75 |
| XREF | CWE:752 |
| XREF | CWE:713 |

### Plugin Information

Published: 2009/11/06, Modified: 2021/01/19

### Plugin Output

tcp/80/www

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

+ The following resources may be vulnerable to SSI injection (on HTTP headers) :

/manual/howto/ssi.html

-------- request --------
POST /manual/howto/ssi.html HTTP/1.1
Host: office.paper
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Close
Content-Length: 68
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
<!--#include file="nessus803744314.html"-->=1&/manual/howto/ssi.html
------------------------

-------- output --------
you get the message</p>
<div class="example"><p><code>
[an error occurred while processing this directive]
</code></p></div>
------------------------
```

## 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 : /xmlrpc.php.bak
    URL  : http://10.10.11.143/xmlrpc.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://10.10.11.143/manual/images/
http://10.10.11.143/manual/style/
http://10.10.11.143/manual/style/css/
http://10.10.11.143/manual/style/lang/
http://10.10.11.143/manual/style/latex/
http://10.10.11.143/manual/style/scripts/
http://10.10.11.143/manual/style/xsl/
```

## 40984 - Browsable Web Directories

### Synopsis

Some directories on the remote web server are browsable.

### Description

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

### See Also

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

### Solution

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

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v2.0 Base Score

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

### Plugin Information

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

### Plugin Output

tcp/443/www

```
The following directories are browsable :

https://10.10.11.143/manual/images/
https://10.10.11.143/manual/style/
https://10.10.11.143/manual/style/css/
https://10.10.11.143/manual/style/lang/
https://10.10.11.143/manual/style/latex/
https://10.10.11.143/manual/style/scripts/
https://10.10.11.143/manual/style/xsl/
```

## 11213 - HTTP TRACE / TRACK Methods Allowed

### Synopsis

Debugging functions are enabled on the remote web server.

### Description

The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

### See Also

https://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf

http://www.apacheweek.com/issues/03-01-24

https://download.oracle.com/sunalerts/1000718.1.html

### Solution

Disable these HTTP methods. Refer to the plugin output for more information.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

### References

| | |
|---|---|
| BID | 9506 |
| BID | 9561 |
| BID | 11604 |
| BID | 33374 |

| | |
|---|---|
| BID | 37995 |
| CVE | CVE-2003-1567 |
| CVE | CVE-2004-2320 |
| CVE | CVE-2010-0386 |
| XREF | CERT:288308 |
| XREF | CERT:867593 |
| XREF | CWE:16 |
| XREF | CWE:200 |

## Plugin Information

Published: 2003/01/23, Modified: 2020/06/12

## Plugin Output

tcp/80/www

```
To disable these methods, add the following lines for each virtual
host in your configuration file :

    RewriteEngine on
    RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
    RewriteRule .* - [F]

Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2
support disabling the TRACE method natively via the 'TraceEnable'
directive.

Nessus sent the following TRACE request :

------------------------------ snip ------------------------------
TRACE /Nessus2041059330.html HTTP/1.1
Connection: Close
Host: office.paper
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------

and received the following response from the remote server :

------------------------------ snip ------------------------------
HTTP/1.1 200 OK
Date: Sun, 10 Apr 2022 22:23:25 GMT
Server: Apache/2.4.37 (centos) OpenSSL/1.1.1k mod_fcgid/2.3.9
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: message/http


TRACE /Nessus2041059330.html HTTP/1.1
Connection: Keep-Alive
Host: office.paper
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
```

```
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------
```

## 11213 - HTTP TRACE / TRACK Methods Allowed

### Synopsis

Debugging functions are enabled on the remote web server.

### Description

The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

### See Also

https://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf

http://www.apacheweek.com/issues/03-01-24

https://download.oracle.com/sunalerts/1000718.1.html

### Solution

Disable these HTTP methods. Refer to the plugin output for more information.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

### References

| | |
|---|---|
| BID | 9506 |
| BID | 9561 |
| BID | 11604 |
| BID | 33374 |

| | |
|---|---|
| BID | 37995 |
| CVE | CVE-2003-1567 |
| CVE | CVE-2004-2320 |
| CVE | CVE-2010-0386 |
| XREF | CERT:288308 |
| XREF | CERT:867593 |
| XREF | CWE:16 |
| XREF | CWE:200 |

## Plugin Information

Published: 2003/01/23, Modified: 2020/06/12

## Plugin Output

tcp/443/www

```

To disable these methods, add the following lines for each virtual
host in your configuration file :

    RewriteEngine on
    RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
    RewriteRule .* - [F]

Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2
support disabling the TRACE method natively via the 'TraceEnable'
directive.

Nessus sent the following TRACE request :

------------------------------ snip ------------------------------
TRACE /Nessus1757121621.html HTTP/1.1
Connection: Close
Host: office.paper
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------

and received the following response from the remote server :

------------------------------ snip ------------------------------
HTTP/1.1 200 OK
Date: Sun, 10 Apr 2022 22:23:25 GMT
Server: Apache/2.4.37 (centos) OpenSSL/1.1.1k mod_fcgid/2.3.9
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: message/http


TRACE /Nessus1757121621.html HTTP/1.1
Connection: Keep-Alive
Host: office.paper
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
```

```
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------
```

## 51192 - SSL Certificate Cannot Be Trusted

### Synopsis

The SSL certificate for this service cannot be trusted.

### Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

### See Also

https://www.itu.int/rec/T-REC-X.509/en

https://en.wikipedia.org/wiki/X.509

### Solution

Purchase or generate a proper SSL certificate for this service.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v2.0 Base Score

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

## Plugin Information

Published: 2010/12/15, Modified: 2020/04/27

## Plugin Output

tcp/443/www

```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : C=US/O=Unspecified/OU=ca-3899279223185377061/CN=localhost.localdomain/
E=root@localhost.localdomain
|-Issuer  : C=US/O=Unspecified/OU=ca-3899279223185377061/CN=localhost.localdomain/
E=root@localhost.localdomain
```

## 57582 - SSL Self-Signed Certificate

### Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

### Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

### Solution

Purchase or generate a proper SSL certificate for this service.

### Risk Factor

Medium

### CVSS v2.0 Base Score

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

### Plugin Information

Published: 2012/01/17, Modified: 2020/04/27

### Plugin Output

tcp/443/www

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : C=US/O=Unspecified/OU=ca-3899279223185377061/CN=localhost.localdomain/
E=root@localhost.localdomain
```

## 57640 - Web Application Information Disclosure

### Synopsis

The remote web application discloses path information.

### Description

At least one web application hosted on the remote web server discloses the physical path to its directories when a malformed request is sent to it.

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

### Solution

Filter error messages containing path information.

### 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: 2012/01/25, Modified: 2021/01/19

### Plugin Output

tcp/80/www

```
The request POST /manual/howto/ssi.html HTTP/1.1
Host: office.paper
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Close
Content-Length: 68
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
<!--#include file="nessus803744314.html"-->=1&/manual/howto/ssi.html

produces the following path information :
<p>Here's something else that you can do with the <code>exec</code>
function. You can actually have SSI execute a command using the
shell (<code>/bin/sh</code>, to be precise - or the DOS shell,
if you're on Win32). The following, for example, will give you
a directory listing.</p>
```

## 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://10.10.11.143/
  - http://10.10.11.143/index.php/2021/
  - http://10.10.11.143/index.php/2021/06/
  - http://10.10.11.143/index.php/2021/06/19/
  - http://10.10.11.143/index.php/2021/06/19/feeling-alone/
  - http://10.10.11.143/index.php/2021/06/19/hello-scranton/
  - http://10.10.11.143/index.php/2021/06/19/secret-of-my-success/
  - http://10.10.11.143/index.php/author/prisonmike/
  - http://10.10.11.143/index.php/category/uncategorized/
  - http://10.10.11.143/manual/
```

## 85582 - Web Application Potentially Vulnerable to Clickjacking

### Synopsis

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

### Description

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

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

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

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

### See Also

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

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

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

### Solution

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

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

### Risk Factor

Medium

### CVSS v2.0 Base Score

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

### References

| | |
|---|---|
| XREF | CWE:693 |

## Plugin Information

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

## Plugin Output

tcp/443/www

```

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

  - https://10.10.11.143/manual/
```

## 90067 - WordPress User Enumeration

### Synopsis

The remote web server contains a PHP application that is affected by an information disclosure vulnerability.

### Description

The version of WordPress hosted on the remote web server is affected by a user enumeration vulnerability. An unauthenticated, remote attacker can exploit this to learn the names of valid WordPress users.

This information could be used to mount further attacks.

### See Also

https://hackertarget.com/wordpress-user-enumeration/

### Solution

n/a

### 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: 2016/03/21, Modified: 2018/05/16

### Plugin Output

tcp/80/www

```
Nessus was able to enumerate the following WordPress users from the WordPress install at
 'http://10.10.11.143/' :
 prisonmike
 nick
 creedthoughts
```

## 12218 - mDNS Detection (Remote Network)

### Synopsis

It is possible to obtain information about the remote host.

### Description

The remote service understands the Bonjour (also known as ZeroConf or mDNS) protocol, which allows anyone to uncover information from the remote host such as its operating system type and exact version, its hostname, and the list of services it is running.

This plugin attempts to discover mDNS used by hosts that are not on the network segment on which Nessus resides.

### Solution

Filter incoming traffic to UDP port 5353, if desired.

### 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: 2004/04/28, Modified: 2021/06/28

### Plugin Output

udp/5353/mdns

```
Nessus was able to extract the following information :

  - mDNS hostname       : paper.local.
```

## 70658 - SSH Server CBC Mode Ciphers Enabled

### Synopsis

The SSH server is configured to use Cipher Block Chaining.

### Description

The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

### Solution

Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

### Risk Factor

Low

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

### References

| | |
|---|---|
| BID | 32319 |
| CVE | CVE-2008-5161 |
| XREF | CERT:958563 |
| XREF | CWE:200 |

### Plugin Information

Published: 2013/10/28, Modified: 2018/07/30

### Plugin Output

tcp/22/ssh

```

The following client-to-server Cipher Block Chaining (CBC) algorithms
are supported :
  aes128-cbc
  aes256-cbc

The following server-to-client Cipher Block Chaining (CBC) algorithms
are supported :

  aes128-cbc
  aes256-cbc
```

## 153953 - SSH Weak Key Exchange Algorithms Enabled

### Synopsis

The remote SSH server is configured to allow weak key exchange algorithms.

### Description

The remote SSH server is configured to allow key exchange algorithms which are considered weak.

This is based on the IETF draft document Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH) draft-ietf-curdle-ssh-kex-sha2-20. Section 4 lists guidance on key exchange algorithms that SHOULD NOT and MUST NOT be enabled. This includes:

diffie-hellman-group-exchange-sha1

diffie-hellman-group1-sha1

gss-gex-sha1-*

gss-group1-sha1-*

gss-group14-sha1-*

rsa1024-sha1

Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

### See Also

http://www.nessus.org/u?b02d91cd

https://datatracker.ietf.org/doc/html/rfc8732

### Solution

Contact the vendor or consult product documentation to disable the weak algorithms.

### Risk Factor

Low

### CVSS v3.0 Base Score

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

### CVSS v2.0 Base Score

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

### Plugin Information

Published: 2021/10/13, Modified: 2021/10/13

## Plugin Output

### tcp/22/ssh

```

The following weak key exchange algorithms are enabled :

  diffie-hellman-group-exchange-sha1
```

## 42057 - Web Server Allows Password Auto-Completion

### Synopsis

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

### Description

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

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

### Solution

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

### Risk Factor

Low

### Plugin Information

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

### Plugin Output

tcp/80/www

```
Page : /wp-login.php
Destination Page: /wp-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 : /wp-login.php
Destination Page: /wp-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: 2020/09/22

### Plugin Output

tcp/80/www

```
URL        : http://10.10.11.143/
Version    : 2.4.99
backported : 1
modules    : OpenSSL/1.1.1k mod_fcgid/2.3.9
os         : ConvertedCentOS
```

## 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: 2020/09/22

### Plugin Output

tcp/443/www

```
  URL        : https://10.10.11.143/
  Version    : 2.4.99
  backported : 1
  modules    : OpenSSL/1.1.1k mod_fcgid/2.3.9
  os         : ConvertedCentOS
```

## 84574 - Backported Security Patch Detection (PHP)

### Synopsis

Security patches have been backported.

### Description

Security patches may have been 'backported' to the remote PHP install without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

### See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2015/07/07, Modified: 2015/07/07

### Plugin Output

tcp/80/www

```
Give Nessus credentials to perform local checks.
```

## 39520 - Backported Security Patch Detection (SSH)

### Synopsis

Security patches are backported.

### Description

Security patches may have been 'backported' to the remote SSH server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

### See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2009/06/25, Modified: 2015/07/07

### Plugin Output

tcp/22/ssh

```
Give Nessus credentials to perform local checks.
```

## 39521 - Backported Security Patch Detection (WWW)

### Synopsis

Security patches are backported.

### Description

Security patches may have been 'backported' to the remote HTTP server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

### See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2009/06/25, Modified: 2015/07/07

### Plugin Output

tcp/80/www

```
Give Nessus credentials to perform local checks.
```

## 39521 - Backported Security Patch Detection (WWW)

### Synopsis

Security patches are backported.

### Description

Security patches may have been 'backported' to the remote HTTP server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

### See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2009/06/25, Modified: 2015/07/07

### Plugin Output

tcp/443/www

```
Give Nessus credentials to perform local checks.
```

## 47830 - CGI Generic Injectable Parameter

### Synopsis

Some CGIs are candidate for extended injection tests.

### Description

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

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

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

### Solution

n/a

### Risk Factor

None

### References

| | |
|---|---|
| XREF | CWE:86 |

### Plugin Information

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

### Plugin Output

tcp/80/www

```

Using the GET HTTP method, Nessus found that :

+ The following resources may be vulnerable to injectable parameter :

+ The 's' parameter of the / CGI :

/?s=cqbdop

-------- output --------
<link rel="profile" href="https://gmpg.org/xfn/11">

<title>Search Results for &#8220;cqbdop&#8221; &#8211; Blunder Tiffin In
c.</title>
<meta name='robots' content='noindex,follow' />
<link rel='dns-prefetch' href='//fonts.googleapis.com' />
------------------------

Clicking directly on these URLs should exhibit the issue :
```

```
(you will probably need to read the HTML source)

http://10.10.11.143/?s=cqbdop


Using the POST HTTP method, Nessus found that :

+ The following resources may be vulnerable to injectable parameter :

+ The 'log' parameter of the /wp-login.php CGI :

/wp-login.php [log=cqbdop]

-------- output --------
<p>
<label for="user_login">Username or Email Address<br />
<input type="text" name="log" id="user_login" aria-describedby="login_er
ror" class="input" value="cqbdop" size="20" autocapitalize="off" /></lab
el>
</p>
<p>
------------------------
```

## 40406 - CGI Generic Tests HTTP Errors

### Synopsis

Nessus encountered errors while running its generic CGI attacks.

### Description

Nessus ran into trouble while running its generic CGI tests against the remote web server (for example, connection refused, timeout, etc). When this happens, Nessus aborts the current test and switches to the next CGI script on the same port or to another web server. Thus, test results may be incomplete.

### Solution

Rescan with a longer network timeout or less parallelism for example, by changing the following options in the scan policy :

- Network -> Network Receive Timeout (check_read_timeout)

- Options -> Number of hosts in parallel (max_hosts)

- Options -> Number of checks in parallel (max_checks)

### Risk Factor

None

### Plugin Information

Published: 2009/07/28, Modified: 2021/01/19

### Plugin Output

tcp/80/www

```
Nessus encountered :

  - 2 errors involving header injection checks :
   . connecting to server: errno=1 (operation timed out)
  - 1 error involving cross-site scripting (extended patterns) checks :
   . connecting to server: errno=1 (operation timed out)
  - 1 error involving script injection checks :
   . connecting to server: errno=1 (operation timed out)
  - 4 errors involving persistent XSS checks :
```

## 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: 2021/01/19

### Plugin Output

tcp/80/www

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

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

SQL injection                            : S=264        SP=264       AP=624       SC=24
 AC=768
unseen parameters                        : S=385        SP=385       AP=910       SC=35
 AC=1120
local file inclusion                     : S=11         SP=11        AP=26        SC=1         AC=32

web code injection                       : S=11         SP=11        AP=26        SC=1         AC=32

XML injection                            : S=11         SP=11        AP=26        SC=1         AC=32

format string                            : S=22         SP=22        AP=52        SC=2         AC=64

script injection                         : S=2          SP=2         AP=2         SC=2         AC=2

cross-site scripting (comprehensive test): S=44         SP=44        AP=104       SC=4
 AC=128
```

```
injectable parameter                     : S=22         SP=22        AP=52        SC=2         AC=64

cross-site scripting (extended patterns) : S=12         SP=12        AP=12        SC=12        AC=12

directory traversal (write access)       : S=22         SP=22        AP=52        SC=2         AC=64

SSI injection                            : S=33         SP=33        AP=78        SC=3         AC=96

header injection                         : S=4          SP=4         AP=4         SC=4         AC=4

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

directory traversal                      : S=275        SP=275       AP=650       SC=25
 AC=800
arbitrary command execution (time based) : S=66         SP=66        AP=156       SC=6
 AC=192
persistent XSS                         [...]
```

## 39470 - CGI Generic Tests Timeout

### Synopsis

Some generic CGI attacks ran out of time.

### Description

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

### Solution

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

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

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

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

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

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

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/80/www

```
The following tests timed out without finding any flaw :
- arbitrary command execution
- blind SQL injection
- persistent XSS
- SQL injection
- cross-site scripting (comprehensive test)
- directory traversal

The following tests were interrupted and did not report all possible flaws :
- SSI injection (on HTTP headers)
```

## 39470 - CGI Generic Tests Timeout

### Synopsis

Some generic CGI attacks ran out of time.

### Description

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

### Solution

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

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

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

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

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

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

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/443/www

```
The following tests timed out without finding any flaw :
- SSI injection (on HTTP headers)
```

## 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: 2022/02/14

### Plugin Output

tcp/0

```

The remote operating system matched the following CPE :

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

Following application CPE's matched on the remote system :

  cpe:/a:apache:http_server:2.4.37 -> Apache Software Foundation Apache HTTP Server
  cpe:/a:apache:http_server:2.4.99 -> Apache Software Foundation Apache HTTP Server
  cpe:/a:openbsd:openssh:8.0 -> OpenBSD OpenSSH
  cpe:/a:openssl:openssl:1.1.1k -> OpenSSL Project OpenSSL
  cpe:/a:php:php:7.2.24 -> PHP PHP
  cpe:/a:wordpress:wordpress:5.2.3 -> WordPress
```

## 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: 2011/05/23

### 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

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


http://apache.webthing.com/mod_diagnostics/ - /manual/mod/mod_filter.html
http://apache.webthing.com/mod_proxy_html/ - /manual/mod/mod_proxy_html.html
http://apr.apache.org                   - /manual/mod/mod_ldap.html
http://apr.apache.org/                  - /manual/glossary.html
http://apr.apache.org/docs/apr-util/trunk/group___a_p_r___util___bucket___brigades.html - /manual/
developer/output-filters.html
http://apr.apache.org/docs/apr/1.4/group__apr__pools.html#ga85f1e193c31d109affda72f9a92c6915 - /
manual/developer/modguide.html
http://apr.apache.org/docs/apr/1.4/group__apr__pools.html#gaf61c098ad258069d64cdf8c0a9369f9e - /
manual/developer/modguide.html
http://apr.apache.org/docs/apr/1.4/group__apr__strings.html#ga3eca76b8d293c5c3f8021e45eda813d8 - /
manual/developer/modguide.html
http://apr.apache.org/docs/apr/1.4/group__apr__strings.html#gabc79e99ff19abbd7cfd18308c5f85d47 - /
manual/developer/modguide.html
http://aspell.sourceforge.net/          - /manual/developer/thread_safety.html
http://bahumbug.wordpress.com/2006/10/12/mod_proxy_html-revisited/ - /manual/mod/mod_xml2enc.html
http://bitnami.com/stack/wamp           - /manual/platform/windows.html
http://blog.haproxy.com/haproxy/proxy-protocol/ - /manual/mod/mod_remoteip.html
http://bugs.apache.org/index/full/467   - /manual/misc/perf-tuning.html
http://caniuse.com/#search=http2        - /manual/howto/http2.html
http://cgiwrap.sourceforge.net/         - /manual/misc/security_tips.html
http://ci.apache.org/projects/httpd/trunk/doxygen/ - /manual/developer/
http://ci.apache.org/projects/httpd/trunk/doxygen/
group__APACHE__CORE__CONFIG.html#ga07c7d22ae17805e61204463326cf9c34 - /manual/developer/
modguide.html
```

```
http://ci.apache.org/projects/httpd/trunk/doxygen/
group__APACHE__CORE__CONFIG.html#ga1093a5908a384eacc929b028c79f2a02 - /manual/developer/
modguide.html
http://ci.apache.org/projects/httpd/trunk/doxygen/group__APACHE__CORE__CONFIG.html#gafaec43534fcf2
 [...]
```

## 49704 - External URLs

### Synopsis

Links to external sites were gathered.

### Description

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/443/www

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


http://apache.webthing.com/mod_diagnostics/ -
http://apache.webthing.com/mod_proxy_html/ -
http://apr.apache.org                   -
http://apr.apache.org/                  -
http://apr.apache.org/docs/apr-util/trunk/group___a_p_r___util___bucket___brigades.html -
http://apr.apache.org/docs/apr/1.4/group__apr__pools.html#ga85f1e193c31d109affda72f9a92c6915 -
http://apr.apache.org/docs/apr/1.4/group__apr__pools.html#gaf61c098ad258069d64cdf8c0a9369f9e -
http://apr.apache.org/docs/apr/1.4/group__apr__strings.html#ga3eca76b8d293c5c3f8021e45eda813d8 -
http://apr.apache.org/docs/apr/1.4/group__apr__strings.html#gabc79e99ff19abbd7cfd18308c5f85d47 -
http://aspell.sourceforge.net/          -
http://bahumbug.wordpress.com/2006/10/12/mod_proxy_html-revisited/ -
http://bitnami.com/stack/wamp           -
http://blog.haproxy.com/haproxy/proxy-protocol/ -
http://bugs.apache.org/index/full/467   -
http://caniuse.com/#search=http2        -
http://cgiwrap.sourceforge.net/         -
http://ci.apache.org/projects/httpd/trunk/doxygen/ -
http://ci.apache.org/projects/httpd/trunk/doxygen/
group__APACHE__CORE__CONFIG.html#ga07c7d22ae17805e61204463326cf9c34 -
http://ci.apache.org/projects/httpd/trunk/doxygen/
group__APACHE__CORE__CONFIG.html#ga1093a5908a384eacc929b028c79f2a02 -
http://ci.apache.org/projects/httpd/trunk/doxygen/
group__APACHE__CORE__CONFIG.html#gafaec43534fcf200f37d9fecbf9247c21 -
http://ci.apache.org/projects/httpd/trunk/doxygen/
group__APACHE__CORE__DAEMON.html#ga9d426b6382b49754d4f87c55f65af202 -
http://ci.apache.org/projects/httpd/trunk/doxygen/
group__APACHE__CORE__PROTO.html#ga5e91eb6ca777c9a427b2e82bf1eeb81d -
```

```
http://ci.apache.org/projects/httpd/trunk/doxygen/
group__APACHE__CORE__PROTO.html#gaa2f8412c400197338ec509f4a45e4579 -
http://ci.apache.org/projects/httpd/trunk/doxygen/
group__APACHE__CORE__PROTO.html#gac827cd0537d2b6213a7c06d7c26cc36e -
http://ci.apache.org/projects/httpd/trunk/doxyg [...]
```

## 84502 - HSTS Missing From HTTPS Server

### Synopsis

The remote web server is not enforcing HSTS.

### Description

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

### See Also

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

### Solution

Configure the remote web server to use HSTS.

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/443/www

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

## 69826 - HTTP Cookie 'secure' Property Transport Mismatch

### Synopsis

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

### Description

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

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

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

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

This should not happen.

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

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

### See Also

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/443/www

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

  Domain   :
  Path     : /
  Name     : wordpress_test_cookie
  Value    : WP+Cookie+check
  Secure   : false
  HttpOnly : false
```

## 43111 - HTTP Methods Allowed (per directory)

### Synopsis

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

### Description

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

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

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

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

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

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

### See Also

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

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

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2009/12/10, Modified: 2019/03/19

### Plugin Output

tcp/80/www

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

  - HTTP method GET is allowed on :

    /index.php/wp-json
    /index.php/wp-json/oembed/1.0

  - HTTP methods GET HEAD OPTIONS POST TRACE are allowed on :

    /icons
    /manual


Based on tests of each method :

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

    /cgi-bin
    /index.php
    /index.php/2021
    /index.php/2021/06
    /index.php/2021/06/19
    /index.php/2021/06/19/feeling-alone
    /index.php/2021/06/19/hello-scranton
    /index.php/2021/06/19/secret-of-my-success
    /index.php/author/prisonmike
    /index.php/author/prisonmike/feed
    /index.php/category/uncategorized
    /index.php/category/uncategorized/feed
    /index.php/comments/feed
    /index.php/feed
    /index.php/wp-json
    /index.php/wp-json/oembed/1.0

  - HTTP methods GET HEAD OPTIONS POST TRACE are allowed on :

    /
    /icons
    /manual

  - Invalid/unknown HTTP methods are allowed on :

    /cgi-bin
    /index.php
    /index.php/2021
    /index.php/2021/06
    /index.php/2021/06/19
    /index.php/2021/06/19/feeling-alone
    /index.php/2021/06/19/hello-scranton
    /index.php/2021/06/19/secret-of-my-success
    /index.php/author/prisonmike
    /index.php/author/prisonmike/feed
    /index.php/category/uncategorized
    /index.php/category/uncategorized/feed
    /index.php/comments/feed
    /index.php/feed
    /index.php/wp-json
    /index.php/wp-json/oembed/1.0
```

## 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: 2019/03/19

### Plugin Output

tcp/443/www

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

  - HTTP methods GET HEAD OPTIONS POST TRACE are allowed on :

    /
    /icons
    /manual
    /manual/developer


Based on tests of each method :

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

    /cgi-bin
    /manual/de/mod
    /manual/de/vhosts
    /manual/en/developer
    /manual/en/howto
    /manual/en/misc
    /manual/en/mod
    /manual/en/platform
    /manual/en/programs
    /manual/en/rewrite
    /manual/en/ssl
    /manual/en/vhosts
    /manual/es/howto
    /manual/es/misc
    /manual/es/mod

  - HTTP methods GET HEAD OPTIONS POST TRACE are allowed on :

    /
    /icons
    /manual
    /manual/developer

  - Invalid/unknown HTTP methods are allowed on :

    /cgi-bin
    /manual/de/mod
    /manual/de/vhosts
    /manual/en/developer
    /manual/en/howto
    /manual/en/misc
    /manual/en/mod
    /manual/en/platform
    /manual/en/programs
    /manual/en/rewrite
    /manual/en/ssl
    /manual/en/vhosts
    /manual/es/howto
    /manual/es/misc
    /manual/es/mod
```

## 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/2.4.37 (centos) OpenSSL/1.1.1k mod_fcgid/2.3.9
```

## 10107 - HTTP Server Type and Version

### Synopsis

A web server is running on the remote host.

### Description

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

### Solution

n/a

### Risk Factor

None

### References

| | |
|---|---|
| XREF | IAVT:0001-T-0931 |

### Plugin Information

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

### Plugin Output

tcp/443/www

```
The remote web server type is :

Apache/2.4.37 (centos) OpenSSL/1.1.1k mod_fcgid/2.3.9
```

## 12053 - Host Fully Qualified Domain Name (FQDN) Resolution

### Synopsis

It was possible to resolve the name of the remote host.

### Description

Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/02/11, Modified: 2017/04/14

### Plugin Output

tcp/0

```
10.10.11.143 resolves as office.paper.
```

## 24260 - HyperText Transfer Protocol (HTTP) Information

### Synopsis

Some information about the remote HTTP configuration can be extracted.

### Description

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

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/80/www

```
Response Code : HTTP/1.1 200 OK

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

  Date: Sun, 10 Apr 2022 22:37:18 GMT
  Server: Apache/2.4.37 (centos) OpenSSL/1.1.1k mod_fcgid/2.3.9
  X-Powered-By: PHP/7.2.24
  Link: <http://office.paper/index.php/wp-json/>; rel="https://api.w.org/"
  X-Backend-Server: office.paper
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Transfer-Encoding: chunked
  Content-Type: text/html; charset=UTF-8

Response Body :


<!doctype html>
<html lang="en-US">
<head>
<meta charset="UTF-8">
<meta name="viewport" content="width=device-width, initial-scale=1">
<link rel="profile" href="https://gmpg.org/xfn/11">
```

```
<title>Blunder Tiffin Inc. &#8211; The best paper company in the electric-city Scranton!</title>
<meta name='robots' content='noindex,follow' />
<link rel='dns-prefetch' href='//fonts.googleapis.com' />
<link rel='dns-prefetch' href='//s.w.org' />
<link rel="alternate" type="application/rss+xml" title="Blunder Tiffin Inc. &raquo; Feed"
 href="http://office.paper/index.php/feed/" />
<link rel="alternate" type="application/rss+xml" title="Blunder Tiffin Inc. &raquo; Comments Feed"
 href="http://office.paper/index.php/comments/feed/" />
<script type="text/javascript">
window._wpemojiSettings = {"baseUrl":"https:\/\/s.w.org\/images\/core\/emoji
\/12.0.0-1\/72x72\/","ext":".png","svgUrl":"https:\/\/s.w.org\/images\/core\/emoji\/12.0.0-1\/
svg\/","svgExt":".svg","source":{"concatemoji":"http:\/\/office.paper\/wp-includes\/js\/wp-emoji-
release.min.js?ver=5.2.3"}};
!function(a,b,c){function d(a,b){var
 c=String.fromCharCode;l.clearRect(0,0,k.width,k.height),l.fillText(c.apply(this,a),0,0);var
 d=k.toDataURL();l.clearRect(0,0,k.width,k.height),l.fillText(c.apply(this,b),0,0);var
 e=k.toDataURL();return d===e}function e(a){var b;if(!l||!l.fillText)return!
1;switch(l.textBaseline="top",l.font="600 32px Arial",a){case"flag":return!
(b=d([55356,56826,55356,56819],[55356,56826,8203,55356,56819]))&&(b=d([55356,57332,56128, [...]
```

## 24260 - HyperText Transfer Protocol (HTTP) Information

### Synopsis

Some information about the remote HTTP configuration can be extracted.

### Description

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

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/443/www

```

Response Code : HTTP/1.1 403 Forbidden

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

  Date: Sun, 10 Apr 2022 22:37:19 GMT
  Server: Apache/2.4.37 (centos) OpenSSL/1.1.1k mod_fcgid/2.3.9
  Last-Modified: Sun, 27 Jun 2021 23:47:13 GMT
  ETag: "30c0b-5c5c7fdeec240"
  Accept-Ranges: bytes
  Content-Length: 199691
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html; charset=UTF-8

Response Body :

<!DOCTYPE html>
<html lang="en">
<head>
  <meta name="generator" content="HTML Tidy for HTML5 for Linux version 5.7.28">
  <title>HTTP Server Test Page powered by CentOS</title>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
  <link rel="shortcut icon" href="http://www.centos.org/favicon.ico">
  <style type="text/css">
      /*<![CDATA[*/
      /*!
       * Bootstrap v4.3.1 (https://getbootstrap.com/)
       * Copyright 2011-2019 The Bootstrap Authors
       * Copyright 2011-2019 Twitter, Inc.
       * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE)
       */:root{--blue:#007bff;--indigo:#6610f2;--purple:#6f42c1;--pink:#e83e8c;--red:#dc3545;--
orange:#fd7e14;--yellow:#ffc107;--green:#28a745;--teal:#20c997;--cyan:#17a2b8;--white:#fff;--
gray:#6c757d;--gray-dark:#343a40;--primary:#007bff;--secondary:#6c757d;--success:#28a745;--
info:#17a2b8;--warning:#ffc107;--danger:#dc3545;--light:#f8f9fa;--dark:#343a40;--breakpoint-xs:0;--
breakpoint-sm:576px;--breakpoint-md:768px;--breakpoint-lg:992px;--breakpoint-xl:1200px;--font-
family-sans-serif:-apple-system,BlinkMacSystemFont,"Segoe UI",Roboto,"Helvetica Neue",Arial,"Noto
 Sans",sans-serif,"Apple Color Emoji","Segoe UI Emoji","Segoe UI Symbol","Noto Color Emoji";--
font-family-monospace:SFMono-Regular,Menlo,Monaco,Consolas,"Liberation Mono","Courier
 New",monospace}*,::after,::before{box-sizing:border-box}html{font-family:sans-serif;line-
height:1.15;-webkit-text-size-adjust:100%;-webkit-tap-highlight-color:t [...]
```

## 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 difference between the local and remote clocks is -1124 seconds.
```

## 46215 - Inconsistent Hostname and IP Address

### Synopsis

The remote host's hostname is not consistent with DNS information.

### Description

The name of this machine either does not resolve or resolves to a different IP address.

This may come from a badly configured reverse DNS or from a host file in use on the Nessus scanning host.

As a result, URLs in plugin output may not be directly usable in a web browser and some web tests may be incomplete.

### Solution

Fix the reverse DNS or host file.

### Risk Factor

None

### Plugin Information

Published: 2010/05/03, Modified: 2016/08/05

### Plugin Output

tcp/0

```
The host name 'office.paper' does not resolve to an IP address
```

## 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://10.10.11.143/
  - http://10.10.11.143/index.php/2021/
  - http://10.10.11.143/index.php/2021/06/
  - http://10.10.11.143/index.php/2021/06/19/
  - http://10.10.11.143/index.php/2021/06/19/feeling-alone/
  - http://10.10.11.143/index.php/2021/06/19/hello-scranton/
  - http://10.10.11.143/index.php/2021/06/19/secret-of-my-success/
  - http://10.10.11.143/index.php/author/prisonmike/
  - http://10.10.11.143/index.php/category/uncategorized/
  - http://10.10.11.143/manual/
  - http://10.10.11.143/manual/bind.html
```

```
    - http://10.10.11.143/manual/caching.html
    - http://10.10.11.143/manual/configuring.html
    - http://10.10.11.143/manual/content-negotiation.html
    - http://10.10.11.143/manual/custom-error.html
    - http://10.10.11.143/manual/developer/
    - http://10.10.11.143/manual/developer/API.html
    - http://10.10.11.143/manual/developer/documenting.html
    - http://10.10.11.143/manual/developer/filters.html
    - http://10.10.11.143/manual/developer/hooks.html
    - http://10.10.11.143/manual/developer/modguide.html
    - http://10.10.11.143/manual/developer/modules.html
    - http://10.10.11.143/manual/developer/new_api_2_4.html
    - http://10.10.11.143/manual/developer/output-filters.html
    - http://10.10.11.143/manual/developer/request.html
    - http://10.10.11.143/manual/developer/thread_safety.html
    - http://10.10.11.143/manual/dns-caveats.html
    - http://10.10.11.143/manual/dso.html
    - http://10.10.11.143/manual/expr.html
    - http://10.10.11.143/manual/filter.html
    - http://10.10.11.143/manual/getting-started.html
    - http://10.10.11.143/manual/glossary.html
    - http://10.10.11.143/manual/handler.html
    - http://10.10.11.143/manual/howto/
    - http://10.10.11.143/manual/howto/access.html
    - http://10.10.11.143/manual/howto/auth.html
    - http://10.10.11.143/manual/howto/cgi.html
    - http://10.10.11.143/manual/howto/htaccess.html
    - http://10.10.11.143/manual/howto/http2.html
    - http://10.10. [...]
```

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

### Synopsis

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

### Description

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

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

### See Also

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

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

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

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

### Solution

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

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/443/www

```

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

  - https://10.10.11.143/manual/
  - https://10.10.11.143/manual/bind.html
  - https://10.10.11.143/manual/caching.html
  - https://10.10.11.143/manual/configuring.html
  - https://10.10.11.143/manual/content-negotiation.html
  - https://10.10.11.143/manual/custom-error.html
  - https://10.10.11.143/manual/developer/
  - https://10.10.11.143/manual/developer/API.html
  - https://10.10.11.143/manual/developer/documenting.html
  - https://10.10.11.143/manual/developer/filters.html
  - https://10.10.11.143/manual/developer/hooks.html
```

```
    - https://10.10.11.143/manual/developer/modguide.html
    - https://10.10.11.143/manual/developer/modules.html
    - https://10.10.11.143/manual/developer/new_api_2_4.html
    - https://10.10.11.143/manual/developer/output-filters.html
    - https://10.10.11.143/manual/developer/request.html
    - https://10.10.11.143/manual/developer/thread_safety.html
    - https://10.10.11.143/manual/dns-caveats.html
    - https://10.10.11.143/manual/dso.html
    - https://10.10.11.143/manual/expr.html
    - https://10.10.11.143/manual/filter.html
    - https://10.10.11.143/manual/getting-started.html
    - https://10.10.11.143/manual/glossary.html
    - https://10.10.11.143/manual/handler.html
    - https://10.10.11.143/manual/howto/
    - https://10.10.11.143/manual/howto/access.html
    - https://10.10.11.143/manual/howto/auth.html
    - https://10.10.11.143/manual/howto/cgi.html
    - https://10.10.11.143/manual/howto/htaccess.html
    - https://10.10.11.143/manual/howto/http2.html
    - https://10.10.11.143/manual/howto/public_html.html
    - https://10.10.11.143/manual/howto/reverse_proxy.html
    - https://10.10.11.143/manual/howto/ssi.html
    - https://10.10.11.143/manual/images/
    - https://10.10.11.143/manual/install.html
    - https://10.10.11.143/manual/invoking.html
    - https://10.10.11.143/manual/license.html
    - https://10.10.11.143/manual/logs.html
    - https://10.10.11.143/manual/misc/
    - https://10.10.11.143/ [...]
```

## 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://10.10.11.143/
  - http://10.10.11.143/index.php/2021/
  - http://10.10.11.143/index.php/2021/06/
  - http://10.10.11.143/index.php/2021/06/19/
  - http://10.10.11.143/index.php/2021/06/19/feeling-alone/
  - http://10.10.11.143/index.php/2021/06/19/hello-scranton/
  - http://10.10.11.143/index.php/2021/06/19/secret-of-my-success/
  - http://10.10.11.143/index.php/author/prisonmike/
  - http://10.10.11.143/index.php/category/uncategorized/
  - http://10.10.11.143/manual/
  - http://10.10.11.143/manual/bind.html
  - http://10.10.11.143/manual/caching.html
  - http://10.10.11.143/manual/configuring.html
  - http://10.10.11.143/manual/content-negotiation.html
  - http://10.10.11.143/manual/custom-error.html
  - http://10.10.11.143/manual/developer/
```

```
    - http://10.10.11.143/manual/developer/API.html
    - http://10.10.11.143/manual/developer/documenting.html
    - http://10.10.11.143/manual/developer/filters.html
    - http://10.10.11.143/manual/developer/hooks.html
    - http://10.10.11.143/manual/developer/modguide.html
    - http://10.10.11.143/manual/developer/modules.html
    - http://10.10.11.143/manual/developer/new_api_2_4.html
    - http://10.10.11.143/manual/developer/output-filters.html
    - http://10.10.11.143/manual/developer/request.html
    - http://10.10.11.143/manual/developer/thread_safety.html
    - http://10.10.11.143/manual/dns-caveats.html
    - http://10.10.11.143/manual/dso.html
    - http://10.10.11.143/manual/expr.html
    - http://10.10.11.143/manual/filter.html
    - http://10.10.11.143/manual/getting-started.html
    - http://10.10.11.143/manual/glossary.html
    - http://10.10.11.143/manual/handler.html
    - http://10.10.11.143/manual/howto/
    - http://10.10.11.143/manual/howto/access.html
    - http://10.10.11.143/manual/howto/auth.html
    - http://10.10.11.143/manual/howto/cgi.html
    - http://10.10.11.143/manual/howto/htaccess.html
    - http://10.10.11.143/manual/howto/http2.html
    - http://10.10.11.143/manual/howto/publ [...]
```

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

### Synopsis

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

### Description

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

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

### See Also

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

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

### Solution

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

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/443/www

```

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

  - https://10.10.11.143/manual/
  - https://10.10.11.143/manual/bind.html
  - https://10.10.11.143/manual/caching.html
  - https://10.10.11.143/manual/configuring.html
  - https://10.10.11.143/manual/content-negotiation.html
  - https://10.10.11.143/manual/custom-error.html
  - https://10.10.11.143/manual/developer/
  - https://10.10.11.143/manual/developer/API.html
  - https://10.10.11.143/manual/developer/documenting.html
  - https://10.10.11.143/manual/developer/filters.html
  - https://10.10.11.143/manual/developer/hooks.html
  - https://10.10.11.143/manual/developer/modguide.html
  - https://10.10.11.143/manual/developer/modules.html
  - https://10.10.11.143/manual/developer/new_api_2_4.html
  - https://10.10.11.143/manual/developer/output-filters.html
  - https://10.10.11.143/manual/developer/request.html
```

```
    - https://10.10.11.143/manual/developer/thread_safety.html
    - https://10.10.11.143/manual/dns-caveats.html
    - https://10.10.11.143/manual/dso.html
    - https://10.10.11.143/manual/expr.html
    - https://10.10.11.143/manual/filter.html
    - https://10.10.11.143/manual/getting-started.html
    - https://10.10.11.143/manual/glossary.html
    - https://10.10.11.143/manual/handler.html
    - https://10.10.11.143/manual/howto/
    - https://10.10.11.143/manual/howto/access.html
    - https://10.10.11.143/manual/howto/auth.html
    - https://10.10.11.143/manual/howto/cgi.html
    - https://10.10.11.143/manual/howto/htaccess.html
    - https://10.10.11.143/manual/howto/http2.html
    - https://10.10.11.143/manual/howto/public_html.html
    - https://10.10.11.143/manual/howto/reverse_proxy.html
    - https://10.10.11.143/manual/howto/ssi.html
    - https://10.10.11.143/manual/images/
    - https://10.10.11.143/manual/install.html
    - https://10.10.11.143/manual/invoking.html
    - https://10.10.11.143/manual/license.html
    - https://10.10.11.143/manual/logs.html
    - https://10.10.11.143/manual/misc/
    - https://10.10.11.143/manual/misc/password_enc [...]
```

## 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: 2022/04/04

### Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.1.2
Nessus build : 20068
Plugin feed version : 202204091550
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : debian6-x86-64
Scan type : Normal
Scan name : Web Application Paper Scan
Scan policy used : Advanced Scan
Scanner IP : 10.10.14.185
Port scanner(s) : nessus_tcp_scanner
Port range : default
Ping RTT : 63.464 ms
Thorough tests : no
Experimental tests : 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 : yes
Web app tests -  Maximum run time : 5 minutes.
Web app tests -  Stop at first flaw : CGI
Max hosts : 100
Max checks : 5
Recv timeout : 5
Backports : Detected
Allow post-scan editing: Yes
Scan Start Date : 2022/4/10 17:52 EDT
Scan duration : 3380 sec
```

## 10335 - Nessus TCP scanner

### Synopsis

It is possible to determine which TCP ports are open.

### Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.

Once a TCP connection is open, it grabs any available banner for the service identification plugins.

Note that TCP scanners are more intrusive than SYN (half open) scanners.

### Solution

Protect your target with an IP filter.

### Risk Factor

None

### Plugin Information

Published: 2009/02/04, Modified: 2022/02/14

### Plugin Output

tcp/22/ssh

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

## 10335 - Nessus TCP scanner

### Synopsis

It is possible to determine which TCP ports are open.

### Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.

Once a TCP connection is open, it grabs any available banner for the service identification plugins.

Note that TCP scanners are more intrusive than SYN (half open) scanners.

### Solution

Protect your target with an IP filter.

### Risk Factor

None

### Plugin Information

Published: 2009/02/04, Modified: 2022/02/14

### Plugin Output

tcp/80/www

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

## 10335 - Nessus TCP scanner

### Synopsis

It is possible to determine which TCP ports are open.

### Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.

Once a TCP connection is open, it grabs any available banner for the service identification plugins.

Note that TCP scanners are more intrusive than SYN (half open) scanners.

### Solution

Protect your target with an IP filter.

### Risk Factor

None

### Plugin Information

Published: 2009/02/04, Modified: 2022/02/14

### Plugin Output

tcp/443/www

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

## 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
```

## 117886 - OS Security Patch Assessment Not Available

### Synopsis

OS Security Patch Assessment is not available.

### Description

OS Security Patch Assessment is not available on the remote host.

This does not necessarily indicate a problem with the scan.

Credentials may not have been provided, OS security patch assessment may not be supported for the target, the target may not have been identified, or another issue may have occurred that prevented OS security patch assessment from being available. See plugin output for details.

This plugin reports non-failure information impacting the availability of OS Security Patch Assessment. Failure information is reported by plugin 21745 : 'OS Security Patch Assessment failed'. If a target host is not supported for OS Security Patch Assessment, plugin 110695 : 'OS Security Patch Assessment Checks Not Supported' will report concurrently with this plugin.

### Solution

n/a

### Risk Factor

None

### References

| | |
|---|---|
| XREF | IAVB:0001-B-0515 |

### Plugin Information

Published: 2018/10/02, Modified: 2021/07/12

### Plugin Output

tcp/0

```
The following issues were reported :

  - Plugin      : no_local_checks_credentials.nasl
    Plugin ID   : 110723
    Plugin Name : Target Credential Status by Authentication Protocol - No Credentials Provided
    Message     :
Credentials were not provided for detected SSH service.
```

## 57323 - OpenSSL Version Detection

### Synopsis

Nessus was able to detect the OpenSSL version.

### Description

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

### See Also

https://www.openssl.org/

### Solution

n/a

### Risk Factor

None

### References

|  |  |
|---|---|
| XREF | IAVT:0001-T-0682 |

### Plugin Information

Published: 2011/12/16, Modified: 2020/09/22

### Plugin Output

tcp/80/www

```
  Source             : Apache/2.4.37 (centos) OpenSSL/1.1.1k mod_fcgid/2.3.9
  Reported version   : 1.1.1k
  Backported version : 1.1.1k
```

## 57323 - OpenSSL Version Detection

### Synopsis

Nessus was able to detect the OpenSSL version.

### Description

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

### See Also

https://www.openssl.org/

### Solution

n/a

### Risk Factor

None

### References

| | |
|---|---|
| XREF | IAVT:0001-T-0682 |

### Plugin Information

Published: 2011/12/16, Modified: 2020/09/22

### Plugin Output

tcp/443/www

```
  Source             : Apache/2.4.37 (centos) OpenSSL/1.1.1k mod_fcgid/2.3.9
  Reported version   : 1.1.1k
  Backported version : 1.1.1k
```

## 48243 - PHP Version Detection

### Synopsis

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

### Description

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

### Solution

n/a

### Risk Factor

None

### References

| | |
|---|---|
| XREF | IAVT:0001-T-0936 |

### Plugin Information

Published: 2010/08/04, Modified: 2020/09/22

### Plugin Output

tcp/80/www

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

  Version : 7.2.24
  Source  : X-Powered-By: PHP/7.2.24
```

## 70657 - SSH Algorithms and Languages Supported

### Synopsis

An SSH server is listening on this port.

### Description

This script detects which algorithms and languages are supported by the remote service for encrypting communications.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2013/10/28, Modified: 2017/08/28

### Plugin Output

tcp/22/ssh

```
Nessus negotiated the following encryption algorithm with the server :

The server supports the following options for kex_algorithms :

  curve25519-sha256
  curve25519-sha256@libssh.org
  diffie-hellman-group-exchange-sha1
  diffie-hellman-group-exchange-sha256
  diffie-hellman-group14-sha1
  diffie-hellman-group14-sha256
  diffie-hellman-group16-sha512
  diffie-hellman-group18-sha512
  ecdh-sha2-nistp256
  ecdh-sha2-nistp384
  ecdh-sha2-nistp521

The server supports the following options for server_host_key_algorithms :

  ecdsa-sha2-nistp256
  rsa-sha2-256
  rsa-sha2-512
  ssh-ed25519
  ssh-rsa

The server supports the following options for encryption_algorithms_client_to_server :

  aes128-cbc
  aes128-ctr
  aes128-gcm@openssh.com
  aes256-cbc
  aes256-ctr
  aes256-gcm@openssh.com
  chacha20-poly1305@openssh.com

The server supports the following options for encryption_algorithms_server_to_client :

  aes128-cbc
  aes128-ctr
  aes128-gcm@openssh.com
  aes256-cbc
  aes256-ctr
  aes256-gcm@openssh.com
  chacha20-poly1305@openssh.com

The server supports the following options for mac_algorithms_client_to_server :

  hmac-sha1
  hmac-sha1-etm@openssh.com
  hmac-sha2-256
  hmac-sha2-256-etm@openssh.com
  hmac-sha2-512
  hmac-sha2-512-etm@openssh.com
  umac-128-etm@openssh.com
  umac-128@openssh.com

The server supports the following options for mac_algorithms_server_to_client :

  hmac-sha1
  hmac-sha1-etm@openssh.com
  hmac-sha2-256
  hmac-sha2-256-etm@openssh.com
  hmac-sha2-512
  hmac-sha2-512-etm@openssh.com
  umac-128-etm@openssh.com
  umac-128@openssh.com

The server supports the following options for compression_algorithms_client_to_server :

  none
  zlib@openssh.com

The server supports the following options for compression_algorithms_server_to_client :

  none
  zlib@openssh.com
```

## 149334 - SSH Password Authentication Accepted

### Synopsis

The SSH server on the remote host accepts password authentication.

### Description

The SSH server on the remote host accepts password authentication.

### See Also

https://tools.ietf.org/html/rfc4252#section-8

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2021/05/07, Modified: 2021/05/07

### Plugin Output

tcp/22/ssh

## 10881 - SSH Protocol Versions Supported

### Synopsis

A SSH server is running on the remote host.

### Description

This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2002/03/06, Modified: 2021/01/19

### Plugin Output

tcp/22/ssh

```
The remote SSH daemon supports the following versions of the
SSH protocol :

  - 1.99
  - 2.0
```

## 153588 - SSH SHA-1 HMAC Algorithms Enabled

### Synopsis

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

### Description

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Although NIST has formally deprecated use of SHA-1 for digital signatures, SHA-1 is still considered secure for HMAC as the security of HMAC does not rely on the underlying hash function being resistant to collisions.

Note that this plugin only checks for the options of the remote SSH server.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2021/09/23, Modified: 2022/04/05

### Plugin Output

tcp/22/ssh

```

The following client-to-server SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are
 supported :

  hmac-sha1
  hmac-sha1-etm@openssh.com

The following server-to-client SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are
 supported :

  hmac-sha1
  hmac-sha1-etm@openssh.com
```

## 10267 - SSH Server Type and Version Information

### Synopsis

An SSH server is listening on this port.

### Description

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

### Solution

n/a

### Risk Factor

None

### References

| | |
|---|---|
| XREF | IAVT:0001-T-0933 |

### Plugin Information

Published: 1999/10/12, Modified: 2020/09/22

### Plugin Output

tcp/22/ssh

```
SSH version : SSH-2.0-OpenSSH_8.0
SSH supported authentication : publickey,gssapi-keyex,gssapi-with-mic,password
```

## 56984 - SSL / TLS Versions Supported

### Synopsis

The remote service encrypts communications.

### Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2011/12/01, Modified: 2021/02/03

### Plugin Output

tcp/443/www

```
This port supports TLSv1.3/TLSv1.2.
```

## 45410 - SSL Certificate 'commonName' Mismatch

### Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

### Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

### Solution

If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

### Risk Factor

None

### Plugin Information

Published: 2010/04/03, Modified: 2021/03/09

### Plugin Output

tcp/443/www

```

The host name known by Nessus is :

  office.paper

The Common Name in the certificate is :

  localhost.localdomain

The Subject Alternate Name in the certificate is :

  localhost.localdomain
```

## 10863 - SSL Certificate Information

### Synopsis

This plugin displays the SSL certificate.

### Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

### Plugin Output

tcp/443/www

```
Subject Name:

Country: US
Organization: Unspecified
Common Name: localhost.localdomain
Email Address: root@localhost.localdomain

Issuer Name:

Country: US
Organization: Unspecified
Organization Unit: ca-3899279223185377061
Common Name: localhost.localdomain
Email Address: root@localhost.localdomain

Serial Number: 76 BC B0 E9 E8 AB 75 45

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jul 03 08:52:34 2021 GMT
Not Valid After: Jul 08 10:32:34 2022 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 BD 7F DE 7D 69 66 F1 60 79 7D 63 6B FC 3C E2 33 71 4F 63
            5C 06 4B B1 B3 90 D8 9D 82 9E 0A 5A A7 73 17 BB 9B 89 B3 FA
            6C B8 B8 FE 89 D6 40 4F E4 CB 9D 2D EE 94 13 AD 8A 15 7D E9
            19 CE 87 0A 9D 86 D0 27 40 D6 04 26 E1 66 20 17 61 3B 68 B3
            47 64 FA CA 43 EA F5 7E A0 41 C3 AA 37 36 43 71 4B 89 9A 5C
            3E C0 BE B0 AA 92 0A 48 0F FA 92 CE 23 09 75 4C EC F6 64 BE
            35 3C D6 AB 42 2E 4A C4 F3 B4 BA 71 50 41 6F ED 3E 97 3C 69
            12 E7 FA 44 DA 13 D6 3B 4B F3 FC 17 79 05 82 FE DC FD 3C 7C
            FB 02 D3 FE 58 BE 09 15 BA F1 5B 16 BC 66 B8 E1 4E 4C 49 2B
            4F 2F 3C 6F 67 CB 91 BB 7C FD 97 A1 E0 B4 9D 99 0A AB 89 2A
            71 0E 76 A0 D6 2D CD FB ED 5A 0E 42 21 02 16 C0 2C F2 BE AD
            9A BD 3E 65 14 15 56 3D 32 A8 B3 04 48 B1 C5 1B D6 85 A5 3D
            81 73 08 CB D6 67 3C 93 E9 8C 3A B2 BE 3B B9 7B E9
Exponent: 01 00 01

Signature Length: 512 bytes / 4096 bits
Signature: 00 B0 E2 E4 1F 51 EF 85 B6 C3 DD 4F 47 97 88 B1 E0 FF 99 17
           04 69 FC 91 F2 59 E3 98 4F 81 CB B0 6B 92 5F 01 07 80 DC 95
           F1 EE 98 93 4A 23 0C 93 41 AB 59 BA 9B AE 95 FD 64 89 30 3E
           76 6B 37 EF 4F 57 DF D2 34 21 09 55 33 32 F8 B0 D0 40 6B 32
           AB 09 19 A4 C2 BC 41 38 73 C5 1B D7 BE 7C 9F DD 77 84 14 32
           FA 37 86 1E 13 35 B3 E3 B5 4D 95 D7 5E A8 E0 47 9A B0 C8 E5
           22 FE 12 26 E1 C3 13 63 F5 45 F0 84 4C 92 52 [...]
```

## 70544 - SSL Cipher Block Chaining Cipher Suites Supported

### Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

### Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

### See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

http://www.nessus.org/u?cc4a822a

https://www.openssl.org/~bodo/tls-cbc.txt

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2013/10/22, Modified: 2021/02/03

### Plugin Output

tcp/443/www

```

Here is the list of SSL CBC ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DHE-RSA-AES128-SHA            0x00, 0x33       DH            RSA      AES-CBC(128)
 SHA1
    DHE-RSA-AES256-SHA            0x00, 0x39       DH            RSA      AES-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)
 SHA1
    AES128-SHA                    0x00, 0x2F       RSA           RSA      AES-CBC(128)
 SHA1
```

```
      AES256-SHA                    0x00, 0x35       RSA           RSA      AES-CBC(256)
   SHA1
      DHE-RSA-AES128-SHA256         0x00, 0x67       DH            RSA      AES-CBC(128)
   SHA256
      DHE-RSA-AES256-SHA256         0x00, 0x6B       DH            RSA      AES-CBC(256)
   SHA256
      ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA      AES-CBC(128)
   SHA256
      RSA-AES128-SHA256             0x00, 0x3C       RSA           RSA      AES-CBC(128)
   SHA256
      RSA-AES256-SHA256             0x00, 0x3D       RSA           RSA      AES-CBC(256)
   SHA256

  The fields above are :

    {Tenable ciphername}
    {Cipher ID code}
    Kex={key exchange}
    Auth={authentication}
    Encrypt={symmetric encryption method}
    MAC={message authentication code}
    {export flag}
```

## 21643 - SSL Cipher Suites Supported

### Synopsis

The remote service encrypts communications using SSL.

### Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

### See Also

https://www.openssl.org/docs/man1.1.0/apps/ciphers.html

http://www.nessus.org/u?3a040ada

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2006/06/05, Modified: 2021/03/09

### Plugin Output

tcp/443/www

```

Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv13
  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    TLS_AES_128_CCM_SHA256        0x13, 0x04        -             -       AES-CCM(128)
 AEAD
    TLS_AES_128_GCM_SHA256        0x13, 0x01        -             -       AES-GCM(128)
 AEAD
    TLS_AES_256_GCM_SHA384        0x13, 0x02        -             -       AES-GCM(256)
 AEAD
    TLS_CHACHA20_POLY1305_SHA256  0x13, 0x03        -             -       ChaCha20-Poly1305(256)
 AEAD


SSL Version : TLSv12
  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
```

```
   DHE-RSA-AES-128-CCM-AEAD      0xC0, 0x9E       DH            RSA      AES-CCM(128)
AEAD
   DHE-RSA-AES128-SHA256         0x00, 0x9E       DH            RSA      AES-GCM(128)
SHA256
   DHE-RSA-AES-256-CCM-AEAD      0xC0, 0x9F       DH            RSA      AES-CCM(256)
AEAD
   DHE-RSA-AES256-SHA384         0x00, 0x9F       DH            RSA      AES-GCM(256)
SHA384
   DHE-RSA-CHACHA20-POLY1305     0xCC, 0xAA       DH            RSA      ChaCha20-Poly1305(256)
SHA256
   ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
SHA256
   ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(256)
SHA384
   ECDHE-RSA-CHACHA20-POLY1305   0xCC, 0xA8       ECDH          RSA      ChaCha20-Poly1305(256)
SHA256
   RSA-AES-128-CCM-AEAD          0xC0, 0x9C       RSA           RSA      AES-CCM(128)
AEAD
   RSA-AES128-SHA256             0x00, 0x9C       RSA           RSA     [...]
```

## 57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

### Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

### Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

### See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

### Plugin Output

tcp/443/www

```
Here is the list of SSL PFS ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DHE-RSA-AES-128-CCM-AEAD      0xC0, 0x9E       DH            RSA      AES-CCM(128)
 AEAD
    DHE-RSA-AES128-SHA256         0x00, 0x9E       DH            RSA      AES-GCM(128)
 SHA256
    DHE-RSA-AES-256-CCM-AEAD      0xC0, 0x9F       DH            RSA      AES-CCM(256)
 AEAD
    DHE-RSA-AES256-SHA384         0x00, 0x9F       DH            RSA      AES-GCM(256)
 SHA384
    DHE-RSA-CHACHA20-POLY1305     0xCC, 0xAA       DH            RSA      ChaCha20-Poly1305(256)
 SHA256
```

```
      ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
   SHA256
      ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(256)
   SHA384
      ECDHE-RSA-CHACHA20-POLY1305   0xCC, 0xA8       ECDH          RSA      ChaCha20-Poly1305(256)
   SHA256
      DHE-RSA-AES128-SHA            0x00, 0x33       DH            RSA      AES-CBC(128)
   SHA1
      DHE-RSA-AES256-SHA            0x00, 0x39       DH            RSA      AES-CBC(256)
   SHA1
      ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
   SHA1
      ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)
   SHA1
      DHE-RSA-AES128-SHA256         0x00, 0x67       DH            RSA      AES-CBC(128)
   SHA256
      DHE-RSA-AES256-SHA256         0x00, 0x6B       DH            RSA      AES-CBC(256)
   SHA256
      ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA      AES-CBC(128)
   SHA256

  The fields above are :

    {Tenable ciphername}
    {Cipher ID code}
    Kex={key exchange}
    Auth={authentication}
    Encrypt={symmetric encryption method}
    MAC={message authentication code [...]
```

## 94761 - SSL Root Certification Authority Certificate Information

### Synopsis

A root Certification Authority certificate was found at the top of the certificate chain.

### Description

The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain.

### See Also

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10)

### Solution

Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.

### Risk Factor

None

### Plugin Information

Published: 2016/11/14, Modified: 2018/11/15

### Plugin Output

tcp/443/www

```
The following root Certification Authority certificate was found :

|-Subject             : C=US/O=Unspecified/OU=ca-3899279223185377061/CN=localhost.localdomain/
E=root@localhost.localdomain
|-Issuer              : C=US/O=Unspecified/OU=ca-3899279223185377061/CN=localhost.localdomain/
E=root@localhost.localdomain
|-Valid From          : Jul 03 08:52:34 2021 GMT
|-Valid To            : Jul 08 10:32:34 2022 GMT
|-Signature Algorithm : SHA-256 With RSA Encryption
```

## 156899 - SSL/TLS Recommended Cipher Suites

### Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

### Description

The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:

TLSv1.3:

- 0x13,0x01 TLS_AES_128_GCM_SHA256
- 0x13,0x02 TLS_AES_256_GCM_SHA384
- 0x13,0x03 TLS_CHACHA20_POLY1305_SHA256

TLSv1.2:

- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256
- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256
- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384
- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384
- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305
- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305
- 0x00,0x9E DHE-RSA-AES128-GCM-SHA256
- 0x00,0x9F DHE-RSA-AES256-GCM-SHA384

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

### See Also

https://wiki.mozilla.org/Security/Server_Side_TLS

https://ssl-config.mozilla.org/

### Solution

Only enable support for recommened cipher suites.

### Risk Factor

None

### Plugin Information

Published: 2022/01/20, Modified: 2022/04/06

## Plugin Output

### tcp/443/www

```
The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined
 below:


  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DHE-RSA-AES-128-CCM-AEAD      0xC0, 0x9E       DH            RSA      AES-CCM(128)
 AEAD
    DHE-RSA-AES-256-CCM-AEAD      0xC0, 0x9F       DH            RSA      AES-CCM(256)
 AEAD
    DHE-RSA-CHACHA20-POLY1305     0xCC, 0xAA       DH            RSA      ChaCha20-Poly1305(256)
 SHA256
    RSA-AES-128-CCM-AEAD          0xC0, 0x9C       RSA           RSA      AES-CCM(128)
 AEAD
    RSA-AES128-SHA256             0x00, 0x9C       RSA           RSA      AES-GCM(128)
 SHA256
    RSA-AES-256-CCM-AEAD          0xC0, 0x9D       RSA           RSA      AES-CCM(256)
 AEAD
    RSA-AES256-SHA384             0x00, 0x9D       RSA           RSA      AES-GCM(256)
 SHA384
    DHE-RSA-AES128-SHA            0x00, 0x33       DH            RSA      AES-CBC(128)
 SHA1
    DHE-RSA-AES256-SHA            0x00, 0x39       DH            RSA      AES-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)
 SHA1
    AES128-SHA                    0x00, 0x2F       RSA           RSA      AES-CBC(128)
 SHA1
    AES256-SHA                    0x00, 0x35       RSA           RSA      AES-CBC(256)
 SHA1
    DHE-RSA-AES128-SHA256         0x00, 0x67       DH            RSA      AES-CBC(128)
 SHA256
    DHE-RSA-AES256-SHA256         0x00, 0x6B       DH            RSA      AES-CBC(256)
 SHA256
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA      AES-CBC(128)
 SHA256
    RSA-AES128-SHA256             0x00, 0x3C       RS [...]
```

## 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: 2021/04/14

### Plugin Output

tcp/22/ssh

```
An SSH server is running on this port.
```

## 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: 2021/04/14

### Plugin Output

tcp/80/www

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

## 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: 2021/04/14

### Plugin Output

tcp/443/www

```
A TLSv1.2 server answered on this port.
```

tcp/443/www

```
A web server is running on this port through TLSv1.2.
```

## 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

## 84821 - TLS ALPN Supported Protocol Enumeration

### Synopsis

The remote host supports the TLS ALPN extension.

### Description

The remote host supports the TLS ALPN extension. This plugin enumerates the protocols the extension supports.

### See Also

https://tools.ietf.org/html/rfc7301

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2015/07/17, Modified: 2021/02/03

### Plugin Output

tcp/443/www

```
http/1.1
```

## 136318 - TLS Version 1.2 Protocol Detection

### Synopsis

The remote service encrypts traffic using a version of TLS.

### Description

The remote service accepts connections encrypted using TLS 1.2.

### See Also

https://tools.ietf.org/html/rfc5246

### Solution

N/A

### Risk Factor

None

### Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

### Plugin Output

tcp/443/www

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

## 138330 - TLS Version 1.3 Protocol Detection

### Synopsis

The remote service encrypts traffic using a version of TLS.

### Description

The remote service accepts connections encrypted using TLS 1.3.

### See Also

https://tools.ietf.org/html/rfc8446

### Solution

N/A

### Risk Factor

None

### Plugin Information

Published: 2020/07/09, Modified: 2020/07/09

### Plugin Output

tcp/443/www

```
TLSv1.3 is enabled and the server supports at least one cipher.
```

## 110723 - Target Credential Status by Authentication Protocol - No Credentials Provided

### Synopsis

Nessus was able to find common ports used for local checks, however, no credentials were provided in the scan policy.

### Description

Nessus was not able to successfully authenticate directly to the remote target on an available authentication protocol. Nessus was able to connect to the remote port and identify that the service running on the port supports an authentication protocol, but Nessus failed to authenticate to the remote service using the provided credentials. There may have been a protocol failure that prevented authentication from being attempted or all of the provided credentials for the authentication protocol may be invalid. See plugin output for error details.

Please note the following :

- This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service.

- Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets than for Linux targets.

### Solution

n/a

### Risk Factor

None

### References

| | |
|---|---|
| XREF | IAVB:0001-B-0504 |

### Plugin Information

Published: 2018/06/27, Modified: 2021/11/19

### Plugin Output

tcp/0

```
SSH was detected on port 22 but no credentials were provided.
SSH local checks were not enabled.
```

## 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 10.10.14.185 to 10.10.11.143 :
10.10.14.185
10.10.14.1
10.10.11.143

Hop Count: 2
```

## 100669 - Web Application Cookies Are Expired

### Synopsis

HTTP cookies have an 'Expires' attribute that is set with a past date or time.

### Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, Nessus has detected that one or more of the cookies have an 'Expires' attribute that is set with a past date or time, meaning that these cookies will be removed by the browser.

### See Also

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

### Solution

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

If needed, set an expiration date in the future so the cookie will persist or remove the Expires cookie attribute altogether to convert the cookie to a session cookie.

### Risk Factor

None

### Plugin Information

Published: 2017/06/07, Modified: 2021/12/20

### Plugin Output

tcp/80/www

```

The following cookies are expired :

Name : wp-settings-0
Path : /
Value : +
Domain :
Version : 1
Expires : Sat, 10-Apr-2021 22:17:50 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : wordpress_logged_in_075942c5921a9d16d1b67219d6575363
Path : /
Value : +
Domain :
Version : 1
Expires : Sat, 10-Apr-2021 22:17:50 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : wordpress_075942c5921a9d16d1b67219d6575363
Path : /wp-content/plugins
Value : +
Domain :
Version : 1
Expires : Sat, 10-Apr-2021 22:17:50 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : wordpress_sec_075942c5921a9d16d1b67219d6575363
Path : /wp-content/plugins
Value : +
Domain :
Version : 1
Expires : Sat, 10-Apr-2021 22:17:50 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : wordpresspass_075942c5921a9d16d1b67219d6575363
Path : /
Value : +
Domain :
Version : 1
Expires : Sat, 10-Apr-2021 22:17:50 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : wp-settings-time-0
Path : /
Value : +
Domain :
Version : 1
Expires : Sat, 10-Apr-2021 22:17:50 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : wp-postpass_075942c5921a9d16d1b67219d6575363
Path : /
Value : +
Domain :
Version : 1
Expires : Sat, 10-Apr-2021 22:17:50 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : wordpress_075942c5921a9d16d1b67219d6575363
```

```
Path : /
Value : +
Domain :
Version : 1
Expires : Sat, 10-Apr-2021 22:17:50 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : wordpress_sec_075942c5921a9d16d1b67219d6575363
Path : /wp-admin
Value : +
Domain :
Version : 1
Expires : Sat, 10-Apr-2021 22:17:50 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : wordpress_075942c5921a9d16d1b67219d6575363
Path : /wp-admin
Value : +
Domain :
Version : 1
Expires : Sat, 10-Apr-2021 22:17:50 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : wordpress_sec_075942c5921a9d16d1b67219d6575363
Path : /
Value : +
Domain :
Version : 1
Expires : Sat, 10-Apr-2021 22:17:50 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : wordpressuser_075942c5921a9d16d1b67219d65 [...]
```

# 100669 - Web Application Cookies Are Expired

## Synopsis

HTTP cookies have an 'Expires' attribute that is set with a past date or time.

## Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, Nessus has detected that one or more of the cookies have an 'Expires' attribute that is set with a past date or time, meaning that these cookies will be removed by the browser.

## See Also

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

## Solution

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

If needed, set an expiration date in the future so the cookie will persist or remove the Expires cookie attribute altogether to convert the cookie to a session cookie.

## Risk Factor

None

## Plugin Information

Published: 2017/06/07, Modified: 2021/12/20

## Plugin Output

tcp/443/www

```

The following cookies are expired :

Name : wp-settings-0
Path : /
Value : +
Domain :
Version : 1
Expires : Sat, 10-Apr-2021 22:17:50 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : wordpress_logged_in_075942c5921a9d16d1b67219d6575363
Path : /
Value : +
Domain :
Version : 1
Expires : Sat, 10-Apr-2021 22:17:50 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : wordpress_075942c5921a9d16d1b67219d6575363
Path : /wp-content/plugins
Value : +
Domain :
Version : 1
Expires : Sat, 10-Apr-2021 22:17:50 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : wordpress_sec_075942c5921a9d16d1b67219d6575363
Path : /wp-content/plugins
Value : +
Domain :
Version : 1
Expires : Sat, 10-Apr-2021 22:17:50 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : wordpresspass_075942c5921a9d16d1b67219d6575363
Path : /
Value : +
Domain :
Version : 1
Expires : Sat, 10-Apr-2021 22:17:50 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : wp-settings-time-0
Path : /
Value : +
Domain :
Version : 1
Expires : Sat, 10-Apr-2021 22:17:50 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : wp-postpass_075942c5921a9d16d1b67219d6575363
Path : /
Value : +
Domain :
Version : 1
Expires : Sat, 10-Apr-2021 22:17:50 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : wordpress_075942c5921a9d16d1b67219d6575363
```

```
Path : /
Value : +
Domain :
Version : 1
Expires : Sat, 10-Apr-2021 22:17:50 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : wordpress_sec_075942c5921a9d16d1b67219d6575363
Path : /wp-admin
Value : +
Domain :
Version : 1
Expires : Sat, 10-Apr-2021 22:17:50 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : wordpress_075942c5921a9d16d1b67219d6575363
Path : /wp-admin
Value : +
Domain :
Version : 1
Expires : Sat, 10-Apr-2021 22:17:50 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : wordpress_sec_075942c5921a9d16d1b67219d6575363
Path : /
Value : +
Domain :
Version : 1
Expires : Sat, 10-Apr-2021 22:17:50 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : wordpressuser_075942c5921a9d16d1b67219d65 [...]
```

## 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 cookie does not set the HttpOnly cookie flag :

Name : wordpress_test_cookie
Path : /
Value : WP+Cookie+check
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :

```

## 85601 - Web Application Cookies Not Marked HttpOnly

### Synopsis

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

### Description

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

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

### See Also

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

### Solution

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

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

### Risk Factor

None

### References

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

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

## Plugin Information

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

## Plugin Output

tcp/443/www

```
The following cookie does not set the HttpOnly cookie flag :

Name : wordpress_test_cookie
Path : /
Value : WP+Cookie+check
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 cookie does not set the secure cookie flag :

Name : wordpress_test_cookie
Path : /
Value : WP+Cookie+check
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :
```

## 85602 - Web Application Cookies Not Marked Secure

### Synopsis

HTTP session cookies might be transmitted in cleartext.

### Description

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

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

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

### See Also

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

### Solution

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

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

### Risk Factor

None

### References

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

### Plugin Information

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

### Plugin Output

tcp/443/www

```
The following cookie does not set the secure cookie flag :

Name : wordpress_test_cookie
Path : /
Value : WP+Cookie+check
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 /wp-login.php :

pwd : 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://10.10.11.143/
  - http://10.10.11.143/index.php/2021/
  - http://10.10.11.143/index.php/2021/06/
  - http://10.10.11.143/index.php/2021/06/19/
  - http://10.10.11.143/index.php/2021/06/19/feeling-alone/
  - http://10.10.11.143/index.php/2021/06/19/hello-scranton/
  - http://10.10.11.143/index.php/2021/06/19/secret-of-my-success/
  - http://10.10.11.143/index.php/author/prisonmike/
  - http://10.10.11.143/index.php/author/prisonmike/feed/
  - http://10.10.11.143/index.php/category/uncategorized/
  - http://10.10.11.143/index.php/category/uncategorized/feed/
  - http://10.10.11.143/index.php/comments/feed/
  - http://10.10.11.143/index.php/feed/
  - http://10.10.11.143/index.php/wp-json
  - http://10.10.11.143/index.php/wp-json/
  - http://10.10.11.143/index.php/wp-json/oembed/1.0
  - http://10.10.11.143/manual/
  - http://10.10.11.143/manual/bind.html
  - http://10.10.11.143/manual/caching.html
  - http://10.10.11.143/manual/configuring.html
  - http://10.10.11.143/manual/content-negotiation.html
  - http://10.10.11.143/manual/custom-error.html
```

```
    - http://10.10.11.143/manual/developer/
    - http://10.10.11.143/manual/developer/API.html
    - http://10.10.11.143/manual/developer/documenting.html
    - http://10.10.11.143/manual/developer/filters.html
    - http://10.10.11.143/manual/developer/hooks.html
    - http://10.10.11.143/manual/developer/modguide.html
    - http://10.10.11.143/manual/developer/modules.html
    - http://10.10.11.143/manual/developer/new_api_2_4.html
    - http://10.10.11.143/manual/developer/output-filters.html
    - http://10.10.11.143/manual/developer/request.html
    - http://10.10.11.143/manual/developer/thread_safety.html
    - http://10.10.11.143/manual/dns-caveats.html
    - http://10.10.11.143/manual/dso.html
    - http://10.10.11.143/manual/expr.html
    - http://10.10.11.143/manual/filter.html
    - http://10.10.11.143/manual/getting-started.html
    - http://10.10.11.143/manual/glossary.html
    - http://10.10.11.143 [...]
```

## 91815 - Web Application Sitemap

### Synopsis

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

### Description

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

### See Also

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/443/www

```

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

  - https://10.10.11.143/manual/
  - https://10.10.11.143/manual/bind.html
  - https://10.10.11.143/manual/caching.html
  - https://10.10.11.143/manual/configuring.html
  - https://10.10.11.143/manual/content-negotiation.html
  - https://10.10.11.143/manual/custom-error.html
  - https://10.10.11.143/manual/developer/
  - https://10.10.11.143/manual/developer/API.html
  - https://10.10.11.143/manual/developer/documenting.html
  - https://10.10.11.143/manual/developer/filters.html
  - https://10.10.11.143/manual/developer/hooks.html
  - https://10.10.11.143/manual/developer/modguide.html
  - https://10.10.11.143/manual/developer/modules.html
  - https://10.10.11.143/manual/developer/new_api_2_4.html
  - https://10.10.11.143/manual/developer/output-filters.html
  - https://10.10.11.143/manual/developer/request.html
  - https://10.10.11.143/manual/developer/thread_safety.html
  - https://10.10.11.143/manual/dns-caveats.html
  - https://10.10.11.143/manual/dso.html
  - https://10.10.11.143/manual/expr.html
  - https://10.10.11.143/manual/filter.html
  - https://10.10.11.143/manual/getting-started.html
```

```
    - https://10.10.11.143/manual/glossary.html
    - https://10.10.11.143/manual/handler.html
    - https://10.10.11.143/manual/howto/
    - https://10.10.11.143/manual/howto/access.html
    - https://10.10.11.143/manual/howto/auth.html
    - https://10.10.11.143/manual/howto/cgi.html
    - https://10.10.11.143/manual/howto/htaccess.html
    - https://10.10.11.143/manual/howto/http2.html
    - https://10.10.11.143/manual/howto/public_html.html
    - https://10.10.11.143/manual/howto/reverse_proxy.html
    - https://10.10.11.143/manual/howto/ssi.html
    - https://10.10.11.143/manual/images/
    - https://10.10.11.143/manual/images/apache_header.gif
    - https://10.10.11.143/manual/images/bal-man-b.png
    - https://10.10.11.143/manual/images/bal-man-w.png
    - https://10.10.11.143/manual/images/bal-man.png
    - https://10.10.11.143/manual/images/build_a_mod_2.png
    [...]
```

## 11032 - Web Server Directory Enumeration

### Synopsis

It is possible to enumerate directories on the web server.

### Description

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

### See Also

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

### Solution

n/a

### Risk Factor

None

### References

| | |
|---|---|
| XREF | OWASP:OWASP-CM-006 |

### Plugin Information

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

### Plugin Output

tcp/80/www

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

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

## 11032 - Web Server Directory Enumeration

### Synopsis

It is possible to enumerate directories on the web server.

### Description

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

### See Also

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

### Solution

n/a

### Risk Factor

None

### References

| | |
|---|---|
| XREF | OWASP:OWASP-CM-006 |

### Plugin Information

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

### Plugin Output

tcp/443/www

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

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 :


- 'raj@cup.hp.com', referenced from :
   /manual/platform/perf-hp.html

- 'users@httpd.apache.org', referenced from :
   /manual/ssl/ssl_faq.html
```

## 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/443/www

```

The following email addresses have been gathered :


- 'raj@cup.hp.com', referenced from :
   /manual/platform/perf-hp.html

- 'users@httpd.apache.org', referenced from :
   /manual/ssl/ssl_faq.html
```

## 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: 2022/04/06

### Plugin Output

tcp/80/www

```

Webmirror performed 1000 queries in 171s (5.0847 queries per second)

The following CGIs have been discovered :


+ CGI : /xmlrpc.php
  Methods : GET
  Argument :
   Value: rsd


+ CGI : /
  Methods : GET
  Argument : p
   Value: 29
  Argument : s


+ CGI : /index.php/wp-json/oembed/1.0/embed
  Methods : GET
  Argument : url
   Value: http%3A%2F%2Foffice.paper%2Findex.php%2F2021%2F06%2F19%2Fhello-scranton%2F


+ CGI : /wp-login.php
  Methods : GET,POST
  Argument : action
```

```
   Value: lostpassword
  Argument : log
  Argument : pwd
  Argument : reauth
   Value: 1
  Argument : redirect_to
   Value: http%3A%2F%2Foffice.paper%2Fwp-admin%2F
  Argument : rememberme
   Value: forever
  Argument : testcookie
   Value: 1
  Argument : wp-submit
   Value: Log In

Directory index found at /manual/style/css/
Directory index found at /manual/style/
Directory index found at /manual/images/
Directory index found at /manual/style/lang/
Directory index found at /manual/style/latex/
Directory index found at /manual/style/scripts/
Directory index found at /manual/style/xsl/
```

## 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: 2022/04/06

### Plugin Output

tcp/443/www

```
Webmirror performed 1000 queries in 163s (6.0134 queries per second)

The following CGIs have been discovered :

Directory index found at /manual/style/css/
Directory index found at /manual/style/
Directory index found at /manual/images/
Directory index found at /manual/style/lang/
Directory index found at /manual/style/latex/
Directory index found at /manual/style/scripts/
Directory index found at /manual/style/xsl/
```

## 18297 - WordPress Detection

### Synopsis

The remote web server contains a blog application written in PHP.

### Description

The remote host is running WordPress, a free blog application written in PHP with a MySQL back-end.

### See Also

https://wordpress.org/

### Solution

n/a

### Risk Factor

None

### References

| | |
|---|---|
| XREF | IAVT:0001-T-0747 |

### Plugin Information

Published: 2005/05/18, Modified: 2021/08/11

### Plugin Output

tcp/80/www

```
  URL     : http://10.10.11.143/
  Version : 5.2.3
```