



# MCUXpresso Web SDK builder complex scan

---

Report generated by Nessus™

Wed, 23 Mar 2022 13:33:30 CDT

---

---

## TABLE OF CONTENTS

---

### Vulnerabilities by Host

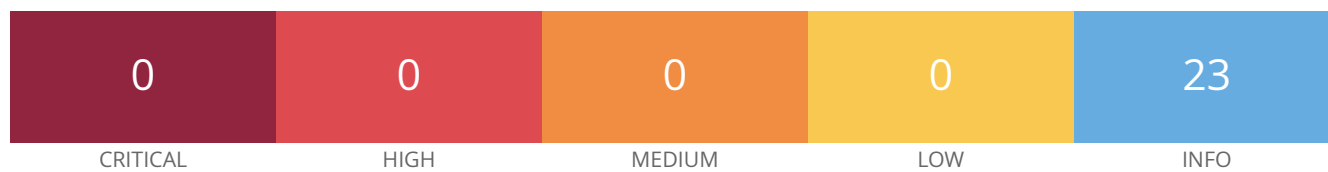
• mcuxpresso.nxp.com.....	4
---------------------------	---

---

## **Vulnerabilities by Host**

---

## mcuxpresso.nxp.com



### Scan Information

Start time: Wed Mar 23 12:44:36 2022

End time: Wed Mar 23 13:33:29 2022

### Host Information

DNS Name: mcuxpresso.nxp.com

IP: 23.37.33.215

### Vulnerabilities

#### 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://mcuxpresso.nxp.com/  
Version  : unknown  
backported : 0
```

## 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://mcuxpresso.nxp.com/  
Version  : unknown  
backported : 0
```

## 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/443/www

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

injectable parameter           : S=4          SP=4          AP=4          SC=4          AC=4
blind SQL injection (4 requests) : S=8          SP=8          AP=8          SC=8          AC=8
arbitrary command execution (time based) : S=12         SP=12         AP=12         SC=12         AC=12
cross-site scripting (comprehensive test): S=34         SP=34         AP=34         SC=34         AC=34
directory traversal (extended test) : S=102        SP=102        AP=102        SC=102
AC=102
arbitrary command execution     : S=44         SP=44         AP=44         SC=44         AC=44
local file inclusion           : S=8          SP=8          AP=8          SC=8          AC=8
web code injection             : S=2          SP=2          AP=2          SC=2          AC=2
SQL injection                   : S=56         SP=56         AP=56         SC=56         AC=56
```

directory traversal (write access)	: S=4	SP=4	AP=4	SC=4	AC=4
unseen parameters	: S=70	SP=70	AP=70	SC=70	AC=70
format string	: S=4	SP=4	AP=4	SC=4	AC=4
directory traversal	: S=58	SP=58	AP=58	SC=58	AC=58
XML injection	: S=2	SP=2	AP=2	SC=2	AC=2
persistent XSS	: S=8	SP=8	AP=8	SC=8	AC=8
SSI injection	: S=6	SP=6	AP=6	SC=6	AC=6
SQL injection (2nd order)	: S=2	SP=2	AP=2	SC=2	AC=2
blind SQL injection	[...]				



## 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

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

http://www.nxp.com - /en/welcome
http://www.nxp.com/about/contact-us:CONTACTUS - /en/welcome
http://www.nxp.com/about/privacy:PRIVACYPRACTICES - /en/welcome
http://www.nxp.com/about/terms-of-use:TERMSOFUSE - /en/welcome
https://community.nxp.com/community/mcuxpresso - /en/welcome
https://community.nxp.com/community/mcuxpresso/mcuxpresso-config - /en/welcome
https://community.nxp.com/community/mcuxpresso/mcuxpresso-ide - /en/welcome
https://community.nxp.com/community/mcuxpresso/mcuxpresso-sdk - /en/welcome
https://community.nxp.com/community/mcuxpresso/mcuxpresso-secure-provisioning-tool - /en/welcome
https://www.nxp.com - /en/welcome
https://www.nxp.com/company/about-nxp/accessibility:ACCESSIBILITY - /en/welcome
https://www.nxp.com/mcuxpresso/secure - /en/welcome
https://www.nxp.com/support/developer-resources/run-time-software/mcuxpresso-software-and-tools/
mcuxpresso-config-tools:MCUXpresso-Config-Tools - /en/welcome
https://www.nxp.com/support/developer-resources/run-time-software/mcuxpresso-software-and-tools/
mcuxpresso-integrated-development-environment-ide:MCUXpresso-IDE - /en/welcome
https://www.nxp.com/support/developer-resources/run-time-software/mcuxpresso-software-and-tools/
mcuxpresso-software-development-kit-sdk:MCUXpresso-SDK - /en/welcome
```

## 84502 - HSTS Missing From HTTPS Server

### Synopsis

The remote web server is not enforcing HSTS.

### Description

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

### See Also

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

### Solution

Configure the remote web server to use HSTS.

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/443/www

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

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

### Synopsis

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

### Description

The remote web server sends out cookies to clients with a 'secure' property that does not match the transport, HTTP or HTTPS, over which they were received. This may occur in two forms :

1. The cookie is sent over HTTP, but has the 'secure' property set, indicating that it should only be sent over a secure, encrypted transport such as HTTPS. This should not happen.
2. The cookie is sent over HTTPS, but has no 'secure' property set, indicating that it may be sent over both HTTP and HTTPS transports. This is common, but care should be taken to ensure that the 'secure' property not being set is deliberate.

### See Also

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/80/www

The following cookie has the 'secure' property enabled, despite being served over HTTP :

```
Domain    :
Path      : /
Name      : session
Value     :
eyJkQVNFQUZURVJfTE9HSU5fU0VlU01PTl9VUkwiOiIvemgvZGFzaGJvYXJkIn0.YjthTg.ywY_7yIKs1N5sLzPTkDMrSUJ2Js
Secure    : true
```

```
HttpOnly : true
```

## 43111 - HTTP Methods Allowed (per directory)

### Synopsis

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

### Description

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

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

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

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

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

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

### See Also

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

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

[https://www.owasp.org/index.php/Test\\_HTTP\\_Methods\\_\(OTG-CONFIG-006\)](https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006))

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/80/www

Based on tests of each method :

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

/

## 43111 - HTTP Methods Allowed (per directory)

### Synopsis

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

### Description

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

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

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

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

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

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

### See Also

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

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

[https://www.owasp.org/index.php/Test\\_HTTP\\_Methods\\_\(OTG-CONFIG-006\)](https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006))

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/443/www

Based on the response to an OPTIONS request :

- HTTP methods GET OPTIONS HEAD are allowed on :

/zh

- HTTP methods HEAD OPTIONS GET are allowed on :

/

/en

- HTTP methods GET HEAD OPTIONS POST are allowed on :

/icons  
/static  
/static/fontawesome  
/static/fontawesome/css  
/static/generated  
/static/icon  
/static/translations

Based on tests of each method :

- HTTP methods GET HEAD OPTIONS are allowed on :

/

- HTTP methods GET HEAD OPTIONS POST are allowed on :

/icons  
/static  
/static/fontawesome  
/static/fontawesome/css  
/static/generated  
/static/icon  
/static/translations

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

/en  
/zh



## 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
```

## 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
```

## 24260 - HyperText Transfer Protocol (HTTP) Information

### Synopsis

Some information about the remote HTTP configuration can be extracted.

### Description

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

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/80/www

Response Code : HTTP/1.1 302 Moved Temporarily

Protocol version : HTTP/1.1

SSL : no

Keep-Alive : no

Options allowed : (Not implemented)

Headers :

Server: Apache

Location: https://mcuxpresso.nxp.com/

Content-Length: 211

Content-Type: text/html; charset=iso-8859-1

Cache-Control: max-age=0

Expires: Wed, 23 Mar 2022 18:15:20 GMT

Date: Wed, 23 Mar 2022 18:15:20 GMT

Connection: keep-alive

Server-Timing: cdn-cache; desc=MISS

Server-Timing: edge; dur=99

Server-Timing: origin; dur=50

Response Body :

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">

<html><head>

<title>302 Found</title>

</head><body>

<h1>Found</h1>

```
<p>The document has moved <a href="https://mcuxpresso.nxp.com/">here</a>.</p>  
</body></html>
```

## 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/1.1 302 Moved Temporarily

Protocol version : HTTP/1.1

SSL : yes

Keep-Alive : no

Options allowed : (Not implemented)

Headers :

Server: Apache

Content-Length: 214

Location: <https://mcuxpresso.nxp.com/en/>

X-XSS-Protection: 1; mode=block

X-Frame-Options: sameorigin

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

Cache-Control: max-age=0

Expires: Wed, 23 Mar 2022 18:15:21 GMT

Date: Wed, 23 Mar 2022 18:15:21 GMT

Connection: keep-alive

Server-Timing: cdn-cache; desc=MISS

Server-Timing: edge; dur=98

Server-Timing: origin; dur=54

Response Body :

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">

<title>Redirecting...</title>

<h1>Redirecting...</h1>

<p>You should be redirected automatically to target URL: <a href="/en/">/en/</a>. If not click the link.

## 91634 - HyperText Transfer Protocol (HTTP) Redirect Information

### Synopsis

The remote web server redirects requests to the root directory.

### Description

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

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

### Solution

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

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/80/www

```
Request      : http://mcuxpresso.nxp.com/
HTTP response : HTTP/1.1 302 Moved Temporarily
Redirect to   : https://mcuxpresso.nxp.com/
Redirect type  : 30x redirect
```

Note that Nessus did not receive a 200 OK response from the last examined redirect.

## 91634 - HyperText Transfer Protocol (HTTP) Redirect Information

### Synopsis

The remote web server redirects requests to the root directory.

### Description

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

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

### Solution

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

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/443/www

```
Request      : https://mcuxpresso.nxp.com/
HTTP response : HTTP/1.1 302 Moved Temporarily
Redirect to   : https://mcuxpresso.nxp.com/en/
Redirect type  : 30x redirect

Request      : https://mcuxpresso.nxp.com/en/
HTTP response : HTTP/1.1 302 Moved Temporarily
Redirect to   : https://mcuxpresso.nxp.com/en/welcome
Redirect type  : 30x redirect

Final page    : https://mcuxpresso.nxp.com/en/welcome
HTTP response : HTTP/1.1 200 OK
```



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

### Synopsis

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

### Description

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

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

### See Also

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

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

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

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

### Solution

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

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/443/www

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

- <https://mcuxpresso.nxp.com/en/welcome>
- <https://mcuxpresso.nxp.com/zh/welcome>

### Synopsis

---

It is possible to determine which TCP ports are open.

### Description

---

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

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

### Solution

---

Protect your target with an IP filter.

### Risk Factor

---

None

### Plugin Information

---

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

### Plugin Output

---

tcp/80/www

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

### Synopsis

---

It is possible to determine which TCP ports are open.

### Description

---

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

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

### Solution

---

Protect your target with an IP filter.

### Risk Factor

---

None

### Plugin Information

---

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

### Plugin Output

---

tcp/443/www

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

### 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: 2021/09/27

### Plugin Output

tcp/0

Information about this scan :

```
Nessus version : 10.1.1
Nessus build : X20061
Plugin feed version : 202203221746
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : debian6-x86-64
Scan type : Normal
Scan name : MCUXpresso Web SDK builder complex scan
```

```
Scan policy used : MCUXpresso Web SDK builder complex scan
Scanner IP : 10.0.2.15

WARNING : No port scanner was enabled during the scan. This may
lead to incomplete results.

Port range : 1-65535
Ping RTT : 51.435 ms
Thorough tests : yes
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 did not launch)
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 : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2022/3/23 12:44 CDT
Scan duration : 2923 sec
```

### 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://mcuxpresso.nxp.com/en/welcome>
- <https://mcuxpresso.nxp.com/static/fontawesome/css/all.css>
- <https://mcuxpresso.nxp.com/static/generated/external.e9e510e2.min.css>
- <https://mcuxpresso.nxp.com/static/generated/internal.da2c2724.min.css>
- <https://mcuxpresso.nxp.com/static/icon/favicon.ico>
- <https://mcuxpresso.nxp.com/static/translations/zh.json>
- <https://mcuxpresso.nxp.com/zh/welcome>

Attached is a copy of the sitemap file.

## 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:  
/icons
```

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

## 10386 - Web Server No 404 Error Code Check

### Synopsis

The remote web server does not return 404 error codes.

### Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2000/04/28, Modified: 2020/06/12

### Plugin Output

tcp/80/www

```
CGI scanning will be disabled for this host because the host responds  
to requests for non-existent URLs with HTTP code 302  
rather than 404. The requested URL was :
```

```
http://mcuxpresso.nxp.com/forLKS3OD04g.html
```



### Synopsis

---

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

### Description

---

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

### See Also

---

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

### Solution

---

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

### Risk Factor

---

None

### Plugin Information

---

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

### Plugin Output

---

tcp/443/www

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

```
User-agent: *  
Allow: /login  
Allow: /apidoc  
Allow: /api_doc  
Allow: /*/welcome  
Allow: /*/apidoc  
Allow: /*/getdoc  
Disallow: /
```

### 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: 2022/02/14

### Plugin Output

tcp/443/www

```
Webmirror performed 29 queries in 12s (2.0416 queries per second)
```

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

```
+ CGI : /static/icon/favicon.ico
  Methods : GET
  Argument : rev
  Value: 2
```

```
+ CGI : /en/
  Methods : GET
  Argument : page
  Value: /zh/welcome?
```

```
+ CGI : /zh/
  Methods : GET
  Argument : page
  Value: /zh/welcome?
```