



**testfire**

---

Report generated by Nessus™

Sun, 29 Oct 2023 12:51:11 India Standard Time

---

---

## TABLE OF CONTENTS

---

### Vulnerabilities by Host

- testfire.net..... 4

Nessus Essentials

---

## **Vulnerabilities by Host**

---

## testfire.net



### Scan Information

Start time: Sun Oct 29 10:17:55 2023  
End time: Sun Oct 29 12:51:11 2023

### Host Information

DNS Name: testfire.net  
IP: 65.61.137.117  
OS: Dell EMC VMX, Microsoft Windows Embedded Standard 7

### Vulnerabilities

#### 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://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://testfire.net/>
- <http://testfire.net/feedback.jsp>
- <http://testfire.net/index.jsp>
- <http://testfire.net/login.jsp>
- <http://testfire.net/search.jsp>
- [http://testfire.net/status\\_check.jsp](http://testfire.net/status_check.jsp)
- <http://testfire.net/subscribe.jsp>
- [http://testfire.net/survey\\_questions.jsp](http://testfire.net/survey_questions.jsp)

## 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://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://testfire.net/>
- <https://testfire.net/feedback.jsp>
- <https://testfire.net/index.jsp>
- <https://testfire.net/login.jsp>
- <https://testfire.net/search.jsp>
- [https://testfire.net/status\\_check.jsp](https://testfire.net/status_check.jsp)
- <https://testfire.net/subscribe.jsp>
- [https://testfire.net/survey\\_questions.jsp](https://testfire.net/survey_questions.jsp)

## 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://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/8080/www

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

- <http://testfire.net:8080/>
- <http://testfire.net:8080/feedback.jsp>
- <http://testfire.net:8080/index.jsp>
- <http://testfire.net:8080/login.jsp>
- <http://testfire.net:8080/search.jsp>
- [http://testfire.net:8080/status\\_check.jsp](http://testfire.net:8080/status_check.jsp)
- <http://testfire.net:8080/subscribe.jsp>
- [http://testfire.net:8080/survey\\_questions.jsp](http://testfire.net:8080/survey_questions.jsp)

## 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: 2023/07/17

### Plugin Output

tcp/80/www

```
Page : /login.jsp  
Destination Page: /doLogin
```

## 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: 2023/07/17

### Plugin Output

tcp/443/www

```
Page : /login.jsp  
Destination Page: /doLogin
```

## 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: 2023/07/17

### Plugin Output

tcp/8080/www

```
Page : /login.jsp  
Destination Page: /doLogin
```

## 26194 - Web Server Transmits Cleartext Credentials

### Synopsis

The remote web server might transmit credentials in cleartext.

### Description

The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext.

An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users.

### Solution

Make sure that every sensitive form transmits content over HTTPS.

### Risk Factor

Low

### CVSS v2.0 Base Score

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

### References

XREF	CWE:522
XREF	CWE:523
XREF	CWE:718
XREF	CWE:724
XREF	CWE:928
XREF	CWE:930

### Plugin Information

Published: 2007/09/28, Modified: 2016/11/29

### Plugin Output

tcp/80/www

```
Page : /login.jsp
Destination Page: /doLogin
```

## 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/8080/www

```
Page : /login.jsp
Destination Page: /doLogin
```

## 39446 - Apache Tomcat Detection

### Synopsis

The remote web server is an Apache Tomcat server.

### Description

Nessus was able to detect a remote Apache Tomcat web server.

### See Also

<https://tomcat.apache.org/>

### Solution

n/a

### Risk Factor

None

### References

XREF IAVT:0001-T-0535

### Plugin Information

Published: 2009/06/18, Modified: 2023/05/24

### Plugin Output

tcp/80/www

```
URL      : http://testfire.net/  
Version  : unknown
```

## 39446 - Apache Tomcat Detection

### Synopsis

The remote web server is an Apache Tomcat server.

### Description

Nessus was able to detect a remote Apache Tomcat web server.

### See Also

<https://tomcat.apache.org/>

### Solution

n/a

### Risk Factor

None

### References

XREF IAVT:0001-T-0535

### Plugin Information

Published: 2009/06/18, Modified: 2023/05/24

### Plugin Output

tcp/443/www

```
URL      : https://testfire.net/  
Version  : unknown
```



## 39446 - Apache Tomcat Detection

### Synopsis

The remote web server is an Apache Tomcat server.

### Description

Nessus was able to detect a remote Apache Tomcat web server.

### See Also

<https://tomcat.apache.org/>

### Solution

n/a

### Risk Factor

None

### References

XREF IAVT:0001-T-0535

### Plugin Information

Published: 2009/06/18, Modified: 2023/05/24

### Plugin Output

tcp/8080/www

```
URL      : http://testfire.net:8080/  
Version  : unknown
```

## 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 :  
  
- 9 errors involving SSI injection (on HTTP headers) checks :  
  . connecting to server: errno=6 (connection refused)  
- 8 errors involving SQL injection (on HTTP headers) checks :  
  . connecting to server: errno=6 (connection refused)  
- 8 errors involving SQL injection (on parameters names) checks :  
  . connecting to server: errno=6 (connection refused)  
- 1 error involving XSS (on HTTP headers) checks :  
  . reading the HTTP status line: errno=2 (connection reset by peer)  
- 8 errors involving XSS (on parameters names) checks :  
  . connecting to server: errno=6 (connection refused)  
- 1 error involving persistent XSS checks :
```

## 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/443/www

```
Nessus encountered :  
  
- 9 errors involving SSI injection (on HTTP headers) checks :  
  . connecting to server: errno=6 (connection refused)  
- 8 errors involving SQL injection (on HTTP headers) checks :  
  . connecting to server: errno=6 (connection refused)  
- 8 errors involving SQL injection (on parameters names) checks :  
  . connecting to server: errno=6 (connection refused)  
- 8 errors involving XSS (on parameters names) checks :  
  . connecting to server: errno=6 (connection refused)
```

## 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/8080/www

```
Nessus encountered :  
  
- 9 errors involving SSI injection (on HTTP headers) checks :  
  . connecting to server: errno=6 (connection refused)  
- 8 errors involving SQL injection (on HTTP headers) checks :  
  . connecting to server: errno=6 (connection refused)  
- 8 errors involving SQL injection (on parameters names) checks :  
  . connecting to server: errno=6 (connection refused)  
- 8 errors involving XSS (on parameters names) checks :  
  . connecting to server: errno=6 (connection refused)
```

## 33817 - CGI Generic Tests Load Estimation (all tests)

### Synopsis

Load estimation for web application tests.

### Description

This script computes the maximum number of requests that would be done by the generic web tests, depending on miscellaneous options. It does not perform any test by itself.

The results can be used to estimate the duration of these tests, or the complexity of additional manual tests.

Note that the script does not try to compute this duration based on external factors such as the network and web servers loads.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2009/10/26, Modified: 2022/04/11

### Plugin Output

tcp/80/www

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

arbitrary command execution (time based) : S=102      SP=102      AP=276      SC=30
AC=576
format string : S=34      SP=34      AP=92      SC=10
AC=192
cross-site scripting (comprehensive test): S=68      SP=68      AP=184     SC=20
AC=384
injectable parameter : S=34      SP=34      AP=92      SC=10
AC=192
arbitrary command execution : S=272     SP=272     AP=736     SC=80
AC=1536
local file inclusion : S=17      SP=17      AP=46      SC=5      AC=96

directory traversal : S=425     SP=425     AP=1150    SC=125
AC=2400
web code injection : S=17      SP=17      AP=46      SC=5      AC=96

blind SQL injection (4 requests) : S=68      SP=68      AP=184     SC=20
AC=384
```

persistent XSS AC=384	: S=68	SP=68	AP=184	SC=20	
directory traversal (write access) AC=192	: S=34	SP=34	AP=92	SC=10	
XML injection	: S=17	SP=17	AP=46	SC=5	AC=96
blind SQL injection AC=1152	: S=204	SP=204	AP=552	SC=60	
SQL injection AC=2304	: S=408	SP=408	AP=1104	SC=120	
directory traversal (extended test) AC=4896	: S=867	SP=867	AP=2346	SC=255	
SSI injection AC=288	: S=51	SP=51	AP=138	SC=15	
unseen parameters AC=3360	: S=595	SP=595	AP=1610	SC=175	
SQL injection (2nd order)	[...]				

## 33817 - CGI Generic Tests Load Estimation (all tests)

### Synopsis

Load estimation for web application tests.

### Description

This script computes the maximum number of requests that would be done by the generic web tests, depending on miscellaneous options. It does not perform any test by itself.

The results can be used to estimate the duration of these tests, or the complexity of additional manual tests.

Note that the script does not try to compute this duration based on external factors such as the network and web servers loads.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2009/10/26, Modified: 2022/04/11

### Plugin Output

tcp/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=34          SP=34          AP=92          SC=10
AC=192
blind SQL injection (4 requests) : S=68          SP=68          AP=184         SC=20
AC=384
arbitrary command execution (time based) : S=102         SP=102         AP=276         SC=30
AC=576
cross-site scripting (comprehensive test): S=68          SP=68          AP=184         SC=20
AC=384
directory traversal (extended test) : S=867         SP=867         AP=2346        SC=255
AC=4896
arbitrary command execution    : S=272         SP=272         AP=736         SC=80
AC=1536
local file inclusion           : S=17          SP=17          AP=46          SC=5          AC=96

web code injection             : S=17          SP=17          AP=46          SC=5          AC=96

SQL injection                  : S=408         SP=408         AP=1104        SC=120
AC=2304
```

directory traversal (write access)	: S=34	SP=34	AP=92	SC=10	
AC=192					
unseen parameters	: S=595	SP=595	AP=1610	SC=175	
AC=3360					
format string	: S=34	SP=34	AP=92	SC=10	
AC=192					
directory traversal	: S=425	SP=425	AP=1150	SC=125	
AC=2400					
XML injection	: S=17	SP=17	AP=46	SC=5	AC=96
persistent XSS	: S=68	SP=68	AP=184	SC=20	
AC=384					
SSI injection	: S=51	SP=51	AP=138	SC=15	
AC=288					
SQL injection (2nd order)	: S=17	SP=17	AP=46	SC=5	AC=96
blind SQL injection	[...]				



## 33817 - CGI Generic Tests Load Estimation (all tests)

### Synopsis

Load estimation for web application tests.

### Description

This script computes the maximum number of requests that would be done by the generic web tests, depending on miscellaneous options. It does not perform any test by itself.

The results can be used to estimate the duration of these tests, or the complexity of additional manual tests.

Note that the script does not try to compute this duration based on external factors such as the network and web servers loads.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2009/10/26, Modified: 2022/04/11

### Plugin Output

tcp/8080/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]
```

XML injection	: S=17	SP=17	AP=46	SC=5	AC=96
persistent XSS	: S=68	SP=68	AP=184	SC=20	
AC=384					
unseen parameters	: S=595	SP=595	AP=1610	SC=175	
AC=3360					
SQL injection	: S=408	SP=408	AP=1104	SC=120	
AC=2304					
SSI injection	: S=51	SP=51	AP=138	SC=15	
AC=288					
directory traversal	: S=425	SP=425	AP=1150	SC=125	
AC=2400					
arbitrary command execution	: S=272	SP=272	AP=736	SC=80	
AC=1536					
directory traversal (write access)	: S=34	SP=34	AP=92	SC=10	
AC=192					
injectable parameter	: S=34	SP=34	AP=92	SC=10	
AC=192					

arbitrary command execution (time based) AC=576	: S=102	SP=102	AP=276	SC=30	
SQL injection (2nd order)	: S=17	SP=17	AP=46	SC=5	AC=96
blind SQL injection (4 requests) AC=384	: S=68	SP=68	AP=184	SC=20	
format string AC=192	: S=34	SP=34	AP=92	SC=10	
web code injection	: S=17	SP=17	AP=46	SC=5	AC=96
blind SQL injection AC=1152	: S=204	SP=204	AP=552	SC=60	
local file inclusion	: S=17	SP=17	AP=46	SC=5	AC=96
directory traversal (extended test) AC=4896	: S=867	SP=867	AP=2346	SC=255	
cross-site scripting (comprehensive te [...])					

## 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 than 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 :  
- 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/80/www

```
2 external URLs were gathered on this web server :  
URL... - Seen on...  
  
http://www-142.ibm.com/software/products/us/en/subcategory/SWI10 -  
https://github.com/AppSecDev/AltoroJ/ -
```

## 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

```
2 external URLs were gathered on this web server :  
URL... - Seen on...  
  
http://www-142.ibm.com/software/products/us/en/subcategory/SWI10 -  
https://github.com/AppSecDev/AltoroJ/ -
```

## 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/8080/www

```
2 external URLs were gathered on this web server :  
URL... - Seen on...  
  
http://www-142.ibm.com/software/products/us/en/subcategory/SWI10 - /  
https://github.com/AppSecDev/AltoroJ/ - /
```

## 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      : JSESSIONID
Value     : AA1CBD23A466DE824766A6758608BA8B
Secure    : false
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: 2022/04/11

### Plugin Output

tcp/8080/www

Based on the response to an OPTIONS request :

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

/status\_check.jsp  
/swagger

Based on tests of each method :

- HTTP methods GET HEAD OPTIONS POST are allowed on :

/  
/status\_check.jsp  
/swagger

## 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-Coyote/1.1
```

## 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-Coyote/1.1
```

## 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/8080/www

```
The remote web server type is :  
Apache-Coyote/1.1
```

## 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://testfire.net/>
- <http://testfire.net/feedback.jsp>
- <http://testfire.net/index.jsp>
- <http://testfire.net/login.jsp>
- <http://testfire.net/search.jsp>
- [http://testfire.net/status\\_check.jsp](http://testfire.net/status_check.jsp)
- <http://testfire.net/subscribe.jsp>
- [http://testfire.net/survey\\_questions.jsp](http://testfire.net/survey_questions.jsp)
- <http://testfire.net/swagger/index.html>

## 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://testfire.net/>
- <https://testfire.net/feedback.jsp>
- <https://testfire.net/index.jsp>
- <https://testfire.net/login.jsp>
- <https://testfire.net/search.jsp>
- [https://testfire.net/status\\_check.jsp](https://testfire.net/status_check.jsp)
- <https://testfire.net/subscribe.jsp>
- [https://testfire.net/survey\\_questions.jsp](https://testfire.net/survey_questions.jsp)
- <https://testfire.net/swagger/index.html>



## 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/8080/www

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

- <http://testfire.net:8080/>
- <http://testfire.net:8080/feedback.jsp>
- <http://testfire.net:8080/index.jsp>
- <http://testfire.net:8080/login.jsp>
- <http://testfire.net:8080/search.jsp>
- [http://testfire.net:8080/status\\_check.jsp](http://testfire.net:8080/status_check.jsp)
- <http://testfire.net:8080/subscribe.jsp>
- [http://testfire.net:8080/survey\\_questions.jsp](http://testfire.net:8080/survey_questions.jsp)
- <http://testfire.net:8080/swagger/index.html>

## 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://testfire.net/>
- <http://testfire.net/feedback.jsp>
- <http://testfire.net/index.jsp>
- <http://testfire.net/login.jsp>
- <http://testfire.net/search.jsp>
- [http://testfire.net/status\\_check.jsp](http://testfire.net/status_check.jsp)
- <http://testfire.net/subscribe.jsp>
- [http://testfire.net/survey\\_questions.jsp](http://testfire.net/survey_questions.jsp)
- <http://testfire.net/swagger/index.html>

## 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://testfire.net/>
- <https://testfire.net/feedback.jsp>
- <https://testfire.net/index.jsp>
- <https://testfire.net/login.jsp>
- <https://testfire.net/search.jsp>
- [https://testfire.net/status\\_check.jsp](https://testfire.net/status_check.jsp)
- <https://testfire.net/subscribe.jsp>
- [https://testfire.net/survey\\_questions.jsp](https://testfire.net/survey_questions.jsp)
- <https://testfire.net/swagger/index.html>

## 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/8080/www

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

- http://testfire.net:8080/
- http://testfire.net:8080/feedback.jsp
- http://testfire.net:8080/index.jsp
- http://testfire.net:8080/login.jsp
- http://testfire.net:8080/search.jsp
- http://testfire.net:8080/status\_check.jsp
- http://testfire.net:8080/subscribe.jsp
- http://testfire.net:8080/survey\_questions.jsp
- http://testfire.net:8080/swagger/index.html

### Synopsis

---

It is possible to determine which TCP ports are open.

### Description

---

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

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

### Solution

---

Protect your target with an IP filter.

### Risk Factor

---

None

### Plugin Information

---

Published: 2009/02/04, Modified: 2023/09/25

### 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: 2023/09/25

### Plugin Output

---

tcp/443/www

```
Port 443/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: 2023/09/25

### Plugin Output

---

tcp/8080/www

```
Port 8080/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: 2023/07/31

### Plugin Output

---

tcp/0

```
Information about this scan :
```

```
Nessus version : 10.6.1
Nessus build : 20021
Plugin feed version : 202310250413
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : testfire
```



```
Scan policy used : Web Application Tests
Scanner IP : 192.168.55.104
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 282.714 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : enabled
Web application tests : enabled
Web app tests - Test mode : single
Web app tests - Try all HTTP methods : no
Web app tests - Maximum run time : 5 minutes.
Web app tests - Stop at first flaw : CGI
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2023/10/29 10:18 India Standard Time
Scan duration : 9183 sec
Scan for malware : no
```

## 85602 - Web Application Cookies Not Marked Secure

### Synopsis

HTTP session cookies might be transmitted in cleartext.

### Description

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

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

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

### See Also

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

### Solution

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

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

### Risk Factor

None

### References

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

### Plugin Information

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

### Plugin Output

tcp/80/www

The following cookie does not set the secure cookie flag :

Name : JSESSIONID  
Path : /  
Value : AA1CBD23A466DE824766A6758608BA8B  
Domain :  
Version : 1  
Expires :  
Comment :  
Secure : 0  
Httponly : 1  
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 : JSESSIONID  
Path : /  
Value : AA1CBD23A466DE824766A6758608BA8B  
Domain :  
Version : 1  
Expires :  
Comment :  
Secure : 0  
Httponly : 1  
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/8080/www

The following cookie does not set the secure cookie flag :

Name : JSESSIONID  
Path : /  
Value : AA1CBD23A466DE824766A6758608BA8B  
Domain :  
Version : 1  
Expires :  
Comment :  
Secure : 0  
Httponly : 1  
Port :

### 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://testfire.net/>
- <http://testfire.net/feedback.jsp>
- <http://testfire.net/index.jsp>
- <http://testfire.net/login.jsp>
- <http://testfire.net/search.jsp>
- [http://testfire.net/status\\_check.jsp](http://testfire.net/status_check.jsp)
- <http://testfire.net/style.css>
- <http://testfire.net/subscribe.jsp>
- [http://testfire.net/survey\\_questions.jsp](http://testfire.net/survey_questions.jsp)
- <http://testfire.net/swagger/favicon-16x16.png>
- <http://testfire.net/swagger/favicon-32x32.png>
- <http://testfire.net/swagger/index.html>
- <http://testfire.net/swagger/properties.json>
- <http://testfire.net/swagger/swagger-ui.css>

Attached is a copy of the sitemap file.



### 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://testfire.net/>
- <https://testfire.net/feedback.jsp>
- <https://testfire.net/index.jsp>
- <https://testfire.net/login.jsp>
- <https://testfire.net/search.jsp>
- [https://testfire.net/status\\_check.jsp](https://testfire.net/status_check.jsp)
- <https://testfire.net/style.css>
- <https://testfire.net/subscribe.jsp>
- [https://testfire.net/survey\\_questions.jsp](https://testfire.net/survey_questions.jsp)
- <https://testfire.net/swagger/favicon-16x16.png>
- <https://testfire.net/swagger/favicon-32x32.png>
- <https://testfire.net/swagger/index.html>
- <https://testfire.net/swagger/properties.json>
- <https://testfire.net/swagger/swagger-ui.css>

Attached is a copy of the sitemap file.

### 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/8080/www

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

- http://testfire.net:8080/
- http://testfire.net:8080/feedback.jsp
- http://testfire.net:8080/index.jsp
- http://testfire.net:8080/login.jsp
- http://testfire.net:8080/search.jsp
- http://testfire.net:8080/status\_check.jsp
- http://testfire.net:8080/style.css
- http://testfire.net:8080/subscribe.jsp
- http://testfire.net:8080/survey\_questions.jsp
- http://testfire.net:8080/swagger/favicon-16x16.png
- http://testfire.net:8080/swagger/favicon-32x32.png
- http://testfire.net:8080/swagger/index.html
- http://testfire.net:8080/swagger/properties.json
- http://testfire.net:8080/swagger/swagger-ui.css

Attached is a copy of the sitemap file.

### Synopsis

Nessus can crawl the remote website.

### Description

This plugin makes a mirror of the remote website(s) and extracts the list of CGIs that are used by the remote host.

It is suggested that you change the number of pages to mirror in the 'Options' section of the client.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2001/05/04, Modified: 2023/09/25

### Plugin Output

tcp/80/www

```
Webmirror performed 27 queries in 35s (0.0771 queries per second)
```

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

```
+ CGI : /index.jsp
  Methods : GET
  Argument : content
  Value: security.htm
```

```
+ CGI : /search.jsp
  Methods : GET
  Argument : query
```

```
+ CGI : /default.jsp
  Methods : GET
  Argument : content
  Value: security.htm
```

```
+ CGI : /doLogin
  Methods : POST
  Argument : btnSubmit
  Value: Login
  Argument : passw
```

```
Argument : uid

+ CGI : /sendFeedback
  Methods : POST
  Argument : cfile
    Value: comments.txt
  Argument : comments
  Argument : email_addr
  Argument : name
  Argument : reset
    Value: Clear Form
  Argument : subject
  Argument : submit
    Value: Submit

+ CGI : /doSubscribe
  Methods : POST
  Argument : btnSubmit
    Value: Subscribe
  Argument : txtEmail

+ CGI : /survey_questions.jsp
  Methods : GET
  Argument : step
    Value: a

+ CGI : /status_check.jsp/util/serverStatusCheckService.jsp
  Methods : GET
  Argument : HostName
```

### Synopsis

Nessus can crawl the remote website.

### Description

This plugin makes a mirror of the remote website(s) and extracts the list of CGIs that are used by the remote host.

It is suggested that you change the number of pages to mirror in the 'Options' section of the client.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2001/05/04, Modified: 2023/09/25

### Plugin Output

tcp/443/www

```
Webmirror performed 27 queries in 68s (0.0397 queries per second)
```

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

```
+ CGI : /index.jsp
  Methods : GET
  Argument : content
  Value: security.htm
```

```
+ CGI : /search.jsp
  Methods : GET
  Argument : query
```

```
+ CGI : /default.jsp
  Methods : GET
  Argument : content
  Value: security.htm
```

```
+ CGI : /doLogin
  Methods : POST
  Argument : btnSubmit
  Value: Login
  Argument : passw
```

```
Argument : uid

+ CGI : /sendFeedback
  Methods : POST
  Argument : cfile
    Value: comments.txt
  Argument : comments
  Argument : email_addr
  Argument : name
  Argument : reset
    Value: Clear Form
  Argument : subject
  Argument : submit
    Value: Submit

+ CGI : /doSubscribe
  Methods : POST
  Argument : btnSubmit
    Value: Subscribe
  Argument : txtEmail

+ CGI : /survey_questions.jsp
  Methods : GET
  Argument : step
    Value: a

+ CGI : /status_check.jsp/util/serverStatusCheckService.jsp
  Methods : GET
  Argument : HostName
```

### Synopsis

Nessus can crawl the remote website.

### Description

This plugin makes a mirror of the remote website(s) and extracts the list of CGIs that are used by the remote host.

It is suggested that you change the number of pages to mirror in the 'Options' section of the client.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2001/05/04, Modified: 2023/09/25

### Plugin Output

tcp/8080/www

```
Webmirror performed 27 queries in 34s (0.0794 queries per second)
```

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

```
+ CGI : /index.jsp
  Methods : GET
  Argument : content
  Value: security.htm
```

```
+ CGI : /search.jsp
  Methods : GET
  Argument : query
```

```
+ CGI : /default.jsp
  Methods : GET
  Argument : content
  Value: security.htm
```

```
+ CGI : /doLogin
  Methods : POST
  Argument : btnSubmit
  Value: Login
  Argument : passw
```

```
Argument : uid

+ CGI : /sendFeedback
  Methods : POST
  Argument : cfile
    Value: comments.txt
  Argument : comments
  Argument : email_addr
  Argument : name
  Argument : reset
    Value: Clear Form
  Argument : subject
  Argument : submit
    Value: Submit

+ CGI : /doSubscribe
  Methods : POST
  Argument : btnSubmit
    Value: Subscribe
  Argument : txtEmail

+ CGI : /survey_questions.jsp
  Methods : GET
  Argument : step
    Value: a

+ CGI : /status_check.jsp/util/serverStatusCheckService.jsp
  Methods : GET
  Argument : HostName
```