tenable Nessus

Report generated by Tenable Nessus™

Itsecgames.com Web App Scan

Sat, 06 Sep 2025 17:55:48 India Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

Collapse All | Expand All

itsecgames.com

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	1	0	15

Severity	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
MEDIUM	6.5	-	-	142960	HSTS Missing From HTTPS Server (RFC 6797)
INFO	N/A	-	-	48204	Apache HTTP Server Version
INFO	N/A	-	-	49704	External URLs
INFO	N/A	-	-	84502	HSTS Missing From HTTPS Server
INFO	N/A	-	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	-	10107	HTTP Server Type and Version
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	50344	Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header
INFO	N/A	-	-	50345	Missing or Permissive X-Frame-Options HTTP Response Header
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	91815	Web Application Sitemap
INFO	N/A	-	-	11032	Web Server Directory Enumeration
INFO	N/A	-	-	49705	Web Server Harvested Email Addresses

INFO	N/A	-	-	11419	Web Server Office File Inventory
INFO	N/A	-	-	10662	Web mirroring

* indicates the v3.0 score was not available; the v2.0 score is shown

Hide

tenable Nessus

Report generated by Tenable Nessus™

Itsecgames.com Web App Scan

Sat, 06 Sep 2025 17:55:48 India Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

Collapse All | Expand All

itsecgames.com

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	1	0	22

Scan Information

Start time:	Sat Sep 6 14:22:34 2025
End time:	Sat Sep 6 17:55:48 2025

Host Information

DNS Name:	itsecgames.com
IP:	31.3.96.40
OS:	Linux Kernel 2.6

Vulnerabilities

142960 - HSTS Missing From HTTPS Server (RFC 6797) -

Synopsis

The remote web server is not enforcing HSTS, as defined by RFC 6797.

Description

The remote web server is not enforcing HSTS, as defined by RFC 6797. 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

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

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

Plugin Information

Published: 2020/11/17, Modified: 2024/03/22

Plugin Output

tcp/443/www

```
HTTP/1.1 200 OK
Date: Sat, 06 Sep 2025 08:56:02 GMT
Server: Apache
Expires: Sun, 19 Nov 1978 05:00:00 GMT
Cache-Control: no-cache, must-revalidate
X-Content-Type-Options: nosniff
Content-Language: en
X-Frame-Options: SAMEORIGIN
X-UA-Compatible: IE=edge
X-Generator: Drupal 7 (http://drupal.org)
Link: <https://itsecgames.com/>; rel="canonical",<https://itsecgames.com/>; rel="shortlink"
Vary: Accept-Encoding
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8


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

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-0030
XREF	IAVT:0001-T-0530

Plugin Information

Published: 2010/07/30, Modified: 2023/08/17

Plugin Output

tcp/80/www

```
URL : http://itsecgames.com/
Version : unknown
Source : Server: Apache
backported : 0
```

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

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

http://creativecommons.org/licenses/by-nc-nd/4.0/ - /
http://itsecgames.blogspot.com - /
https://be.linkedin.com/in/malikmesellem - /
https://fonts.googleapis.com/css?family=Architects+Daughter - /
https://itsecgames.blogspot.com - /
https://sourceforge.net/projects/bwapp/files/bWAPP/ - /download.htm
https://sourceforge.net/projects/bwapp/files/bee-box/ - /download.htm

https://twitter.com/MME_IT - /
https://www.facebook.com/mmebv/ - /
https://www.mmesec.com - /
https://www.mmesec.com/training - /
https://www.mmesec.com/training/cyber-security-bootcamp - /training.htm
https://www.mmesec.com/training/ethical-hacking-bootcamp - /training.htm
https://www.mmesec.com/training/web-security-bootcamp - /training.htm
https://www.owasp.org - /
```

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://sourceforge.net/projects/bwapp/ - /software/web-security-testing-framework
http://www.mmesec.com - /
https://ccb.belgium.be/nl/de-nis2-richtlijn-wat-betekent-dit-voor-mijn-organisatie - /news-items
https://customerconnect.vmware.com/en/downloads/info/slug/desktop_end_user_computing/vmware_workstation_player/16_0 -
/training/ethical-hacking-bootcamp
https://fonts.googleapis.com/css?family=Roboto+Condensed:300,300italic&subset=latin-ext - /
https://gdpr.eu - /audits/full-security-audit
https://maps.google.com/?q=50.80355,3.126870&z=15&output=embed&t=m&iwloc=near - /contact

https://www.mmesec.com/about - /
https://www.mmesec.com/audits/penetration-testing - /
https://www.mmesec.com/gdpr - /
https://www.mmesec.com/security-audits - /
https://www.mmesec.com/security-training - /
https://www.mmesec.com/software/vulnerability-assessment-solution - /
https://www.mmesec.com/training -
https://www.mmesec.com/training/ethical-hacking-bootcamp -
```

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: 2024/08/09

Plugin Output

tcp/443/www

```
HTTP/1.1 200 OK
Date: Sat, 06 Sep 2025 08:56:02 GMT
Server: Apache
Expires: Sun, 19 Nov 1978 05:00:00 GMT
Cache-Control: no-cache, must-revalidate
X-Content-Type-Options: nosniff
Content-Language: en
X-Frame-Options: SAMEORIGIN
X-UA-Compatible: IE=edge
X-Generator: Drupal 7 (http://drupal.org)
Link: <https://itsecgames.com/>; rel="canonical",<https://itsecgames.com/>; rel="shortlink"
Vary: Accept-Encoding
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8
```

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

43111 - HTTP Methods Allowed (per directory)

Synopsis

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

Description

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

The following HTTP methods are considered insecure:
PUT, DELETE, CONNECT, TRACE, HEAD

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

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes' in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

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

See Also

http://www.nessus.org/u?d9c03a9a
http://www.nessus.org/u?b019cbdb
https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/12/10, Modified: 2022/04/11

Plugin Output

tcp/80/www

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

- HTTP methods GET HEAD OPTIONS POST are allowed on :

/
/downloads
/icons
/images
/javascript
/js
/stylesheets


Based on tests of each method :

- HTTP methods GET HEAD OPTIONS POST are allowed on :

/
/downloads
/icons
/images
/javascript
/js
/stylesheets
```

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 is 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: 2024/02/26

Plugin Output

tcp/80/www

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

Date: Sat, 06 Sep 2025 10:38:23 GMT
Server: Apache
Last-Modified: Wed, 09 Feb 2022 13:14:08 GMT
ETag: "e43-5d7959bd3c800"
Accept-Ranges: bytes
Content-Length: 3651
Vary: Accept-Encoding
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html

Response Body :

<!DOCTYPE html>
<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Architects+Daughter">
<link rel="stylesheet" type="text/css" href="stylesheets/stylesheet.css" media="screen" />
<link rel="shortcut icon" href="images/favicon.ico" type="image/x-icon" />

<!--<script src="//html5shiv.googlecode.com/svn/trunk/html5.js"></script>-->
<script src="js/html5.js"></script>

<title>bWAPP, a buggy web application!</title>

</head>

<body>

<header>

<h1>bWAPP</h1>

<h2>an extremely buggy web app !</h2>

</header>

<div id="menu">

<table>

<tr>

<td><font color="#ffb717">Home</font></td>
```

```
<td><a href="bugs.htm">Bugs</a></td>
<td><a href="download.htm">Download</a></td>
<td><a href="training.htm">Talks & Training</a></td>
<td><a href="http://itsecgames.blogspot.com" target="_blank">Blog</a></td>

</tr>

</table>

</div>

<div id="main">

<h1>Home</h1>

<p>bWAPP, or a <i>buggy web application</i>, is a free and open source deliberately insecure web application.<br />
It helps security enthusiasts, developers and students to discover and to prevent web vulnerabilities.<br />
bWAPP prepares one to conduct successful penetration testing and ethical hacking projects.</p>

<p>What makes bWAPP so unique? Well, it has over <a href="./downloads/vulnerabilities.txt" target="blank">100 web
vulnerabilities</a>!<br />
It covers all major known web bugs, including all risks from the OWASP Top 10 project.</p>

<p>bWAPP is a PHP application that uses a MySQL database. It can be hosted on Linux/Windows with Apache/IIS and MySQL.
It can also be installed with WAMP or XAMPP.<br />
Another possibility is to download the <i>bee-box</i>, a custom Linux VM pre-installed with bWAPP.</p>

<p>Download our <a href="./downloads/bWAPP_intro.pdf" target="_blank">What is bWAPP?</a> introduction tutorial, including free
exercises...</p>

<p>bWAPP is for web application security-testing and educational purposes only.<br />
Have fun with this free and open source project!</p>

<p>Cheers, Malik Mesellem</p>

</div>

<div id="sponsor">

<table>

<tr>
<td align="center"><a href="https://www.mmesec.com" target="_blank"><img src="./images/mme.png"></a> </td>
<td>    </td>
<td align="center"><a href="https://www.owasp.org" target="_blank"><img src="./images/owasp.png"></a></td>

</tr>

</table>

</div>

<div id="side">

<a href="https://twitter.com/MME_IT" target="blank_" class="button"><img src="./images/twitter.png"></a>
<a href="https://be.linkedin.com/in/malikmesellem" target="blank_" class="button"><img src="./images/linkedin.png"></a>
<a href="https://www.facebook.com/mmebv/" target="blank_" class="button"><img src="./images/facebook.png"></a>
<a href="https://itsecgames.blogspot.com" target="blank_" class="button"><img src="./images/blogger.png"></a>

</div>

<div id="disclaimer">

<p>bWAPP is licensed under <a rel="license" href="http://creativecommons.org/licenses/by-nc-nd/4.0/" target="_blank"><img
style="vertical-align:middle" src="./images/cc.png"></a> &copy; 2022 MME BV / Follow <a href="https://twitter.com/MME_IT"
target="_blank">@MME_IT</a> on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive <a
href="https://www.mmesec.com/training" target="blank_">training</a>?</p>

</div>

<div id="bee">

<img src="./images/bee_1.png">

</div>

</body>

</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/80/www

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

- http://itsecgames.com/
- http://itsecgames.com/bugs.htm
- http://itsecgames.com/download.htm
- http://itsecgames.com/index.htm
- http://itsecgames.com/training.htm
```

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://itsecgames.com/
- https://itsecgames.com/about
- https://itsecgames.com/audits/full-security-audit
- https://itsecgames.com/audits/penetration-testing
- https://itsecgames.com/audits/social-engineering-campaigns
- https://itsecgames.com/audits/vulnerability-assessment
- https://itsecgames.com/audits/web-security-testing
- https://itsecgames.com/contact
- https://itsecgames.com/contact-us-1
- https://itsecgames.com/cyber-security-bootcamp-26092025
- https://itsecgames.com/ethical-hacking-bootcamp-17092025
- https://itsecgames.com/news-items
- https://itsecgames.com/news/blackhat-usa
- https://itsecgames.com/news/een-cyber-veilig-nieuwjaar
- https://itsecgames.com/news/een-hack-proof-nieuwjaar
- https://itsecgames.com/news/fast-track
- https://itsecgames.com/news/kmo-portefeuille
- https://itsecgames.com/news/menselijke-firewall
- https://itsecgames.com/news/mme-cyberclass
- https://itsecgames.com/news/nis2-richtlijn
- https://itsecgames.com/news/op-user-awareness-staat-geen-leeftijd
- https://itsecgames.com/news/technical-awareness
- https://itsecgames.com/news/webinar-cybersecurity-awareness
- https://itsecgames.com/node
- https://itsecgames.com/node/63/register
- https://itsecgames.com/node/75/register
- https://itsecgames.com/security-audits
- https://itsecgames.com/security-training
- https://itsecgames.com/software
- https://itsecgames.com/software/managed-security-awareness
- https://itsecgames.com/software/vulnerability-assessment-solution
- https://itsecgames.com/software/web-application-security-scanner
- https://itsecgames.com/software/web-security-testing-framework
- https://itsecgames.com/training/awareness-for-employees
- https://itsecgames.com/training/cyber-security-bootcamp
- https://itsecgames.com/training/ethical-hacking-bootcamp
- https://itsecgames.com/training/user-awareness
- https://itsecgames.com/training/web-security-bootcamp
```

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://itsecgames.com/
- http://itsecgames.com/bugs.htm
- http://itsecgames.com/download.htm
- http://itsecgames.com/index.htm
- http://itsecgames.com/training.htm
```

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/07/14

Plugin Output

tcp/22

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

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/07/14

Plugin Output

tcp/80/www

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/07/14

Plugin Output

tcp/443/www

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

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2025/06/25

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.9.3
Nessus build : 20023
Plugin feed version : 202509050739
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : Itsecgames.com Web App Scan
Scan policy used : Web Application Tests
Scanner IP : 10.81.24.60
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 421.845 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : 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 did not launch)
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 : 2025/9/6 14:22 India Standard Time (UTC +05:30)
Scan duration : 12786 sec
Scan for malware : no
```

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://itsecgames.com/
```

```
- http://itsecgames.com/bugs.htm
- http://itsecgames.com/download.htm
- http://itsecgames.com/downloads/bWAPP_intro.pdf
- http://itsecgames.com/downloads/vulnerabilities.txt
- http://itsecgames.com/images/bWAPP_10.png
- http://itsecgames.com/images/bWAPP_11.png
- http://itsecgames.com/images/bWAPP_12.png
- http://itsecgames.com/images/bWAPP_13.png
- http://itsecgames.com/images/bWAPP_2.png
- http://itsecgames.com/images/bWAPP_3.png
- http://itsecgames.com/images/bWAPP_4.png
- http://itsecgames.com/images/bWAPP_5.png
- http://itsecgames.com/images/bWAPP_6.png
- http://itsecgames.com/images/bWAPP_7.png
- http://itsecgames.com/images/bWAPP_8.png
- http://itsecgames.com/images/bWAPP_9.png
- http://itsecgames.com/images/favicon.ico
- http://itsecgames.com/index.htm
- http://itsecgames.com/stylesheets/stylesheet.css
- http://itsecgames.com/training.htm

Attached is a copy of the sitemap file.
```

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://itsecgames.com/
- https://itsecgames.com/about
- https://itsecgames.com/audits/full-security-audit
- https://itsecgames.com/audits/penetration-testing
- https://itsecgames.com/audits/social-engineering-campaigns
- https://itsecgames.com/audits/vulnerability-assessment
- https://itsecgames.com/audits/web-security-testing
- https://itsecgames.com/contact
- https://itsecgames.com/contact-us-1
- https://itsecgames.com/cyber-security-bootcamp-26092025
- https://itsecgames.com/ethical-hacking-bootcamp-17092025
- https://itsecgames.com/news-items
- https://itsecgames.com/news/blackhat-usa
- https://itsecgames.com/news/een-cyber-veilig-nieuwjaar
- https://itsecgames.com/news/een-hack-proof-nieuwjaar
- https://itsecgames.com/news/fast-track
- https://itsecgames.com/news/kmo-portefeuille
- https://itsecgames.com/news/menselijke-firewall
- https://itsecgames.com/news/mme-cyberclass
- https://itsecgames.com/news/nis2-richtlijn
- https://itsecgames.com/news/op-user-awareness-staat-geen-leeftijd
- https://itsecgames.com/news/technical-awareness
- https://itsecgames.com/news/webinar-cybersecurity-awareness
- https://itsecgames.com/node
```

```
- https://itsecgames.com/node/63/register
- https://itsecgames.com/node/75/register
- https://itsecgames.com/security-audits
- https://itsecgames.com/security-training
- https://itsecgames.com/sites/default/files/downloads/OWASP_Top_10.pdf
- https://itsecgames.com/sites/default/files/downloads/bWAPP_sample_report.pdf
- https://itsecgames.com/sites/default/files/favicon.ico
- https://itsecgames.com/sites/default/files/images/bWAPP-1.png
- https://itsecgames.com/sites/default/files/images/bWAPP-2.png
- https://itsecgames.com/sites/default/files/images/bWAPP-3.png
- https://itsecgames.com/sites/default/files/images/bWAPP-4.png
- https://itsecgames.com/sites/default/files/images/bWAPP-5.png
- https://itsecgames.com/sites/default/files/images/bWAPP-6.png
- https://itsecgames.com/sites/default/files/images/bWAPP-7.png
- https://itsecgames.com/sites/default/files/images/bWAPP-8.png
- https://itsecgames.com/sites/default/files/images/netsparker-1.png
- https://itsecgames.com/sites/default/files/images/netsparker-2.png
- https://itsecgames.com/sites/default/files/images/phished-1.png
- https://itsecgames.com/sites/default/files/images/phished-2.png
- https://itsecgames.com/sites/default/files/images/phished-3.png
- https://itsecgames.com/sites/default/files/images/phished-4.png
- https://itsecgames.com/sites/default/files/images/phished-7.png
- https://itsecgames.com/sites/default/files/images/phished-9.png
- https://itsecgames.com/software
- https://itsecgames.com/software/managed-security-awareness
- https://itsecgames.com/software/vulnerability-assessment-solution
- https://itsecgames.com/software/web-application-security-scanner
- https://itsecgames.com/software/web-security-testing-framework
- https://itsecgames.com/training/awareness-for-employees
- https://itsecgames.com/training/cyber-security-bootcamp
- https://itsecgames.com/training/ethical-hacking-bootcamp
- https://itsecgames.com/training/user-awareness
- https://itsecgames.com/training/web-security-bootcamp

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: 2024/06/07

Plugin Output

tcp/80/www

```
The following directories were discovered:
/downloads, /icons, /images, /javascript, /js

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: 2024/06/07

Plugin Output

tcp/443/www

```
The following directories were discovered:
/includes, /sites, /icons, /javascript, /misc, /scripts

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/443/www

```
The following email address has been gathered :


- 'info@mmesec.com', referenced from :
/audits/penetration-testing
/news/technical-awareness
/news/een-hack-proof-nieuwjaar
/training/user-awareness
/audits/vulnerability-assessment
/training/cyber-security-bootcamp
/cyber-security-bootcamp-26092025
/news/op-user-awareness-staat-geen-leeftijd
/node
/training/web-security-bootcamp
/security-audits
/news-items
/security-training
/audits/web-security-testing
/news/mme-cyberclass
/news/kmo-portefeuille
/news/fast-track
/training/ethical-hacking-bootcamp
/software/web-application-security-scanner
/node/75/register
/
/ethical-hacking-bootcamp-17092025
/about
/news/blackhat-usa
/software
/audits/full-security-audit
/news/menselijke-firewall
/software/managed-security-awareness
/node/63/register
/news/nis2-richtlijn
/news/webinar-cybersecurity-awareness
/software/vulnerability-assessment-solution
/audits/social-engineering-campaigns
/contact
/news/een-cyber-veilig-nieuwjaar
/contact-us-1
/software/web-security-testing-framework
/training/awareness-for-employees
```

11419 - Web Server Office File Inventory

Synopsis

The remote web server hosts office-related files.

Description

This plugin connects to the remote web server and attempts to find office-related files such as .doc, .ppt, .xls, .pdf etc.

Solution

Make sure that such files do not contain any confidential or otherwise sensitive information and that they are only accessible to those with valid credentials.

Risk Factor

None

Plugin Information

Published: 2003/03/19, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
The following office-related files are available on the remote server :

- Adobe Acrobat files (.pdf) :
/downloads/bWAPP_intro.pdf
```

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: 2025/07/14

Plugin Output

tcp/443/www

```
Webmirror performed 122 queries in 395s (0.0308 queries per second)

The following CGIs have been discovered :


+ CGI : /audits/full-security-audit
Methods : POST
Argument : captcha_cacheable
Value: 1
Argument : captcha_response
Value: Google no captcha
Argument : captcha_sid
Value: 3954312
Argument : captcha_token
Value: af38de3ed978b6b099c0a662a6ffd0b9
Argument : details[finished]
Value: 0
Argument : details[page_count]
Value: 1
Argument : details[page_num]
Value: 1
Argument : details[sid]
Argument : form_build_id
Value: form-ZjMxwi3pDWB0I00H74OhmYaLRhm69bxDcGAGRcjXZBM
Argument : form_id
Value: webform_client_form_41
Argument : op
Value: Submit
Argument : submitted[email]
Argument : submitted[message]
Argument : submitted[name]
Argument : submitted[topic]


+ CGI : /audits/vulnerability-assessment
Methods : POST
Argument : captcha_cacheable
Value: 1
Argument : captcha_response
Value: Google no captcha
Argument : captcha_sid
Value: 3954314
Argument : captcha_token
Value: 04038b74d6d4d4909917b74ca4e8cd50
Argument : details[finished]
Value: 0
Argument : details[page_count]
Value: 1
Argument : details[page_num]
Value: 1
Argument : details[sid]
Argument : form_build_id
Value: form-EilenJuKC9OyATZ0RPzGUo_ONKLy5ELcFLBSBzBAaIU
Argument : form_id
Value: webform_client_form_41
```

```
Argument : op
Value: Submit
Argument : submitted[email]
Argument : submitted[message]
Argument : submitted[name]
Argument : submitted[topic]


+ CGI : /audits/social-engineering-campaigns
Methods : POST
Argument : captcha_cacheable
Value: 1
Argument : captcha_response
Value: Google no captcha
Argument : captcha_sid
Value: 3954316
Argument : captcha_token
Value: 67163ff390115269c7010546a0fc76e8
Argument : details[finished]
Value: 0
Argument : details[page_count]
Value: 1
Argument : details[page_num]
Value: 1
Argument : details[sid]
Argument : form_build_id
Value: form-pCHv5J1JUWMuHGxTnrUfcFo6V8wtn2ew6XOSpT4z5oM
Argument : form_id
Value: webform_client_form_41
Argument : op
Value: Submit
Argument : submitted[email]
Argument : submitted[message]
Argument : submitted[name]
Argument : submitted[topic]


+ CGI : /audits/web-security-testing
Methods : POST
Argument : captcha_cacheable
Value: 1
Argument : captcha_response
Value: Google no captcha
Argument : captcha_sid
Value: 3954318
Argument : captcha_token
Value: 3fea24e9d36533cc27f5753351fa1d3e
Argument : details[finished]
Value: 0
Argument : details[page_count]
Value: 1
Argument : details[page_num]
Value: 1
Argument : details[sid]
Argument : form_build_id
Value: form-x4AOXi0xSJstZAStN8ZKffuUcxOfAA3aik9ZczFgCoY
Argument : form_id
Value: webform_client_form_41
Argument : op
Value: Submit
Argument : submitted[email]
Argument : submitted[message]
Argument : submitted[name]
Argument : submitted[topic]


+ CGI : /training/user-awareness
Methods : POST
Argument : captcha_cacheable
Value: 1
Argument : captcha_response
Value: Google no captcha
Argument : captcha_sid
Value: 3954320
Argument : captcha_token
Value: 00d80e8211548ae9a4ee7dcb7aa70125
Argument : details[finished]
Value: 0
Argument : details[page_count]
Value: 1
Argument : details[page_num]
Value: 1
Argument : details[sid]
Argument : form_build_id
Value: form--kNu3U82BJIYq6dGDUqj2Te7bl3wPMnSDZzOqFDZom0
Argument : form_id
Value: webform_client_form_80
Argument : op
Value: Verstuur
Argument : submitted[email]
```

```
Argument : submitted[message]
Argument : submitted[name]
Argument : submitted[topic]
Value: phishing


+ CGI : /training/web-security-bootcamp
Methods : POST
Argument : captcha_cacheable
Value: 1
Argument : captcha_response
Value: Google no captcha
Argument : captcha_sid
Value: 3954322
Argument : captcha_token
Value: 276fbe1129b6d43b30e5663946d912f2
Argument : details[finished]
Value: 0
Argument : details[page_count]
Value: 1
Argument : details[page_num]
Value: 1
Argument : details[sid]
Argument : form_build_id
Value: form-WLTnLW8kx_1y71w31_687W6MErN9oDOuvI8aA3u-suA
Argument : form_id
Value: webform_client_form_41
Argument : op
Value: Submit
Argument : submitted[email]
Argument : submitted[message]
Argument : submitted[name]
Argument : submitted[topic]


+ CGI : /software/managed-security-awareness
Methods : POST
Argument : captcha_cacheable
Value: 1
Argument : captcha_response
Value: Google no captcha
Argument : captcha_sid
Value: 3954324
Argument : captcha_token
Value: b62308d10c6d2878c0e0bb134304c172
Argument : details[finished]
Value: 0
Argument : details[page_count]
Value: 1
Argument : details[page_num]
Value: 1
Argument : details[sid]
Argument : form_build_id
Value: form-kj-tfvi_D8dBUyJQGKpmytFsjex_kPgl0-NsxKk7fmc
Argument : form_id
Value: webform_client_form_41
Argument : op
Value: Submit
Argument : submitted[email]
Argument : submitted[message]
Argument : submitted[name]
Argument : submitted[topic]


+ CGI : /software/vulnerability-assessment-solution
Methods : POST
Argument : captcha_cacheable
Value: 1
Argument : captcha_response
Value: Google no captcha
Argument : captcha_sid
Value: 3954326
Argument : captcha_token
Value: e70f08285fc0a129846a011e710da268
Argument : details[finished]
Value: 0
Argument : details[page_count]
Value: 1
Argument : details[page_num]
Value: 1
Argument : details[sid]
Argument : form_build_id
Value: form-V0iqFnhABX8BaNOHZuJwiYqvUAGoyOqoLGCiQGY-EbU
Argument : form_id
Value: webform_client_form_41
Argument : op
Value: Submit
Argument : submitted[email]
Argument : submitted[message]
Argument : submitted[name]
```

```
Argument : submitted[topic]


+ CGI : /news-items
Methods : GET
Argument : page
Value: 2


+ CGI : /contact
Methods : POST
Argument : captcha_cacheable
Value: 1
Argument : captcha_response
Value: Google no captcha
Argument : captcha_sid
Value: 3954328
Argument : captcha_token
Value: 65830c2dc76cedfc91155653b1de783b
Argument : details[finished]
Value: 0
Argument : details[page_count]
Value: 1
Argument : details[page_num]
Value: 1
Argument : details[sid]
Argument : form_build_id
Value: form-dSJ0Npqm-GgMpZlQ-XCIa6OVP6pjIWx-auClhuEyiA0
Argument : form_id
Value: webform_client_form_12
Argument : op
Value: Submit
Argument : submitted[email]
Argument : submitted[message]
Argument : submitted[name]
Argument : submitted[topic]
Value: general


+ CGI : /software/web-application-security-scanner
Methods : POST
Argument : captcha_cacheable
Value: 1
Argument : captcha_response
Value: Google no captcha
Argument : captcha_sid
Value: 3954336
Argument : captcha_token
Value: a962a0c2f57e2855dfe820dd75e0227c
Argument : details[finished]
Value: 0
Argument : details[page_count]
Value: 1
Argument : details[page_num]
Value: 1
Argument : details[sid]
Argument : form_build_id
Value: form-nB9e-1LnWqOQzw4jYeTk_nuAC5nVaDFBAupSN5ZMyZs
Argument : form_id
Value: webform_client_form_41
Argument : op
Value: Submit
Argument : submitted[email]
Argument : submitted[message]
Argument : submitted[name]
Argument : submitted[topic]


+ CGI : /training/awareness-for-employees
Methods : POST
Argument : captcha_cacheable
Value: 1
Argument : captcha_response
Value: Google no captcha
Argument : captcha_sid
Value: 3954339
Argument : captcha_token
Value: d544f4f8b6fecdd09bba338f75f28ee1
Argument : details[finished]
Value: 0
Argument : details[page_count]
Value: 1
Argument : details[page_num]
Value: 1
Argument : details[sid]
Argument : form_build_id
Value: form-5RqTSiLUpGEh6T_SmfakdVH6Bn61vld8kZthflF_MWk
Argument : form_id
Value: webform_client_form_41
Argument : op
```

```
Value: Submit
Argument : submitted[email]
Argument : submitted[message]
Argument : submitted[name]
Argument : submitted[topic]


+ CGI : /node/75/register
Methods : POST
Argument : captcha_cacheable
Value: 1
Argument : captcha_response
Value: Google no captcha
Argument : captcha_sid
Value: 3954341
Argument : captcha_token
Value: 756ac9c6b98ba335b6f6c96a2fec626e
Argument : email
Argument : field_first_name[und][0][value]
Argument : field_last_name[und][0][value]
Argument : field_telephone[und][0][value]
Argument : form_build_id
Value: form-YeXWIlvbf7xD_lzOTlMx7YZgk1xlINWK5kWHYztuXMc
Argument : form_id
Value: node_registration_form
Argument : op
Value: Create registration


+ CGI : /node/63/register
Methods : POST
Argument : captcha_cacheable
Value: 1
Argument : captcha_response
Value: Google no captcha
Argument : captcha_sid
Value: 3954343
Argument : captcha_token
Value: a642240b4d8340ba4c6990156d4347ff
Argument : email
Argument : field_first_name[und][0][value]
Argument : field_last_name[und][0][value]
Argument : field_telephone[und][0][value]
Argument : form_build_id
Value: form-quiX2tM0czofSfE3pFWqF_frkm3fFwA0tzZ4OYMsQu4
Argument : form_id
Value: node_registration_form
Argument : op
Value: Create registration


+ CGI : /contact-us-1
Methods : POST
Argument : captcha_cacheable
Value: 1
Argument : captcha_response
Value: Google no captcha
Argument : captcha_sid
Value: 3954360
Argument : captcha_token
Value: 93902a23c05ed3ae88995668be21bdde
Argument : details[finished]
Value: 0
Argument : details[page_count]
Value: 1
Argument : details[page_num]
Value: 1
Argument : details[sid]
Argument : form_build_id
Value: form-11kz5pTOiWAsir8zs74hLeDzIom-FSvohvgjpks_Qjs
Argument : form_id
Value: webform_client_form_12
Argument : op
Value: Submit
Argument : submitted[email]
Argument : submitted[message]
Argument : submitted[name]
Argument : submitted[topic]
Value: general
```

tenable Nessus

Report generated by Tenable Nessus™

Itsecgames.com Web App Scan

Sat, 06 Sep 2025 17:55:48 India Standard Time

TABLE OF CONTENTS

Vulnerabilities by Plugin

Collapse All | Expand All

142960 (1) - HSTS Missing From HTTPS Server (RFC 6797)

Synopsis

The remote web server is not enforcing HSTS, as defined by RFC 6797.

Description

The remote web server is not enforcing HSTS, as defined by RFC 6797. 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

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

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

Plugin Information

Published: 2020/11/17, Modified: 2024/03/22

Plugin Output

itsecgames.com (tcp/443/www)

```
HTTP/1.1 200 OK
Date: Sat, 06 Sep 2025 08:56:02 GMT
Server: Apache
Expires: Sun, 19 Nov 1978 05:00:00 GMT
Cache-Control: no-cache, must-revalidate
X-Content-Type-Options: nosniff
Content-Language: en
X-Frame-Options: SAMEORIGIN
X-UA-Compatible: IE=edge
X-Generator: Drupal 7 (http://drupal.org)
Link: <https://itsecgames.com/>; rel="canonical",<https://itsecgames.com/>; rel="shortlink"
Vary: Accept-Encoding
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8


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

11219 (3) - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/07/14

Plugin Output

itsecgames.com (tcp/22)

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

itsecgames.com (tcp/80/www)

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

itsecgames.com (tcp/443/www)

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

10107 (2) - 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

itsecgames.com (tcp/80/www)

```
The remote web server type is :

Apache
```

itsecgames.com (tcp/443/www)

```
The remote web server type is :

Apache
```

11032 (2) - 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: 2024/06/07

Plugin Output

itsecgames.com (tcp/80/www)

```
The following directories were discovered:
/downloads, /icons, /images, /javascript, /js

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
```

itsecgames.com (tcp/443/www)

```
The following directories were discovered:
/includes, /sites, /icons, /javascript, /misc, /scripts

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
```

49704 (2) - 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

itsecgames.com (tcp/80/www)

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

http://creativecommons.org/licenses/by-nc-nd/4.0/ - /
http://itsecgames.blogspot.com - /
https://be.linkedin.com/in/malikmesellem - /
https://fonts.googleapis.com/css?family=Architects+Daughter - /
https://itsecgames.blogspot.com - /
https://sourceforge.net/projects/bwapp/files/bWAPP/ - /download.htm
https://sourceforge.net/projects/bwapp/files/bee-box/ - /download.htm

https://twitter.com/MME_IT - /
https://www.facebook.com/mmebv/ - /
https://www.mmesec.com - /
https://www.mmesec.com/training - /
https://www.mmesec.com/training/cyber-security-bootcamp - /training.htm
https://www.mmesec.com/training/ethical-hacking-bootcamp - /training.htm
https://www.mmesec.com/training/web-security-bootcamp - /training.htm
https://www.owasp.org - /
```

itsecgames.com (tcp/443/www)

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

http://sourceforge.net/projects/bwapp/ - /software/web-security-testing-framework
```

```
http://www.mmesec.com - /
https://ccb.belgium.be/nl/de-nis2-richtlijn-wat-betekent-dit-voor-mijn-organisatie - /news-items
https://customerconnect.vmware.com/en/downloads/info/slug/desktop_end_user_computing/vmware_workstation_player/16_0 -
/training/ethical-hacking-bootcamp
https://fonts.googleapis.com/css?family=Roboto+Condensed:300,300italic&subset=latin-ext - /
https://gdpr.eu - /audits/full-security-audit
https://maps.google.com/?q=50.80355,3.126870&z=15&output=embed&t=m&iwloc=near - /contact

https://www.mmesec.com/about - /
https://www.mmesec.com/audits/penetration-testing - /
https://www.mmesec.com/gdpr - /
https://www.mmesec.com/security-audits - /
https://www.mmesec.com/security-training - /
https://www.mmesec.com/software/vulnerability-assessment-solution - /
https://www.mmesec.com/training -
https://www.mmesec.com/training/ethical-hacking-bootcamp -
```

50344 (2) - 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

itsecgames.com (tcp/80/www)

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

- http://itsecgames.com/
- http://itsecgames.com/bugs.htm
- http://itsecgames.com/download.htm
- http://itsecgames.com/index.htm
- http://itsecgames.com/training.htm
```

itsecgames.com (tcp/443/www)

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

- https://itsecgames.com/
- https://itsecgames.com/about
- https://itsecgames.com/audits/full-security-audit
- https://itsecgames.com/audits/penetration-testing
- https://itsecgames.com/audits/social-engineering-campaigns
- https://itsecgames.com/audits/vulnerability-assessment
- https://itsecgames.com/audits/web-security-testing
- https://itsecgames.com/contact
- https://itsecgames.com/contact-us-1
- https://itsecgames.com/cyber-security-bootcamp-26092025
- https://itsecgames.com/ethical-hacking-bootcamp-17092025
- https://itsecgames.com/news-items
```

- https://itsecgames.com/news/blackhat-usa
- https://itsecgames.com/news/een-cyber-veilig-nieuwjaar
- https://itsecgames.com/news/een-hack-proof-nieuwjaar
- https://itsecgames.com/news/fast-track
- https://itsecgames.com/news/kmo-portefeuille
- https://itsecgames.com/news/menselijke-firewall
- https://itsecgames.com/news/mme-cyberclass
- https://itsecgames.com/news/nis2-richtlijn
- https://itsecgames.com/news/op-user-awareness-staat-geen-leeftijd
- https://itsecgames.com/news/technical-awareness
- https://itsecgames.com/news/webinar-cybersecurity-awareness
- https://itsecgames.com/node
- https://itsecgames.com/node/63/register
- https://itsecgames.com/node/75/register
- https://itsecgames.com/security-audits
- https://itsecgames.com/security-training
- https://itsecgames.com/software
- https://itsecgames.com/software/managed-security-awareness
- https://itsecgames.com/software/vulnerability-assessment-solution
- https://itsecgames.com/software/web-application-security-scanner
- https://itsecgames.com/software/web-security-testing-framework
- https://itsecgames.com/training/awareness-for-employees
- https://itsecgames.com/training/cyber-security-bootcamp
- https://itsecgames.com/training/ethical-hacking-bootcamp
- https://itsecgames.com/training/user-awareness
- https://itsecgames.com/training/web-security-bootcamp

91815 (2) - 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

itsecgames.com (tcp/80/www)

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

- http://itsecgames.com/
- http://itsecgames.com/bugs.htm
- http://itsecgames.com/download.htm
- http://itsecgames.com/downloads/bWAPP_intro.pdf
- http://itsecgames.com/downloads/vulnerabilities.txt
- http://itsecgames.com/images/bWAPP_10.png
- http://itsecgames.com/images/bWAPP_11.png
- http://itsecgames.com/images/bWAPP_12.png
- http://itsecgames.com/images/bWAPP_13.png
- http://itsecgames.com/images/bWAPP_2.png
- http://itsecgames.com/images/bWAPP_3.png
- http://itsecgames.com/images/bWAPP_4.png
- http://itsecgames.com/images/bWAPP_5.png
- http://itsecgames.com/images/bWAPP_6.png
- http://itsecgames.com/images/bWAPP_7.png
- http://itsecgames.com/images/bWAPP_8.png
- http://itsecgames.com/images/bWAPP_9.png
- http://itsecgames.com/images/favicon.ico
- http://itsecgames.com/index.htm
- http://itsecgames.com/stylesheets/stylesheet.css
- http://itsecgames.com/training.htm

Attached is a copy of the sitemap file.

itsecgames.com (tcp/443/www)

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

- https://itsecgames.com/
- https://itsecgames.com/about
- https://itsecgames.com/audits/full-security-audit
- https://itsecgames.com/audits/penetration-testing
- https://itsecgames.com/audits/social-engineering-campaigns
- https://itsecgames.com/audits/vulnerability-assessment
- https://itsecgames.com/audits/web-security-testing
- https://itsecgames.com/contact
- https://itsecgames.com/contact-us-1
- https://itsecgames.com/cyber-security-bootcamp-26092025
- https://itsecgames.com/ethical-hacking-bootcamp-17092025
- https://itsecgames.com/news-items
- https://itsecgames.com/news/blackhat-usa
- https://itsecgames.com/news/een-cyber-veilig-nieuwjaar
- https://itsecgames.com/news/een-hack-proof-nieuwjaar
- https://itsecgames.com/news/fast-track
- https://itsecgames.com/news/kmo-portefeuille
- https://itsecgames.com/news/menselijke-firewall
- https://itsecgames.com/news/mme-cyberclass
- https://itsecgames.com/news/nis2-richtlijn
- https://itsecgames.com/news/op-user-awareness-staat-geen-leeftijd
- https://itsecgames.com/news/technical-awareness
- https://itsecgames.com/news/webinar-cybersecurity-awareness
- https://itsecgames.com/node
- https://itsecgames.com/node/63/register
- https://itsecgames.com/node/75/register
- https://itsecgames.com/security-audits
- https://itsecgames.com/security-training
- https://itsecgames.com/sites/default/files/downloads/OWASP_Top_10.pdf
- https://itsecgames.com/sites/default/files/downloads/bWAPP_sample_report.pdf
- https://itsecgames.com/sites/default/files/favicon.ico
- https://itsecgames.com/sites/default/files/images/bWAPP-1.png
- https://itsecgames.com/sites/default/files/images/bWAPP-2.png
- https://itsecgames.com/sites/default/files/images/bWAPP-3.png
- https://itsecgames.com/sites/default/files/images/bWAPP-4.png
- https://itsecgames.com/sites/default/files/images/bWAPP-5.png
- https://itsecgames.com/sites/default/files/images/bWAPP-6.png
- https://itsecgames.com/sites/default/files/images/bWAPP-7.png
- https://itsecgames.com/sites/default/files/images/bWAPP-8.png
- https://itsecgames.com/sites/default/files/images/netsparker-1.png
- https://itsecgames.com/sites/default/files/images/netsparker-2.png
- https://itsecgames.com/sites/default/files/images/phished-1.png
- https://itsecgames.com/sites/default/files/images/phished-2.png
- https://itsecgames.com/sites/default/files/images/phished-3.png
- https://itsecgames.com/sites/default/files/images/phished-4.png
- https://itsecgames.com/sites/default/files/images/phished-7.png
- https://itsecgames.com/sites/default/files/images/phished-9.png
- https://itsecgames.com/software
- https://itsecgames.com/software/managed-security-awareness
- https://itsecgames.com/software/vulnerability-assessment-solution
- https://itsecgames.com/software/web-application-security-scanner
- https://itsecgames.com/software/web-security-testing-framework
- https://itsecgames.com/training/awareness-for-employees
- https://itsecgames.com/training/cyber-security-bootcamp
- https://itsecgames.com/training/ethical-hacking-bootcamp
- https://itsecgames.com/training/user-awareness
- https://itsecgames.com/training/web-security-bootcamp

Attached is a copy of the sitemap file.
```

10662 (1) - 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: 2025/07/14

Plugin Output

itsecgames.com (tcp/443/www)

```
Webmirror performed 122 queries in 395s (0.0308 queries per second)

The following CGIs have been discovered :


+ CGI : /audits/full-security-audit
Methods : POST
Argument : captcha_cacheable
Value: 1
Argument : captcha_response
Value: Google no captcha
Argument : captcha_sid
Value: 3954312
Argument : captcha_token
Value: af38de3ed978b6b099c0a662a6ffd0b9
Argument : details[finished]
Value: 0
Argument : details[page_count]
Value: 1
Argument : details[page_num]
Value: 1
Argument : details[sid]
Argument : form_build_id
Value: form-ZjMxwi3pDWB0I00H74OhmYaLRhm69bxDcGAGRcjXZBM
Argument : form_id
Value: webform_client_form_41
Argument : op
Value: Submit
Argument : submitted[email]
Argument : submitted[message]
Argument : submitted[name]
Argument : submitted[topic]


+ CGI : /audits/vulnerability-assessment
Methods : POST
Argument : captcha_cacheable
Value: 1
Argument : captcha_response
Value: Google no captcha
Argument : captcha_sid
Value: 3954314
Argument : captcha_token
Value: 04038b74d6d4d4909917b74ca4e8cd50
Argument : details[finished]
Value: 0
Argument : details[page_count]
Value: 1
Argument : details[page_num]
Value: 1
Argument : details[sid]
Argument : form_build_id
Value: form-EilenJuKC9OyATZ0RPzGUo_ONKLy5ELcFLBSBzBAaIU
Argument : form_id
Value: webform_client_form_41
Argument : op
Value: Submit
Argument : submitted[email]
Argument : submitted[message]
Argument : submitted[name]
Argument : submitted[topic]


+ CGI : /audits/social-engineering-campaigns
Methods : POST
Argument : captcha_cacheable
Value: 1
Argument : captcha_response
Value: Google no captcha
Argument : captcha_sid
Value: 3954316
Argument : captcha_token
Value: 67163ff390115269c7010546a0fc76e8
Argument : details[finished]
Value: 0
Argument : details[page_count]
Value: 1
```

```
Argument : details[page_num]
Value: 1
Argument : details[sid]
Argument : form_build_id
Value: form-pCHv5J1JUWMuHGxTnrUfcFo6V8wtn2ew6XOSpT4z5oM
Argument : form_id
Value: webform_client_form_41
Argument : op
Value: Submit
Argument : submitted[email]
Argument : submitted[message]
Argument : submitted[name]
Argument : submitted[topic]


+ CGI : /audits/web-security-testing
Methods : POST
Argument : captcha_cacheable
Value: 1
Argument : captcha_response
Value: Google no captcha
Argument : captcha_sid
Value: 3954318
Argument : captcha_token
Value: 3fea24e9d36533cc27f5753351fa1d3e
Argument : details[finished]
Value: 0
Argument : details[page_count]
Value: 1
Argument : details[page_num]
Value: 1
Argument : details[sid]
Argument : form_build_id
Value: form-x4AOXi0xSJstZAStN8ZKffuUcxOfAA3aik9ZczFgCoY
Argument : form_id
Value: webform_client_form_41
Argument : op
Value: Submit
Argument : submitted[email]
Argument : submitted[message]
Argument : submitted[name]
Argument : submitted[topic]


+ CGI : /training/user-awareness
Methods : POST
Argument : captcha_cacheable
Value: 1
Argument : captcha_response
Value: Google no captcha
Argument : captcha_sid
Value: 3954320
Argument : captcha_token
Value: 00d80e8211548ae9a4ee7dcb7aa70125
Argument : details[finished]
Value: 0
Argument : details[page_count]
Value: 1
Argument : details[page_num]
Value: 1
Argument : details[sid]
Argument : form_build_id
Value: form--kNu3U82BJIYq6dGDUqj2Te7bl3wPMnSDZzOqFDZom0
Argument : form_id
Value: webform_client_form_80
Argument : op
Value: Verstuur
Argument : submitted[email]
Argument : submitted[message]
Argument : submitted[name]
Argument : submitted[topic]
Value: phishing


+ CGI : /training/web-security-bootcamp
Methods : POST
Argument : captcha_cacheable
Value: 1
Argument : captcha_response
Value: Google no captcha
Argument : captcha_sid
Value: 3954322
Argument : captcha_token
Value: 276fbe1129b6d43b30e5663946d912f2
Argument : details[finished]
Value: 0
Argument : details[page_count]
Value: 1
Argument : details[page_num]
Value: 1
```

```
Argument : details[sid]
Argument : form_build_id
Value: form-WLTnLW8kx_1y71w31_687W6MErN9oDOuvI8aA3u-suA
Argument : form_id
Value: webform_client_form_41
Argument : op
Value: Submit
Argument : submitted[email]
Argument : submitted[message]
Argument : submitted[name]
Argument : submitted[topic]


+ CGI : /software/managed-security-awareness
Methods : POST
Argument : captcha_cacheable
Value: 1
Argument : captcha_response
Value: Google no captcha
Argument : captcha_sid
Value: 3954324
Argument : captcha_token
Value: b62308d10c6d2878c0e0bb134304c172
Argument : details[finished]
Value: 0
Argument : details[page_count]
Value: 1
Argument : details[page_num]
Value: 1
Argument : details[sid]
Argument : form_build_id
Value: form-kj-tfvi_D8dBUyJQGKpmytFsjex_kPgl0-NsxKk7fmc
Argument : form_id
Value: webform_client_form_41
Argument : op
Value: Submit
Argument : submitted[email]
Argument : submitted[message]
Argument : submitted[name]
Argument : submitted[topic]


+ CGI : /software/vulnerability-assessment-solution
Methods : POST
Argument : captcha_cacheable
Value: 1
Argument : captcha_response
Value: Google no captcha
Argument : captcha_sid
Value: 3954326
Argument : captcha_token
Value: e70f08285fc0a129846a011e710da268
Argument : details[finished]
Value: 0
Argument : details[page_count]
Value: 1
Argument : details[page_num]
Value: 1
Argument : details[sid]
Argument : form_build_id
Value: form-V0iqFnhABX8BaNOHZuJwiYqvUAGoyOqoLGCiQGY-EbU
Argument : form_id
Value: webform_client_form_41
Argument : op
Value: Submit
Argument : submitted[email]
Argument : submitted[message]
Argument : submitted[name]
Argument : submitted[topic]


+ CGI : /news-items
Methods : GET
Argument : page
Value: 2


+ CGI : /contact
Methods : POST
Argument : captcha_cacheable
Value: 1
Argument : captcha_response
Value: Google no captcha
Argument : captcha_sid
Value: 3954328
Argument : captcha_token
Value: 65830c2dc76cedfc91155653b1de783b
Argument : details[finished]
Value: 0
Argument : details[page_count]
```

```
Value: 1
Argument : details[page_num]
Value: 1
Argument : details[sid]
Argument : form_build_id
Value: form-dSJ0Npqm-GgMpZlQ-XCIa6OVP6pjIWx-auClhuEyiA0
Argument : form_id
Value: webform_client_form_12
Argument : op
Value: Submit
Argument : submitted[email]
Argument : submitted[message]
Argument : submitted[name]
Argument : submitted[topic]
Value: general


+ CGI : /software/web-application-security-scanner
Methods : POST
Argument : captcha_cacheable
Value: 1
Argument : captcha_response
Value: Google no captcha
Argument : captcha_sid
Value: 3954336
Argument : captcha_token
Value: a962a0c2f57e2855dfe820dd75e0227c
Argument : details[finished]
Value: 0
Argument : details[page_count]
Value: 1
Argument : details[page_num]
Value: 1
Argument : details[sid]
Argument : form_build_id
Value: form-nB9e-1LnWqOQzw4jYeTk_nuAC5nVaDFBAupSN5ZMyZs
Argument : form_id
Value: webform_client_form_41
Argument : op
Value: Submit
Argument : submitted[email]
Argument : submitted[message]
Argument : submitted[name]
Argument : submitted[topic]


+ CGI : /training/awareness-for-employees
Methods : POST
Argument : captcha_cacheable
Value: 1
Argument : captcha_response
Value: Google no captcha
Argument : captcha_sid
Value: 3954339
Argument : captcha_token
Value: d544f4f8b6fecdd09bba338f75f28ee1
Argument : details[finished]
Value: 0
Argument : details[page_count]
Value: 1
Argument : details[page_num]
Value: 1
Argument : details[sid]
Argument : form_build_id
Value: form-5RqTSiLUpGEh6T_SmfakdVH6Bn61vld8kZthflF_MWk
Argument : form_id
Value: webform_client_form_41
Argument : op
Value: Submit
Argument : submitted[email]
Argument : submitted[message]
Argument : submitted[name]
Argument : submitted[topic]


+ CGI : /node/75/register
Methods : POST
Argument : captcha_cacheable
Value: 1
Argument : captcha_response
Value: Google no captcha
Argument : captcha_sid
Value: 3954341
Argument : captcha_token
Value: 756ac9c6b98ba335b6f6c96a2fec626e
Argument : email
Argument : field_first_name[und][0][value]
Argument : field_last_name[und][0][value]
Argument : field_telephone[und][0][value]
Argument : form_build_id
```

```
Value: form-YeXWIlvbf7xD_lzOTlMx7YZgk1xlINWK5kWHYztuXMc
Argument : form_id
Value: node_registration_form
Argument : op
Value: Create registration


+ CGI : /node/63/register
Methods : POST
Argument : captcha_cacheable
Value: 1
Argument : captcha_response
Value: Google no captcha
Argument : captcha_sid
Value: 3954343
Argument : captcha_token
Value: a642240b4d8340ba4c6990156d4347ff
Argument : email
Argument : field_first_name[und][0][value]
Argument : field_last_name[und][0][value]
Argument : field_telephone[und][0][value]
Argument : form_build_id
Value: form-quiX2tM0czofSfE3pFWqF_frkm3fFwA0tzZ4OYMsQu4
Argument : form_id
Value: node_registration_form
Argument : op
Value: Create registration


+ CGI : /contact-us-1
Methods : POST
Argument : captcha_cacheable
Value: 1
Argument : captcha_response
Value: Google no captcha
Argument : captcha_sid
Value: 3954360
Argument : captcha_token
Value: 93902a23c05ed3ae88995668be21bdde
Argument : details[finished]
Value: 0
Argument : details[page_count]
Value: 1
Argument : details[page_num]
Value: 1
Argument : details[sid]
Argument : form_build_id
Value: form-11kz5pTOiWAsir8zs74hLeDzIom-FSvohvgjpks_Qjs
Argument : form_id
Value: webform_client_form_12
Argument : op
Value: Submit
Argument : submitted[email]
Argument : submitted[message]
Argument : submitted[name]
Argument : submitted[topic]
Value: general
```

11419 (1) - Web Server Office File Inventory

Synopsis

The remote web server hosts office-related files.

Description

This plugin connects to the remote web server and attempts to find office-related files such as .doc, .ppt, .xls, .pdf etc.

Solution

Make sure that such files do not contain any confidential or otherwise sensitive information and that they are only accessible to those with valid credentials.

Risk Factor

None

Plugin Information

Published: 2003/03/19, Modified: 2022/04/11

Plugin Output

itsecgames.com (tcp/80/www)

```
The following office-related files are available on the remote server :

- Adobe Acrobat files (.pdf) :
/downloads/bWAPP_intro.pdf
```

19506 (1) - 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: 2025/06/25

Plugin Output

itsecgames.com (tcp/0)

```
Information about this scan :

Nessus version : 10.9.3
Nessus build : 20023
Plugin feed version : 202509050739
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : Itsecgames.com Web App Scan
Scan policy used : Web Application Tests
Scanner IP : 10.81.24.60
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 421.845 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : 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 did not launch)
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 : 2025/9/6 14:22 India Standard Time (UTC +05:30)
Scan duration : 12786 sec
Scan for malware : no
```

24260 (1) - 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 is 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: 2024/02/26

Plugin Output

itsecgames.com (tcp/80/www)

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

Date: Sat, 06 Sep 2025 10:38:23 GMT
Server: Apache
Last-Modified: Wed, 09 Feb 2022 13:14:08 GMT
ETag: "e43-5d7959bd3c800"
Accept-Ranges: bytes
Content-Length: 3651
Vary: Accept-Encoding
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html

Response Body :

<!DOCTYPE html>
<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Architects+Daughter">
<link rel="stylesheet" type="text/css" href="stylesheets/stylesheet.css" media="screen" />
<link rel="shortcut icon" href="images/favicon.ico" type="image/x-icon" />

<!--<script src="//html5shiv.googlecode.com/svn/trunk/html5.js"></script>-->
<script src="js/html5.js"></script>

<title>bWAPP, a buggy web application!</title>

</head>

<body>

<header>

<h1>bWAPP</h1>
```

```
<h2>an extremely buggy web app !</h2>

</header>

<div id="menu">

<table>

<tr>

<td><font color="#ffb717">Home</font></td>
<td><a href="bugs.htm">Bugs</a></td>
<td><a href="download.htm">Download</a></td>
<td><a href="training.htm">Talks & Training</a></td>
<td><a href="http://itsecgames.blogspot.com" target="_blank">Blog</a></td>

</tr>

</table>

</div>

<div id="main">

<h1>Home</h1>

<p>bWAPP, or a <i>buggy web application</i>, is a free and open source deliberately insecure web application.<br />
It helps security enthusiasts, developers and students to discover and to prevent web vulnerabilities.<br />
bWAPP prepares one to conduct successful penetration testing and ethical hacking projects.</p>

<p>What makes bWAPP so unique? Well, it has over <a href="./downloads/vulnerabilities.txt" target="blank">100 web
vulnerabilities</a>!<br />
It covers all major known web bugs, including all risks from the OWASP Top 10 project.</p>

<p>bWAPP is a PHP application that uses a MySQL database. It can be hosted on Linux/Windows with Apache/IIS and MySQL.
It can also be installed with WAMP or XAMPP.<br />
Another possibility is to download the <i>bee-box</i>, a custom Linux VM pre-installed with bWAPP.</p>

<p>Download our <a href="./downloads/bWAPP_intro.pdf" target="_blank">What is bWAPP?</a> introduction tutorial, including free
exercises...</p>

<p>bWAPP is for web application security-testing and educational purposes only.<br />
Have fun with this free and open source project!</p>

<p>Cheers, Malik Mesellem</p>

</div>

<div id="sponsor">

<table>

<tr>
<td align="center"><a href="https://www.mmesec.com" target="_blank"><img src="./images/mme.png"></a> </td>
<td>    </td>
<td align="center"><a href="https://www.owasp.org" target="_blank"><img src="./images/owasp.png"></a></td>

</tr>

</table>

</div>

<div id="side">

<a href="https://twitter.com/MME_IT" target="blank_" class="button"><img src="./images/twitter.png"></a>
<a href="https://be.linkedin.com/in/malikmesellem" target="blank_" class="button"><img src="./images/linkedin.png"></a>
<a href="https://www.facebook.com/mmebv/" target="blank_" class="button"><img src="./images/facebook.png"></a>
<a href="https://itsecgames.blogspot.com" target="blank_" class="button"><img src="./images/blogger.png"></a>

</div>

<div id="disclaimer">

<p>bWAPP is licensed under <a rel="license" href="http://creativecommons.org/licenses/by-nc-nd/4.0/" target="_blank"><img
style="vertical-align:middle" src="./images/cc.png"></a> &copy; 2022 MME BV / Follow <a href="https://twitter.com/MME_IT"
target="_blank">@MME_IT</a> on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive <a
href="https://www.mmesec.com/training" target="blank_">training</a>?</p>

</div>

<div id="bee">

<img src="./images/bee_1.png">

</div>

</body>
```

```
</html>
```

43111 (1) - HTTP Methods Allowed (per directory)

Synopsis

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

Description

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

The following HTTP methods are considered insecure:
PUT, DELETE, CONNECT, TRACE, HEAD

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

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes' in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

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

See Also

http://www.nessus.org/u?d9c03a9a
http://www.nessus.org/u?b019cbdb
https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/12/10, Modified: 2022/04/11

Plugin Output

itsecgames.com (tcp/80/www)

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

- HTTP methods GET HEAD OPTIONS POST are allowed on :

/
/downloads
/icons
/images
/javascript
/js
/stylesheets


Based on tests of each method :

- HTTP methods GET HEAD OPTIONS POST are allowed on :

/
/downloads
/icons
/images
/javascript
/js
/stylesheets
```

48204 (1) - 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-0030
XREF	IAVT:0001-T-0530

Plugin Information

Published: 2010/07/30, Modified: 2023/08/17

Plugin Output

itsecgames.com (tcp/80/www)

```
URL : http://itsecgames.com/
Version : unknown
Source : Server: Apache
backported : 0
```

49705 (1) - 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

itsecgames.com (tcp/443/www)

```
The following email address has been gathered :

- 'info@mmesec.com', referenced from :
/audits/penetration-testing
/news/technical-awareness
/news/een-hack-proof-nieuwjaar
/training/user-awareness
/audits/vulnerability-assessment
/training/cyber-security-bootcamp
/cyber-security-bootcamp-26092025
/news/op-user-awareness-staat-geen-leeftijd
```

```
/node
/training/web-security-bootcamp
/security-audits
/news-items
/security-training
/audits/web-security-testing
/news/mme-cyberclass
/news/kmo-portefeuille
/news/fast-track
/training/ethical-hacking-bootcamp
/software/web-application-security-scanner
/node/75/register
/
/ethical-hacking-bootcamp-17092025
/about
/news/blackhat-usa
/software
/audits/full-security-audit
/news/menselijke-firewall
/software/managed-security-awareness
/node/63/register
/news/nis2-richtlijn
/news/webinar-cybersecurity-awareness
/software/vulnerability-assessment-solution
/audits/social-engineering-campaigns
/contact
/news/een-cyber-veilig-nieuwjaar
/contact-us-1
/software/web-security-testing-framework
/training/awareness-for-employees
```

50345 (1) - 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

itsecgames.com (tcp/80/www)

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

- http://itsecgames.com/
- http://itsecgames.com/bugs.htm
- http://itsecgames.com/download.htm
- http://itsecgames.com/index.htm
- http://itsecgames.com/training.htm
```

84502 (1) - 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: 2024/08/09

Plugin Output

itsecgames.com (tcp/443/www)

```
HTTP/1.1 200 OK
Date: Sat, 06 Sep 2025 08:56:02 GMT
Server: Apache
Expires: Sun, 19 Nov 1978 05:00:00 GMT
Cache-Control: no-cache, must-revalidate
X-Content-Type-Options: nosniff
Content-Language: en
X-Frame-Options: SAMEORIGIN
X-UA-Compatible: IE=edge
X-Generator: Drupal 7 (http://drupal.org)
Link: <https://itsecgames.com/>; rel="canonical",<https://itsecgames.com/>; rel="shortlink"
Vary: Accept-Encoding
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8


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

tenable Nessus

Report generated by Tenable Nessus™

Itsecgames.com Web App Scan

Sat, 06 Sep 2025 17:55:48 India Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

Collapse All | Expand All

itsecgames.com

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	1	0	22

Host Information

DNS Name:	itsecgames.com
IP:	31.3.96.40
OS:	Linux Kernel 2.6

Vulnerabilities

142960 - HSTS Missing From HTTPS Server (RFC 6797) -

Synopsis

The remote web server is not enforcing HSTS, as defined by RFC 6797.

Description

The remote web server is not enforcing HSTS, as defined by RFC 6797. 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

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

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

Plugin Information

Published: 2020/11/17, Modified: 2024/03/22

Plugin Output

tcp/443/www

```
HTTP/1.1 200 OK
Date: Sat, 06 Sep 2025 08:56:02 GMT
Server: Apache
Expires: Sun, 19 Nov 1978 05:00:00 GMT
Cache-Control: no-cache, must-revalidate
X-Content-Type-Options: nosniff
Content-Language: en
X-Frame-Options: SAMEORIGIN
X-UA-Compatible: IE=edge
X-Generator: Drupal 7 (http://drupal.org)
Link: <https://itsecgames.com/>; rel="canonical",<https://itsecgames.com/>; rel="shortlink"
Vary: Accept-Encoding
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8


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

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-0030
XREF	IAVT:0001-T-0530

Plugin Information

Published: 2010/07/30, Modified: 2023/08/17

Plugin Output

tcp/80/www

```
URL : http://itsecgames.com/
Version : unknown
Source : Server: Apache
backported : 0
```

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

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

http://creativecommons.org/licenses/by-nc-nd/4.0/ - /
http://itsecgames.blogspot.com - /
https://be.linkedin.com/in/malikmesellem - /
https://fonts.googleapis.com/css?family=Architects+Daughter - /
https://itsecgames.blogspot.com - /
https://sourceforge.net/projects/bwapp/files/bWAPP/ - /download.htm
https://sourceforge.net/projects/bwapp/files/bee-box/ - /download.htm

https://twitter.com/MME_IT - /
https://www.facebook.com/mmebv/ - /
https://www.mmesec.com - /
https://www.mmesec.com/training - /
https://www.mmesec.com/training/cyber-security-bootcamp - /training.htm
https://www.mmesec.com/training/ethical-hacking-bootcamp - /training.htm
https://www.mmesec.com/training/web-security-bootcamp - /training.htm
https://www.owasp.org - /
```

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://sourceforge.net/projects/bwapp/ - /software/web-security-testing-framework
http://www.mmesec.com - /
https://ccb.belgium.be/nl/de-nis2-richtlijn-wat-betekent-dit-voor-mijn-organisatie - /news-items
https://customerconnect.vmware.com/en/downloads/info/slug/desktop_end_user_computing/vmware_workstation_player/16_0 -
/training/ethical-hacking-bootcamp
https://fonts.googleapis.com/css?family=Roboto+Condensed:300,300italic&subset=latin-ext - /
https://gdpr.eu - /audits/full-security-audit
https://maps.google.com/?q=50.80355,3.126870&z=15&output=embed&t=m&iwloc=near - /contact

https://www.mmesec.com/about - /
https://www.mmesec.com/audits/penetration-testing - /
https://www.mmesec.com/gdpr - /
https://www.mmesec.com/security-audits - /
https://www.mmesec.com/security-training - /
https://www.mmesec.com/software/vulnerability-assessment-solution - /
https://www.mmesec.com/training -
https://www.mmesec.com/training/ethical-hacking-bootcamp -
```

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: 2024/08/09

Plugin Output

tcp/443/www

```
HTTP/1.1 200 OK
Date: Sat, 06 Sep 2025 08:56:02 GMT
Server: Apache
Expires: Sun, 19 Nov 1978 05:00:00 GMT
Cache-Control: no-cache, must-revalidate
X-Content-Type-Options: nosniff
Content-Language: en
X-Frame-Options: SAMEORIGIN
X-UA-Compatible: IE=edge
X-Generator: Drupal 7 (http://drupal.org)
Link: <https://itsecgames.com/>; rel="canonical",<https://itsecgames.com/>; rel="shortlink"
Vary: Accept-Encoding
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8


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

43111 - HTTP Methods Allowed (per directory)

Synopsis

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

Description

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

The following HTTP methods are considered insecure:
PUT, DELETE, CONNECT, TRACE, HEAD

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

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes' in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

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

See Also

http://www.nessus.org/u?d9c03a9a
http://www.nessus.org/u?b019cbdb
https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/12/10, Modified: 2022/04/11

Plugin Output

tcp/80/www

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

- HTTP methods GET HEAD OPTIONS POST are allowed on :

/
/downloads
/icons
/images
/javascript
/js
/stylesheets


Based on tests of each method :

- HTTP methods GET HEAD OPTIONS POST are allowed on :

/
/downloads
/icons
/images
/javascript
/js
/stylesheets
```

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 is 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: 2024/02/26

Plugin Output

tcp/80/www

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

Date: Sat, 06 Sep 2025 10:38:23 GMT
Server: Apache
Last-Modified: Wed, 09 Feb 2022 13:14:08 GMT
ETag: "e43-5d7959bd3c800"
Accept-Ranges: bytes
Content-Length: 3651
Vary: Accept-Encoding
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html

Response Body :

<!DOCTYPE html>
<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Architects+Daughter">
<link rel="stylesheet" type="text/css" href="stylesheets/stylesheet.css" media="screen" />
<link rel="shortcut icon" href="images/favicon.ico" type="image/x-icon" />

<!--<script src="//html5shiv.googlecode.com/svn/trunk/html5.js"></script>-->
<script src="js/html5.js"></script>

<title>bWAPP, a buggy web application!</title>

</head>

<body>

<header>

<h1>bWAPP</h1>

<h2>an extremely buggy web app !</h2>

</header>

<div id="menu">

<table>

<tr>

<td><font color="#ffb717">Home</font></td>
<td><a href="bugs.htm">Bugs</a></td>
<td><a href="download.htm">Download</a></td>
<td><a href="training.htm">Talks & Training</a></td>
<td><a href="http://itsecgames.blogspot.com" target="_blank">Blog</a></td>

</tr>
```

```
</table>

</div>

<div id="main">

<h1>Home</h1>

<p>bWAPP, or a <i>buggy web application</i>, is a free and open source deliberately insecure web application.<br />
It helps security enthusiasts, developers and students to discover and to prevent web vulnerabilities.<br />
bWAPP prepares one to conduct successful penetration testing and ethical hacking projects.</p>

<p>What makes bWAPP so unique? Well, it has over <a href="./downloads/vulnerabilities.txt" target="blank">100 web
vulnerabilities</a>!<br />
It covers all major known web bugs, including all risks from the OWASP Top 10 project.</p>

<p>bWAPP is a PHP application that uses a MySQL database. It can be hosted on Linux/Windows with Apache/IIS and MySQL.
It can also be installed with WAMP or XAMPP.<br />
Another possibility is to download the <i>bee-box</i>, a custom Linux VM pre-installed with bWAPP.</p>

<p>Download our <a href="./downloads/bWAPP_intro.pdf" target="_blank">What is bWAPP?</a> introduction tutorial, including free
exercises...</p>

<p>bWAPP is for web application security-testing and educational purposes only.<br />
Have fun with this free and open source project!</p>

<p>Cheers, Malik Mesellem</p>

</div>

<div id="sponsor">

<table>

<tr>
<td align="center"><a href="https://www.mmesec.com" target="_blank"><img src="./images/mme.png"></a> </td>
<td>    </td>
<td align="center"><a href="https://www.owasp.org" target="_blank"><img src="./images/owasp.png"></a></td>

</tr>

</table>

</div>

<div id="side">

<a href="https://twitter.com/MME_IT" target="blank_" class="button"><img src="./images/twitter.png"></a>
<a href="https://be.linkedin.com/in/malikmesellem" target="blank_" class="button"><img src="./images/linkedin.png"></a>
<a href="https://www.facebook.com/mmebv/" target="blank_" class="button"><img src="./images/facebook.png"></a>
<a href="https://itsecgames.blogspot.com" target="blank_" class="button"><img src="./images/blogger.png"></a>

</div>

<div id="disclaimer">

<p>bWAPP is licensed under <a rel="license" href="http://creativecommons.org/licenses/by-nc-nd/4.0/" target="_blank"><img
style="vertical-align:middle" src="./images/cc.png"></a> &copy; 2022 MME BV / Follow <a href="https://twitter.com/MME_IT"
target="_blank">@MME_IT</a> on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive <a
href="https://www.mmesec.com/training" target="blank_">training</a>?</p>

</div>

<div id="bee">

<img src="./images/bee_1.png">

</div>

</body>

</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/80/www

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

- http://itsecgames.com/
- http://itsecgames.com/bugs.htm
- http://itsecgames.com/download.htm
- http://itsecgames.com/index.htm
- http://itsecgames.com/training.htm
```

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://itsecgames.com/
- https://itsecgames.com/about
- https://itsecgames.com/audits/full-security-audit
- https://itsecgames.com/audits/penetration-testing
- https://itsecgames.com/audits/social-engineering-campaigns
- https://itsecgames.com/audits/vulnerability-assessment
- https://itsecgames.com/audits/web-security-testing
- https://itsecgames.com/contact
- https://itsecgames.com/contact-us-1
- https://itsecgames.com/cyber-security-bootcamp-26092025
- https://itsecgames.com/ethical-hacking-bootcamp-17092025
- https://itsecgames.com/news-items
- https://itsecgames.com/news/blackhat-usa
- https://itsecgames.com/news/een-cyber-veilig-nieuwjaar
- https://itsecgames.com/news/een-hack-proof-nieuwjaar
- https://itsecgames.com/news/fast-track
- https://itsecgames.com/news/kmo-portefeuille
- https://itsecgames.com/news/menselijke-firewall
- https://itsecgames.com/news/mme-cyberclass
- https://itsecgames.com/news/nis2-richtlijn
- https://itsecgames.com/news/op-user-awareness-staat-geen-leeftijd
- https://itsecgames.com/news/technical-awareness
- https://itsecgames.com/news/webinar-cybersecurity-awareness
- https://itsecgames.com/node
- https://itsecgames.com/node/63/register
- https://itsecgames.com/node/75/register
- https://itsecgames.com/security-audits
- https://itsecgames.com/security-training
- https://itsecgames.com/software
- https://itsecgames.com/software/managed-security-awareness
- https://itsecgames.com/software/vulnerability-assessment-solution
- https://itsecgames.com/software/web-application-security-scanner
- https://itsecgames.com/software/web-security-testing-framework
- https://itsecgames.com/training/awareness-for-employees
- https://itsecgames.com/training/cyber-security-bootcamp
- https://itsecgames.com/training/ethical-hacking-bootcamp
- https://itsecgames.com/training/user-awareness
- https://itsecgames.com/training/web-security-bootcamp
```

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://itsecgames.com/
- http://itsecgames.com/bugs.htm
- http://itsecgames.com/download.htm
```

```
- http://itsecgames.com/index.htm
- http://itsecgames.com/training.htm
```

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/07/14

Plugin Output

tcp/22

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

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/07/14

Plugin Output

tcp/80/www

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

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/07/14

Plugin Output

tcp/443/www

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

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2025/06/25

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.9.3
Nessus build : 20023
```

```
Plugin feed version : 202509050739
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : Itsecgames.com Web App Scan
Scan policy used : Web Application Tests
Scanner IP : 10.81.24.60
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 421.845 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : 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 did not launch)
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 : 2025/9/6 14:22 India Standard Time (UTC +05:30)
Scan duration : 12786 sec
Scan for malware : no
```

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://itsecgames.com/
- http://itsecgames.com/bugs.htm
- http://itsecgames.com/download.htm
- http://itsecgames.com/downloads/bWAPP_intro.pdf
- http://itsecgames.com/downloads/vulnerabilities.txt
- http://itsecgames.com/images/bWAPP_10.png
- http://itsecgames.com/images/bWAPP_11.png
- http://itsecgames.com/images/bWAPP_12.png
```

```
- http://itsecgames.com/images/bWAPP_13.png
- http://itsecgames.com/images/bWAPP_2.png
- http://itsecgames.com/images/bWAPP_3.png
- http://itsecgames.com/images/bWAPP_4.png
- http://itsecgames.com/images/bWAPP_5.png
- http://itsecgames.com/images/bWAPP_6.png
- http://itsecgames.com/images/bWAPP_7.png
- http://itsecgames.com/images/bWAPP_8.png
- http://itsecgames.com/images/bWAPP_9.png
- http://itsecgames.com/images/favicon.ico
- http://itsecgames.com/index.htm
- http://itsecgames.com/stylesheets/stylesheet.css
- http://itsecgames.com/training.htm

Attached is a copy of the sitemap file.
```

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://itsecgames.com/
- https://itsecgames.com/about
- https://itsecgames.com/audits/full-security-audit
- https://itsecgames.com/audits/penetration-testing
- https://itsecgames.com/audits/social-engineering-campaigns
- https://itsecgames.com/audits/vulnerability-assessment
- https://itsecgames.com/audits/web-security-testing
- https://itsecgames.com/contact
- https://itsecgames.com/contact-us-1
- https://itsecgames.com/cyber-security-bootcamp-26092025
- https://itsecgames.com/ethical-hacking-bootcamp-17092025
- https://itsecgames.com/news-items
- https://itsecgames.com/news/blackhat-usa
- https://itsecgames.com/news/een-cyber-veilig-nieuwjaar
- https://itsecgames.com/news/een-hack-proof-nieuwjaar
- https://itsecgames.com/news/fast-track
- https://itsecgames.com/news/kmo-portefeuille
- https://itsecgames.com/news/menselijke-firewall
- https://itsecgames.com/news/mme-cyberclass
- https://itsecgames.com/news/nis2-richtlijn
- https://itsecgames.com/news/op-user-awareness-staat-geen-leeftijd
- https://itsecgames.com/news/technical-awareness
- https://itsecgames.com/news/webinar-cybersecurity-awareness
- https://itsecgames.com/node
- https://itsecgames.com/node/63/register
- https://itsecgames.com/node/75/register
- https://itsecgames.com/security-audits
- https://itsecgames.com/security-training
- https://itsecgames.com/sites/default/files/downloads/OWASP_Top_10.pdf
- https://itsecgames.com/sites/default/files/downloads/bWAPP_sample_report.pdf
- https://itsecgames.com/sites/default/files/favicon.ico
```

```
- https://itsecgames.com/sites/default/files/images/bWAPP-1.png
- https://itsecgames.com/sites/default/files/images/bWAPP-2.png
- https://itsecgames.com/sites/default/files/images/bWAPP-3.png
- https://itsecgames.com/sites/default/files/images/bWAPP-4.png
- https://itsecgames.com/sites/default/files/images/bWAPP-5.png
- https://itsecgames.com/sites/default/files/images/bWAPP-6.png
- https://itsecgames.com/sites/default/files/images/bWAPP-7.png
- https://itsecgames.com/sites/default/files/images/bWAPP-8.png
- https://itsecgames.com/sites/default/files/images/netsparker-1.png
- https://itsecgames.com/sites/default/files/images/netsparker-2.png
- https://itsecgames.com/sites/default/files/images/phished-1.png
- https://itsecgames.com/sites/default/files/images/phished-2.png
- https://itsecgames.com/sites/default/files/images/phished-3.png
- https://itsecgames.com/sites/default/files/images/phished-4.png
- https://itsecgames.com/sites/default/files/images/phished-7.png
- https://itsecgames.com/sites/default/files/images/phished-9.png
- https://itsecgames.com/software
- https://itsecgames.com/software/managed-security-awareness
- https://itsecgames.com/software/vulnerability-assessment-solution
- https://itsecgames.com/software/web-application-security-scanner
- https://itsecgames.com/software/web-security-testing-framework
- https://itsecgames.com/training/awareness-for-employees
- https://itsecgames.com/training/cyber-security-bootcamp
- https://itsecgames.com/training/ethical-hacking-bootcamp
- https://itsecgames.com/training/user-awareness
- https://itsecgames.com/training/web-security-bootcamp

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: 2024/06/07

Plugin Output

tcp/80/www

```
The following directories were discovered:
/downloads, /icons, /images, /javascript, /js

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: 2024/06/07

Plugin Output

tcp/443/www

```
The following directories were discovered:
/includes, /sites, /icons, /javascript, /misc, /scripts

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/443/www

```
The following email address has been gathered :

- 'info@mmesec.com', referenced from :
/audits/penetration-testing
```

```
/news/technical-awareness
/news/een-hack-proof-nieuwjaar
/training/user-awareness
/audits/vulnerability-assessment
/training/cyber-security-bootcamp
/cyber-security-bootcamp-26092025
/news/op-user-awareness-staat-geen-leeftijd
/node
/training/web-security-bootcamp
/security-audits
/news-items
/security-training
/audits/web-security-testing
/news/mme-cyberclass
/news/kmo-portefeuille
/news/fast-track
/training/ethical-hacking-bootcamp
/software/web-application-security-scanner
/node/75/register
/
/ethical-hacking-bootcamp-17092025
/about
/news/blackhat-usa
/software
/audits/full-security-audit
/news/menselijke-firewall
/software/managed-security-awareness
/node/63/register
/news/nis2-richtlijn
/news/webinar-cybersecurity-awareness
/software/vulnerability-assessment-solution
/audits/social-engineering-campaigns
/contact
/news/een-cyber-veilig-nieuwjaar
/contact-us-1
/software/web-security-testing-framework
/training/awareness-for-employees
```

11419 - Web Server Office File Inventory

Synopsis

The remote web server hosts office-related files.

Description

This plugin connects to the remote web server and attempts to find office-related files such as .doc, .ppt, .xls, .pdf etc.

Solution

Make sure that such files do not contain any confidential or otherwise sensitive information and that they are only accessible to those with valid credentials.

Risk Factor

None

Plugin Information

Published: 2003/03/19, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
The following office-related files are available on the remote server :

- Adobe Acrobat files (.pdf) :
/downloads/bWAPP_intro.pdf
```

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: 2025/07/14

Plugin Output

tcp/443/www

```
Webmirror performed 122 queries in 395s (0.0308 queries per second)

The following CGIs have been discovered :


+ CGI : /audits/full-security-audit
Methods : POST
Argument : captcha_cacheable
Value: 1
Argument : captcha_response
Value: Google no captcha
Argument : captcha_sid
Value: 3954312
Argument : captcha_token
Value: af38de3ed978b6b099c0a662a6ffd0b9
Argument : details[finished]
Value: 0
Argument : details[page_count]
Value: 1
Argument : details[page_num]
Value: 1
Argument : details[sid]
Argument : form_build_id
Value: form-ZjMxwi3pDWB0I00H74OhmYaLRhm69bxDcGAGRcjXZBM
Argument : form_id
Value: webform_client_form_41
Argument : op
Value: Submit
Argument : submitted[email]
Argument : submitted[message]
Argument : submitted[name]
Argument : submitted[topic]


+ CGI : /audits/vulnerability-assessment
Methods : POST
Argument : captcha_cacheable
Value: 1
Argument : captcha_response
Value: Google no captcha
Argument : captcha_sid
Value: 3954314
Argument : captcha_token
Value: 04038b74d6d4d4909917b74ca4e8cd50
Argument : details[finished]
Value: 0
Argument : details[page_count]
Value: 1
Argument : details[page_num]
Value: 1
Argument : details[sid]
Argument : form_build_id
Value: form-EilenJuKC9OyATZ0RPzGUo_ONKLy5ELcFLBSBzBAaIU
Argument : form_id
Value: webform_client_form_41
Argument : op
Value: Submit
Argument : submitted[email]
Argument : submitted[message]
Argument : submitted[name]
Argument : submitted[topic]


+ CGI : /audits/social-engineering-campaigns
```

```
Methods : POST
Argument : captcha_cacheable
Value: 1
Argument : captcha_response
Value: Google no captcha
Argument : captcha_sid
Value: 3954316
Argument : captcha_token
Value: 67163ff390115269c7010546a0fc76e8
Argument : details[finished]
Value: 0
Argument : details[page_count]
Value: 1
Argument : details[page_num]
Value: 1
Argument : details[sid]
Argument : form_build_id
Value: form-pCHv5J1JUWMuHGxTnrUfcFo6V8wtn2ew6XOSpT4z5oM
Argument : form_id
Value: webform_client_form_41
Argument : op
Value: Submit
Argument : submitted[email]
Argument : submitted[message]
Argument : submitted[name]
Argument : submitted[topic]


+ CGI : /audits/web-security-testing
Methods : POST
Argument : captcha_cacheable
Value: 1
Argument : captcha_response
Value: Google no captcha
Argument : captcha_sid
Value: 3954318
Argument : captcha_token
Value: 3fea24e9d36533cc27f5753351fa1d3e
Argument : details[finished]
Value: 0
Argument : details[page_count]
Value: 1
Argument : details[page_num]
Value: 1
Argument : details[sid]
Argument : form_build_id
Value: form-x4AOXi0xSJstZAStN8ZKffuUcxOfAA3aik9ZczFgCoY
Argument : form_id
Value: webform_client_form_41
Argument : op
Value: Submit
Argument : submitted[email]
Argument : submitted[message]
Argument : submitted[name]
Argument : submitted[topic]


+ CGI : /training/user-awareness
Methods : POST
Argument : captcha_cacheable
Value: 1
Argument : captcha_response
Value: Google no captcha
Argument : captcha_sid
Value: 3954320
Argument : captcha_token
Value: 00d80e8211548ae9a4ee7dcb7aa70125
Argument : details[finished]
Value: 0
Argument : details[page_count]
Value: 1
Argument : details[page_num]
Value: 1
Argument : details[sid]
Argument : form_build_id
Value: form--kNu3U82BJIYq6dGDUqj2Te7bl3wPMnSDZzOqFDZom0
Argument : form_id
Value: webform_client_form_80
Argument : op
Value: Verstuur
Argument : submitted[email]
Argument : submitted[message]
Argument : submitted[name]
Argument : submitted[topic]
Value: phishing


+ CGI : /training/web-security-bootcamp
Methods : POST
Argument : captcha_cacheable
```

```
Value: 1
Argument : captcha_response
Value: Google no captcha
Argument : captcha_sid
Value: 3954322
Argument : captcha_token
Value: 276fbe1129b6d43b30e5663946d912f2
Argument : details[finished]
Value: 0
Argument : details[page_count]
Value: 1
Argument : details[page_num]
Value: 1
Argument : details[sid]
Argument : form_build_id
Value: form-WLTnLW8kx_1y71w31_687W6MErN9oDOuvI8aA3u-suA
Argument : form_id
Value: webform_client_form_41
Argument : op
Value: Submit
Argument : submitted[email]
Argument : submitted[message]
Argument : submitted[name]
Argument : submitted[topic]


+ CGI : /software/managed-security-awareness
Methods : POST
Argument : captcha_cacheable
Value: 1
Argument : captcha_response
Value: Google no captcha
Argument : captcha_sid
Value: 3954324
Argument : captcha_token
Value: b62308d10c6d2878c0e0bb134304c172
Argument : details[finished]
Value: 0
Argument : details[page_count]
Value: 1
Argument : details[page_num]
Value: 1
Argument : details[sid]
Argument : form_build_id
Value: form-kj-tfvi_D8dBUyJQGKpmytFsjex_kPgl0-NsxKk7fmc
Argument : form_id
Value: webform_client_form_41
Argument : op
Value: Submit
Argument : submitted[email]
Argument : submitted[message]
Argument : submitted[name]
Argument : submitted[topic]


+ CGI : /software/vulnerability-assessment-solution
Methods : POST
Argument : captcha_cacheable
Value: 1
Argument : captcha_response
Value: Google no captcha
Argument : captcha_sid
Value: 3954326
Argument : captcha_token
Value: e70f08285fc0a129846a011e710da268
Argument : details[finished]
Value: 0
Argument : details[page_count]
Value: 1
Argument : details[page_num]
Value: 1
Argument : details[sid]
Argument : form_build_id
Value: form-V0iqFnhABX8BaNOHZuJwiYqvUAGoyOqoLGCiQGY-EbU
Argument : form_id
Value: webform_client_form_41
Argument : op
Value: Submit
Argument : submitted[email]
Argument : submitted[message]
Argument : submitted[name]
Argument : submitted[topic]


+ CGI : /news-items
Methods : GET
Argument : page
Value: 2
```

```
+ CGI : /contact
Methods : POST
Argument : captcha_cacheable
Value: 1
Argument : captcha_response
Value: Google no captcha
Argument : captcha_sid
Value: 3954328
Argument : captcha_token
Value: 65830c2dc76cedfc91155653b1de783b
Argument : details[finished]
Value: 0
Argument : details[page_count]
Value: 1
Argument : details[page_num]
Value: 1
Argument : details[sid]
Argument : form_build_id
Value: form-dSJ0Npqm-GgMpZlQ-XCIa6OVP6pjIWx-auClhuEyiA0
Argument : form_id
Value: webform_client_form_12
Argument : op
Value: Submit
Argument : submitted[email]
Argument : submitted[message]
Argument : submitted[name]
Argument : submitted[topic]
Value: general


+ CGI : /software/web-application-security-scanner
Methods : POST
Argument : captcha_cacheable
Value: 1
Argument : captcha_response
Value: Google no captcha
Argument : captcha_sid
Value: 3954336
Argument : captcha_token
Value: a962a0c2f57e2855dfe820dd75e0227c
Argument : details[finished]
Value: 0
Argument : details[page_count]
Value: 1
Argument : details[page_num]
Value: 1
Argument : details[sid]
Argument : form_build_id
Value: form-nB9e-1LnWqOQzw4jYeTk_nuAC5nVaDFBAupSN5ZMyZs
Argument : form_id
Value: webform_client_form_41
Argument : op
Value: Submit
Argument : submitted[email]
Argument : submitted[message]
Argument : submitted[name]
Argument : submitted[topic]


+ CGI : /training/awareness-for-employees
Methods : POST
Argument : captcha_cacheable
Value: 1
Argument : captcha_response
Value: Google no captcha
Argument : captcha_sid
Value: 3954339
Argument : captcha_token
Value: d544f4f8b6fecdd09bba338f75f28ee1
Argument : details[finished]
Value: 0
Argument : details[page_count]
Value: 1
Argument : details[page_num]
Value: 1
Argument : details[sid]
Argument : form_build_id
Value: form-5RqTSiLUpGEh6T_SmfakdVH6Bn61vld8kZthflF_MWk
Argument : form_id
Value: webform_client_form_41
Argument : op
Value: Submit
Argument : submitted[email]
Argument : submitted[message]
Argument : submitted[name]
Argument : submitted[topic]


+ CGI : /node/75/register
Methods : POST
```

```
Argument : captcha_cacheable
Value: 1
Argument : captcha_response
Value: Google no captcha
Argument : captcha_sid
Value: 3954341
Argument : captcha_token
Value: 756ac9c6b98ba335b6f6c96a2fec626e
Argument : email
Argument : field_first_name[und][0][value]
Argument : field_last_name[und][0][value]
Argument : field_telephone[und][0][value]
Argument : form_build_id
Value: form-YeXWIlvbf7xD_lzOTlMx7YZgk1xlINWK5kWHYztuXMc
Argument : form_id
Value: node_registration_form
Argument : op
Value: Create registration


+ CGI : /node/63/register
Methods : POST
Argument : captcha_cacheable
Value: 1
Argument : captcha_response
Value: Google no captcha
Argument : captcha_sid
Value: 3954343
Argument : captcha_token
Value: a642240b4d8340ba4c6990156d4347ff
Argument : email
Argument : field_first_name[und][0][value]
Argument : field_last_name[und][0][value]
Argument : field_telephone[und][0][value]
Argument : form_build_id
Value: form-quiX2tM0czofSfE3pFWqF_frkm3fFwA0tzZ4OYMsQu4
Argument : form_id
Value: node_registration_form
Argument : op
Value: Create registration


+ CGI : /contact-us-1
Methods : POST
Argument : captcha_cacheable
Value: 1
Argument : captcha_response
Value: Google no captcha
Argument : captcha_sid
Value: 3954360
Argument : captcha_token
Value: 93902a23c05ed3ae88995668be21bdde
Argument : details[finished]
Value: 0
Argument : details[page_count]
Value: 1
Argument : details[page_num]
Value: 1
Argument : details[sid]
Argument : form_build_id
Value: form-11kz5pTOiWAsir8zs74hLeDzIom-FSvohvgjpks_Qjs
Argument : form_id
Value: webform_client_form_12
Argument : op
Value: Submit
Argument : submitted[email]
Argument : submitted[message]
Argument : submitted[name]
Argument : submitted[topic]
Value: general
```