tatilcity

Report generated by Nessus™ Wed, 29 May 2019 19:19:25 GMT+0300

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

www.tatilcity.net

0	0	3	0	99
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Tue May 28 19:33:38 2019
End time:	Wed May 29 19:19:23 2019

Host Information

DNS Name:	www.tatilcity.net
IP:	176.53.62.186
OS:	Linux Kernel 2.6

Vulnerabilities

40984 - Browsable Web Directories

Synopsis

Some directories on the remote web server are browsable.

Description

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

See Also

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

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information

Published: 2009/09/15, Modified: 2016/12/30

Plugin Output

tcp/80

```

The following directories are browsable :

http://www.tatilcity.net/css/
http://www.tatilcity.net/form/
```

40984 - Browsable Web Directories

Synopsis

Some directories on the remote web server are browsable.

Description

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

See Also

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

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information

Published: 2009/09/15, Modified: 2016/12/30

Plugin Output

tcp/443

```
The following directories are browsable :

https://www.tatilcity.net/css/
https://www.tatilcity.net/wp-content/cache/
https://www.tatilcity.net/wp-content/cache/min/
https://www.tatilcity.net/wp-content/cache/min/1/
https://www.tatilcity.net/wp-content/uploads/
https://www.tatilcity.net/wp-content/uploads/2018/
https://www.tatilcity.net/wp-content/uploads/2018/11/
https://www.tatilcity.net/wp-includes/
```

85582 - Web Application Potentially Vulnerable to Clickjacking

Synopsis

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

Description

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

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

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

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

See Also

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

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

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

Solution

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

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

Risk Factor

Medium

CVSS Base Score

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

References

XREF	CWE:693

Plugin Information

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

Plugin Output

tcp/443

```

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

  - https://www.tatilcity.net/
  - https://www.tatilcity.net/accommodation
  - https://www.tatilcity.net/accommodation/
  - https://www.tatilcity.net/accommodation/page/2
  - https://www.tatilcity.net/accommodation/page/2/
  - https://www.tatilcity.net/arac-kiralama/fiat-egea
  - https://www.tatilcity.net/arac-kiralama/fiat-egea/
  - https://www.tatilcity.net/arac/alfa-romeo-mito
  - https://www.tatilcity.net/arac/alfa-romeo-mito/
  - https://www.tatilcity.net/arac/bmw-5-series
  - https://www.tatilcity.net/arac/bmw-5-series/
  - https://www.tatilcity.net/arac/bmw-mini
  - https://www.tatilcity.net/arac/bmw-mini/
  - https://www.tatilcity.net/arac/citroen-ds3
  - https://www.tatilcity.net/arac/citroen-ds3/
  - https://www.tatilcity.net/arac/fiat-500
  - https://www.tatilcity.net/arac/fiat-500/
  - https://www.tatilcity.net/arac/holden-sv6
  - https://www.tatilcity.net/arac/holden-sv6/
  - https://www.tatilcity.net/arac/renault-grand-scenic
  - https://www.tatilcity.net/arac/renault-grand-scenic/
  - https://www.tatilcity.net/arac/vokswagen-polo
  - https://www.tatilcity.net/arac/vokswagen-polo/
  - https://www.tatilcity.net/author/buse
  - https://www.tatilcity.net/author/buse/
  - https://www.tatilcity.net/car
  - https://www.tatilcity.net/car/
  - https://www.tatilcity.net/cruise
  - https://www.tatilcity.net/cruise/
  - https://www.tatilcity.net/etiket/bursa
  - https://www.tatilcity.net/etiket/bursa/
  - https://www.tatilcity.net/etiket/istanbul
  - https://www.tatilcity.net/etiket/istanbul/
  - https://www.tatilcity.net/gezi-rehberi/antalya-gezi-rehberi
  - https://www.tatilcity.net/gezi-rehberi/antalya-gezi-rehberi/
  - https://www.tatilcity.net/gezi-rehberi/istanbul-gezi-rehberi
  - https://www.tatilcity.net/gezi-rehberi/istanbul-gezi-rehberi/
  - https://www.tatilcity.net/hava-limanlari/adana-sakirpasa-havalimani
  - https://www.tatilcity.net/hava-limanlari/adana-sakirpasa-havalimani/
  - https://www. [...]
```

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

Plugin Information

Published: 2010/07/30, Modified: 2018/07/31

Plugin Output

tcp/80

```
URL        : http://www.tatilcity.net/
Version    : unknown
backported : 0
```

48204 - Apache HTTP Server Version

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

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

See Also

https://httpd.apache.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/07/30, Modified: 2018/07/31

Plugin Output

tcp/443

```
URL        : https://www.tatilcity.net/
Version    : unknown
backported : 0
```

47830 - CGI Generic Injectable Parameter

Synopsis

Some CGIs are candidate for extended injection tests.

Description

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

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

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

Solution

n/a

Risk Factor

None

References

XREF	CWE:86

Plugin Information

Published: 2010/07/26, Modified: 2017/01/05

Plugin Output

tcp/443

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

+ The following resources may be vulnerable to injectable parameter :

+ The 'action' parameter of the /login/ CGI :

/login/?action=%00uwhsba

-------- output --------
float: left!important
width: 364px;
[...] -button" href="/login/?action=%00uwhsba&#038;pdf=745" target="_blank"><s [...]
var themeurl = "https:\/\/www.tatilcity.net\/wp-content\/themes\/T [...]
var date_format = "dd\/mm\/yy";
------------------------

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

/wp-login.php?log=%00uwhsba
```

```
-------- output --------
float: left!important
width: 364px;
[...] dkpdf-button" href="/login/?log=0uwhsba&#038;pdf=745" target="_blank"><s [...]
var themeurl = "https:\/\/www.tatilcity.net\/wp-content\/themes\/T [...]
var date_format = "dd\/mm\/yy";
------------------------

Clicking directly on these URLs should exhibit the issue :
(you will probably need to read the HTML source)

https://www.tatilcity.net/login/?action=%00uwhsba
https://www.tatilcity.net/wp-login.php?log=%00uwhsba
```

40406 - CGI Generic Tests HTTP Errors

Synopsis

Nessus encountered errors while running its generic CGI attacks.

Description

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

Solution

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

- Network -> Network Receive Timeout (check_read_timeout)

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

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

Risk Factor

None

Plugin Information

Published: 2009/07/28, Modified: 2011/09/21

Plugin Output

tcp/443

```
Nessus encountered :

  - 3 errors involving SSI injection checks :
   . reading the HTTP status line: errno=1 (operation timed out)
  - 2 errors involving on site request forgery checks :
   . reading the HTTP status line: errno=1 (operation timed out)
  - 1 error involving SQL injection checks :
   . reading the HTTP status line: errno=1 (operation timed out)
  - 1 error involving blind SQL injection (time based) checks :
   . reading the HTTP status line: errno=1 (operation timed out)
  - 4 errors involving XSS (on HTTP headers) checks :
   . reading the HTTP status line: errno=1 (operation timed out)
  - 34 errors involving persistent XSS checks :
```

33817 - CGI Generic Tests Load Estimation (all tests)

Synopsis

Load estimation for web application tests.

Description

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

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/10/26, Modified: 2014/03/12

Plugin Output

tcp/443

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

cross-site scripting (comprehensive test): S=20960      SP=520308     AP=520308     SC=>2G
 AC=>2G
persistent XSS                           : S=20960      SP=520308     AP=520308     SC=>2G
 AC=>2G
arbitrary command execution              : S=83840      SP=2081232    AP=2081232    SC=>2G
 AC=>2G
web code injection                       : S=5240       SP=130077     AP=130077     SC=>2G
 AC=>2G
HTML injection                           : S=10         SP=10         AP=10         SC=10         AC=10

arbitrary command execution (time based) : S=31440      SP=780462     AP=780462     SC=>2G
 AC=>2G
script injection                         : S=2          SP=2          AP=2          SC=2          AC=2

XML injection                            : S=5240       SP=130077     AP=130077     SC=>2G
 AC=>2G
unseen parameters                        : S=183400     SP=4552695    AP=4552695    SC=>2G
 AC=>2G
directory traversal (write access)       : S=10480      SP=260154     AP=260154     SC=>2G
 AC=>2G
```

```
SQL injection (2nd order)                : S=5240       SP=130077    AP=130077    SC=>2G
 AC=>2G
on site request forgery                  : S=2          SP=2         AP=2         SC=2         AC=2

blind SQL injection (4 requests)         : S=20960      SP=520308    AP=520308    SC=>2G
 AC=>2G
HTTP response splitting                  : S=18         SP=18        AP=18        SC=18        AC=18

directory traversal (extended test)      : S=267240     SP=6633927   AP=6633927   SC=>2G
 AC=>2G
header injection                         : S=4          SP=4         AP=4         SC=4         AC=4

injectable parameter                     : S=10480      SP=260154    AP=260154    SC=>2G
 AC=>2G
directory traversal                    [...]
```

39470 - CGI Generic Tests Timeout

Synopsis

Some generic CGI attacks ran out of time.

Description

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

Solution

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

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

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

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

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

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

Risk Factor

None

Plugin Information

Published: 2009/06/19, Modified: 2016/09/21

Plugin Output

tcp/443

```
The following tests timed out without finding any flaw :
- XSS (on HTTP headers)
- XML injection
- SSI injection
- XSS (on parameters names)
- SSI injection (on HTTP headers)
- SQL injection (on parameters names)
- SQL injection
- directory traversal
- directory traversal (write access)
- arbitrary command execution
- cross-site scripting (comprehensive test)
- web code injection
- SQL injection (on HTTP headers)
- arbitrary command execution (time based)
- blind SQL injection
- persistent XSS
- local file inclusion
- SQL injection (2nd order)

The following tests were interrupted and did not report all possible flaws :
- injectable parameter
```

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

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

http://cpanel.tatilcity.net             - /controlpanel
http://www.tatilcity.net:2082           - /controlpanel
http://www.tatilcity.net:2082/unprotected/loader.html?random=3Az5XYILmJ4AsSiw&goto_uri= - /
controlpanel
```

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

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

https://content.tatilcity.net           - /
https://cpanel.tatilcity.net            - /controlpanel
https://developers.google.com           - /
https://fonts.googleapis.com            - /

https://googletagmanager.com            - /
https://linkedin.com                    - /
https://maps.googleapis.com             - /
https://n8b8m5z7.stackpathcdn.com       - /
https://plus.google.com                 - /
https://plus.google.com/100657171534058931456 - /
https://tatilcitynet.tumblr.com/        - /
https://tr.pinterest.com/tatilcity/     - /
https://twitter.com                     - /
https://twitter.com/tatilcitynet        - /
https://ucuzauc.com                     - /
https://www.alobando.com/               - /vize-islemleri/italya-vizesi/
https://www.anadolujet.com/             - /ucak-bileti/anadolujet/
https://www.atlasglb.com/               - /ucak-bileti/atlasglobal/
https://www.cssscript.com/demo/animated-customizable-range-slider-pure-javascript-rslider-js/css/
rSlider.min.css - /ucak-bileti/
https://www.facebook.com/tatilcitynet/  - /
https://www.flypgs.com/                 - /ucak-bileti/pegasus/
https://www.google.com/maps/embed?pb=!1m18!1m12!1m3!1d100637.77864527276!2d32.49048312830489!
3d37.97874929444639!2m3!1f0!2f0!3f0!3m2!1i1024!2i768!4f13.1!3m3!1m2!1s0x14d09253eb2debcd
%3A0xd92f69841acfb35f!2sKonya+Havaliman%C4%B1!5e0!3m2!1str!2str!4v1538494187273 - /hava-limanlari/
konya-havalimani/
```

```
https://www.google.com/maps/embed?pb=!1m18!1m12!1m3!1d12045.648060812535!2d39.78071089297533!
3d40.99435437794819!2m3!1f0!2f0!3f0!3m2!1i1024!2i768!4f13.1!3m3!1m2!1s0x40643b9d271b08fb
%3A0x7df292f5eedabe39!2sDhmi+Trabzon+Uluslararas%C4%B1+Havaliman%C4%B1!5e0!3m2!1str!2str!
4v1538568170006 - /ucak-bileti/trabzon-havalimani/
https://www.google.com/maps/embed?pb=!1m18!1m12!1m3!1d12061.89248311013!
2d29.30810555565337!3d40.905371082741766!2m3!1f0!2f0!3f0!3m2!1i1024!2i768!4f13.1!3m3!1m2!
1s0x14cadbcbf424a153%3A0xacefca4d8098d [...]
```

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). 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: 2015/07/02

Plugin Output

tcp/443

```

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

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). 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: 2015/07/02

Plugin Output

tcp/2078

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

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). 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: 2015/07/02

Plugin Output

tcp/2080

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

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). 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: 2015/07/02

Plugin Output

tcp/2083

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

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). 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: 2015/07/02

Plugin Output

tcp/2087

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

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). 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: 2015/07/02

Plugin Output

tcp/2096

```

  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: 2019/03/19

Plugin Output

tcp/80

```
Based on the response to an OPTIONS request :
  - HTTP methods GET HEAD OPTIONS POST are allowed on :

    /css
    /form
    /pipermail


Based on tests of each method :

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

    /
    /controlpanel
    /css
    /form
    /pipermail

  - Invalid/unknown HTTP methods are allowed on :

    /
    /controlpanel
    /css
    /form
    /pipermail
```

43111 - HTTP Methods Allowed (per directory)

Synopsis

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

Description

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

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

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

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

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

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

See Also

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

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/443

```

Based on tests of each method :
```

```
- HTTP methods ACL BASELINE-CONTROL BCOPY BDELETE BMOVE BPROPFIND
  BPROPPATCH CHECKIN CHECKOUT are allowed on :

  /accommodation/page
  /accommodation/page/2
  /arac

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

  /
  /accommodation
  /accommodation/feed

- Invalid/unknown HTTP methods are allowed on :

  /
  /accommodation
  /accommodation/feed
```

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

Plugin Information

Published: 2000/01/04, Modified: 2019/04/26

Plugin Output

tcp/80

```
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

Plugin Information

Published: 2000/01/04, Modified: 2019/04/26

Plugin Output

tcp/443

```
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

Plugin Information

Published: 2000/01/04, Modified: 2019/04/26

Plugin Output

tcp/2078

```
The remote web server type is :

cPanel
```

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

Plugin Information

Published: 2000/01/04, Modified: 2019/04/26

Plugin Output

tcp/2080

```
The remote web server type is :

cPanel
```

85805 - HTTP/2 Cleartext Detection

Synopsis

An HTTP/2 server is listening on the remote host.

Description

The remote host is running an HTTP server that supports HTTP/2 running over cleartext TCP (h2c).

See Also

https://http2.github.io/

https://tools.ietf.org/html/rfc7540

https://github.com/http2/http2-spec

Solution

Limit incoming traffic to this port if desired.

Risk Factor

None

Plugin Information

Published: 2015/09/04, Modified: 2019/05/06

Plugin Output

tcp/80

```
The server supports direct HTTP/2 connections
without encryption.
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2017/11/13

Plugin Output

tcp/80

```

Response Code : HTTP/1.1 301 Moved Permanently

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

  Date: Tue, 28 May 2019 19:08:04 GMT
  Server: Apache
  Expires: Thu, 19 Nov 1981 08:52:00 GMT
  Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
  Pragma: no-cache
  Upgrade: h2,h2c
  Connection: Upgrade, Keep-Alive
  Location: https://www.tatilcity.net/
  Vary: User-Agent,Accept-Encoding
  Content-Length: 0
  Keep-Alive: timeout=15, max=100
  Content-Type: text/html; charset=UTF-8

Response Body :

```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2017/11/13

Plugin Output

tcp/443

```

Response Code : HTTP/1.1 200 OK

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

  Date: Tue, 28 May 2019 19:08:06 GMT
  Server: Apache
  Upgrade: h2,h2c
  Connection: Upgrade, close
  Last-Modified: Tue, 28 May 2019 19:07:45 GMT
  Cache-Control: max-age=0
  Expires: Tue, 28 May 2019 19:08:06 GMT
  Vary: Accept-Encoding,User-Agent
  Transfer-Encoding: chunked
  Content-Type: text/html; charset=UTF-8

Response Body :

<!DOCTYPE html> <!--[if IE 7 ]><html class="ie7 oldie" lang="tr-TR" prefix="og: http://ogp.me/
ns#"> <![endif]--> <!--[if IE 8 ]><html class="ie8 oldie" lang="tr-TR" prefix="og: http://
ogp.me/ns#"> <![endif]--> <!--[if IE   ]><html class="ie" lang="tr-TR" prefix="og: http://ogp.me/
ns#"> <![endif]--> <!--[if lt IE 9]><script src="https://html5shim.googlecode.com/svn/trunk/
html5.js"></script><![endif]--><html lang="tr-TR" prefix="og: http://ogp.me/ns#"><head><title>Ucuz
 U..ak Bileti - Otel Rezervasyonu - Tur paketleri - TatilCity.NET</title><link rel="stylesheet"
 href="https://www.tatilcity.net/wp-content/cache/min/1/e18d23dbb00d1a6245c4b8b1175be86e.css" data-
minify="1" /><meta http-equiv="X-UA-Compatible" content="IE=Edge"/><meta charset="UTF-8"><meta
 name="viewport" content="width=device-width, initial-scale=1.0"><meta name="yandex-verification"
 content="1a83c5778007e9ee" /><link rel="shortcut icon" href="https://www.tatilcity.net/wp-
content/uploads/2018/11/favicon.ico" type="image/x-icon" /> <!--[if lt IE 9]> <script type='text/
javascript' src="https://html5shiv.googlecode.com/svn/trunk/html5.js"></script> <script type='text/
javascript' src="https://cdnjs.cloudflare.com/ajax/libs/respond.js/1.4.2/respond.js"></script>
 <![endif]--><meta name="description" content="Ucuz tatil planlar, ucuz u..ak bileti buluruz. En
 uygun otel rezervasyonu ile tur paketleri fiyatlar.., vize i..lemleri Tatil City&#039;de."/><link
 rel="canonical" href="https://www.tatilcity.net/" /><meta property="og:locale" content="tr_TR" /
><meta property="og:type" content="website" [...]
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2017/11/13

Plugin Output

tcp/2078

```
Response Code : HTTP/1.1 401 Unauthorized

Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : yes
Options allowed : OPTIONS, PROPFIND, GET, COPY, MKCOL, LOCK, PROPPATCH, DELETE, MOVE, PUT, UNLOCK,
 HEAD, POST
Headers :

  Date: Tue, 28 May 2019 19:08:07 GMT
  Server: cPanel
  Persistent-Auth: false
  Host: www.tatilcity.net:2078
  Cache-Control: no-cache, no-store, must-revalidate, private
  Connection: Keep-Alive
  Vary: Accept-Encoding
  WWW-Authenticate: Basic realm="Restricted Area"
  Content-Length: 35
  Content-Type: text/html; charset="utf-8"
  Expires: Fri, 01 Jan 1990 00:00:00 GMT

Response Body :

<html>Authorization Required</html>
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2017/11/13

Plugin Output

tcp/2080

```

Response Code : HTTP/1.1 401 Unauthorized

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

  Date: Tue, 28 May 2019 19:08:07 GMT
  Server: cPanel
  Persistent-Auth: false
  Host: www.tatilcity.net:2080
  Cache-Control: no-cache, no-store, must-revalidate, private
  Connection: Keep-Alive
  Vary: Accept-Encoding
  WWW-Authenticate: Basic realm="Restricted Area"
  Content-Length: 35
  Content-Type: text/html; charset="utf-8"
  Expires: Fri, 01 Jan 1990 00:00:00 GMT

Response Body :

<html>Authorization Required</html>
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2017/11/13

Plugin Output

tcp/2083

```

Response Code : HTTP/1.1 401 Access Denied

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

  Connection: close
  Content-Type: text/html; charset="utf-8"
  Date: Tue, 28 May 2019 19:08:08 GMT
  Cache-Control: no-cache, no-store, must-revalidate, private
  Pragma: no-cache
  Set-Cookie: cprelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083;
 secure
  Set-Cookie: cpsession=%3atH7efuaDi6u_9AeP%2c7430271d22e74cf9fda41ebf0d693dd0; HttpOnly; path=/;
 port=2083; secure
  Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/;
 port=2083; secure
  Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=www.tatilcity.net; expires=Thu, 01-
Jan-1970 00:00:01 GMT; path=/; port=2083; secure
  Set-Cookie: Horde=expired; HttpOnly; domain=.www.tatilcity.net; expires=Thu, 01-Jan-1970 00:00:01
 GMT; path=/; port=2083; secure
  Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.www.tatilcity.net; expires=Thu, 01-
Jan-1970 00:00:01 GMT; path=/; port=2083; secure
  Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083;
 secure
```

```
  Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/horde;
 port=2083; secure
  Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083;
 secure
  Set-Cookie: imp_key=expired; HttpOnly; domain=www.tatilcity.net; expires=Thu, 01-Jan-1970 00:00:01
 GMT; path=/; port=2083; secure
  Set-Cookie: Horde=expired; HttpOnly; domain=.www.tatilcity.net; expires=Thu, 01-Jan-1970 00:00:01
 GMT; path=/; port=2083
  Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.www.tatilcity.net; expires=Thu, 01-
Jan-1970 00:00:01 GMT; path=/; port=2083
  Cache-Control: no-cache, no-store, must-revalidate, private
  Content-Length: 36359

Response Body :


<!DOCTYPE html>
<html lang="en" dir="ltr">
<head>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
    <meta name="viewport" conten [...]
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2017/11/13

Plugin Output

tcp/2087

```

Response Code : HTTP/1.1 401 Access Denied

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

  Connection: close
  Content-Type: text/html; charset="utf-8"
  Date: Tue, 28 May 2019 19:08:09 GMT
  Cache-Control: no-cache, no-store, must-revalidate, private
  Pragma: no-cache
  Set-Cookie: whostmgrrelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/;
 port=2087; secure
  Set-Cookie: whostmgrsession=%3an5zZQyAO3GEFCySF%2ce330b5fbf409da2846dfd03ddc7a681e; HttpOnly;
 path=/; port=2087; secure
  Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/;
 port=2087; secure
  Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=www.tatilcity.net; expires=Thu, 01-
Jan-1970 00:00:01 GMT; path=/; port=2087; secure
  Set-Cookie: Horde=expired; HttpOnly; domain=.www.tatilcity.net; expires=Thu, 01-Jan-1970 00:00:01
 GMT; path=/; port=2087; secure
  Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.www.tatilcity.net; expires=Thu, 01-
Jan-1970 00:00:01 GMT; path=/; port=2087; secure
  Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087;
 secure
```

```
  Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/horde;
 port=2087; secure
  Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087;
 secure
  Set-Cookie: imp_key=expired; HttpOnly; domain=www.tatilcity.net; expires=Thu, 01-Jan-1970 00:00:01
 GMT; path=/; port=2087; secure
  Set-Cookie: Horde=expired; HttpOnly; domain=.www.tatilcity.net; expires=Thu, 01-Jan-1970 00:00:01
 GMT; path=/; port=2087
  Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.www.tatilcity.net; expires=Thu, 01-
Jan-1970 00:00:01 GMT; path=/; port=2087
  Cache-Control: no-cache, no-store, must-revalidate, private
  Content-Length: 36354

Response Body :


<!DOCTYPE html>
<html lang="en" dir="ltr">
<head>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
    <meta name="view [...]
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2017/11/13

Plugin Output

tcp/2096

```

Response Code : HTTP/1.1 401 Access Denied

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

  Connection: close
  Content-Type: text/html; charset="utf-8"
  Date: Tue, 28 May 2019 19:08:10 GMT
  Cache-Control: no-cache, no-store, must-revalidate, private
  Pragma: no-cache
  Set-Cookie: webmailrelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2096;
 secure
  Set-Cookie: webmailsession=%3avrVqGMV1zHomJeRb%2ccc75edc802b15c726fc338b10b93853a; HttpOnly;
 path=/; port=2096; secure
  Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/;
 port=2096; secure
  Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=www.tatilcity.net; expires=Thu, 01-
Jan-1970 00:00:01 GMT; path=/; port=2096; secure
  Set-Cookie: Horde=expired; HttpOnly; domain=.www.tatilcity.net; expires=Thu, 01-Jan-1970 00:00:01
 GMT; path=/; port=2096; secure
  Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.www.tatilcity.net; expires=Thu, 01-
Jan-1970 00:00:01 GMT; path=/; port=2096; secure
  Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2096;
 secure
```

```
  Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/horde;
 port=2096; secure
  Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2096;
 secure
  Set-Cookie: imp_key=expired; HttpOnly; domain=www.tatilcity.net; expires=Thu, 01-Jan-1970 00:00:01
 GMT; path=/; port=2096; secure
  Set-Cookie: Horde=expired; HttpOnly; domain=.www.tatilcity.net; expires=Thu, 01-Jan-1970 00:00:01
 GMT; path=/; port=2096
  Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.www.tatilcity.net; expires=Thu, 01-
Jan-1970 00:00:01 GMT; path=/; port=2096
  Set-Cookie: roundcube_cookies=enabled; HttpOnly; expires=Wed, 27-May-2020 19:08:10 GMT; path=/;
 port=2096; secure
  Cache-Control: no-cache, no-store, must-revalidate, private
  Content-Length: 36371

Response Body :


<!DOCTYPE html>
<html lang="en [...]
```

91634 - HyperText Transfer Protocol (HTTP) Redirect Information

Synopsis

The remote web server redirects requests to the root directory.

Description

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

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/80

```

  Request         : http://www.tatilcity.net/
  HTTP response   : HTTP/1.1 301 Moved Permanently
  Redirect to     : https://www.tatilcity.net/
  Redirect type   : 30x redirect


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

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: 2018/11/15

Plugin Output

tcp/80

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

  - http://www.tatilcity.net/controlpanel
  - http://www.tatilcity.net/css/
  - http://www.tatilcity.net/form/
  - http://www.tatilcity.net/pipermail/
```

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: 2018/11/15

Plugin Output

tcp/443

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

  - https://www.tatilcity.net/
  - https://www.tatilcity.net/accommodation
  - https://www.tatilcity.net/accommodation/
  - https://www.tatilcity.net/accommodation/page/2
  - https://www.tatilcity.net/accommodation/page/2/
  - https://www.tatilcity.net/arac-kiralama/fiat-egea
  - https://www.tatilcity.net/arac-kiralama/fiat-egea/
  - https://www.tatilcity.net/arac/alfa-romeo-mito
  - https://www.tatilcity.net/arac/alfa-romeo-mito/
  - https://www.tatilcity.net/arac/bmw-5-series
  - https://www.tatilcity.net/arac/bmw-5-series/
```

```
    - https://www.tatilcity.net/arac/bmw-mini
    - https://www.tatilcity.net/arac/bmw-mini/
    - https://www.tatilcity.net/arac/citroen-ds3
    - https://www.tatilcity.net/arac/citroen-ds3/
    - https://www.tatilcity.net/arac/fiat-500
    - https://www.tatilcity.net/arac/fiat-500/
    - https://www.tatilcity.net/arac/holden-sv6
    - https://www.tatilcity.net/arac/holden-sv6/
    - https://www.tatilcity.net/arac/renault-grand-scenic
    - https://www.tatilcity.net/arac/renault-grand-scenic/
    - https://www.tatilcity.net/arac/vokswagen-polo
    - https://www.tatilcity.net/arac/vokswagen-polo/
    - https://www.tatilcity.net/author/buse
    - https://www.tatilcity.net/author/buse/
    - https://www.tatilcity.net/car
    - https://www.tatilcity.net/car/
    - https://www.tatilcity.net/controlpanel
    - https://www.tatilcity.net/cruise
    - https://www.tatilcity.net/cruise/
    - https://www.tatilcity.net/css/
    - https://www.tatilcity.net/etiket/bursa
    - https://www.tatilcity.net/etiket/bursa/
    - https://www.tatilcity.net/etiket/istanbul
    - https://www.tatilcity.net/etiket/istanbul/
    - https://www.tatilcity.net/gezi-rehberi/antalya-gezi-rehberi
    - https://www.tatilcity.net/gezi-rehberi/antalya-gezi-rehberi/
    - https://www.tatilcity.net/gezi-rehberi/istanbul-gezi-rehberi
    - https://www.tatilcity.net/gezi-rehberi/istanbul-gezi-rehberi/
    - https://www.tatilcity.net/hava-limanlari/adana-sakirpasa-havalimani [...]
```

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: 2017/05/16

Plugin Output

tcp/80

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

  - http://www.tatilcity.net/controlpanel
  - http://www.tatilcity.net/css/
  - http://www.tatilcity.net/form/
  - http://www.tatilcity.net/pipermail/
```

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: 2017/05/16

Plugin Output

tcp/443

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

  - https://www.tatilcity.net/
  - https://www.tatilcity.net/accommodation
  - https://www.tatilcity.net/accommodation/
  - https://www.tatilcity.net/accommodation/page/2
  - https://www.tatilcity.net/accommodation/page/2/
  - https://www.tatilcity.net/arac-kiralama/fiat-egea
  - https://www.tatilcity.net/arac-kiralama/fiat-egea/
  - https://www.tatilcity.net/arac/alfa-romeo-mito
  - https://www.tatilcity.net/arac/alfa-romeo-mito/
  - https://www.tatilcity.net/arac/bmw-5-series
  - https://www.tatilcity.net/arac/bmw-5-series/
  - https://www.tatilcity.net/arac/bmw-mini
  - https://www.tatilcity.net/arac/bmw-mini/
  - https://www.tatilcity.net/arac/citroen-ds3
  - https://www.tatilcity.net/arac/citroen-ds3/
  - https://www.tatilcity.net/arac/fiat-500
```

```
    - https://www.tatilcity.net/arac/fiat-500/
    - https://www.tatilcity.net/arac/holden-sv6
    - https://www.tatilcity.net/arac/holden-sv6/
    - https://www.tatilcity.net/arac/renault-grand-scenic
    - https://www.tatilcity.net/arac/renault-grand-scenic/
    - https://www.tatilcity.net/arac/vokswagen-polo
    - https://www.tatilcity.net/arac/vokswagen-polo/
    - https://www.tatilcity.net/author/buse
    - https://www.tatilcity.net/author/buse/
    - https://www.tatilcity.net/car
    - https://www.tatilcity.net/car/
    - https://www.tatilcity.net/controlpanel
    - https://www.tatilcity.net/cruise
    - https://www.tatilcity.net/cruise/
    - https://www.tatilcity.net/css/
    - https://www.tatilcity.net/etiket/bursa
    - https://www.tatilcity.net/etiket/bursa/
    - https://www.tatilcity.net/etiket/istanbul
    - https://www.tatilcity.net/etiket/istanbul/
    - https://www.tatilcity.net/gezi-rehberi/antalya-gezi-rehberi
    - https://www.tatilcity.net/gezi-rehberi/antalya-gezi-rehberi/
    - https://www.tatilcity.net/gezi-rehberi/istanbul-gezi-rehberi
    - https://www.tatilcity.net/gezi-rehberi/istanbul-gezi-rehberi/
    - https://www.tatilcity.net/hava-limanlari/adana-sakirpasa-havalimani
    - https://www.tatilci [...]
```

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: 2019/03/06

Plugin Output

tcp/21

```
Port 21/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: 2019/03/06

Plugin Output

tcp/53

```
Port 53/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: 2019/03/06

Plugin Output

tcp/80

```
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: 2019/03/06

Plugin Output

tcp/110

```
Port 110/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: 2019/03/06

Plugin Output

tcp/111

```
Port 111/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: 2019/03/06

Plugin Output

tcp/143

```
Port 143/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: 2019/03/06

Plugin Output

tcp/443

```
Port 443/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: 2019/03/06

Plugin Output

tcp/465

```
Port 465/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: 2019/03/06

Plugin Output

tcp/587

```
Port 587/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: 2019/03/06

Plugin Output

tcp/993

```
Port 993/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: 2019/03/06

Plugin Output

tcp/995

```
Port 995/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: 2019/03/06

Plugin Output

tcp/2077

```
Port 2077/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: 2019/03/06

Plugin Output

tcp/2078

```
Port 2078/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: 2019/03/06

Plugin Output

tcp/2079

```
Port 2079/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: 2019/03/06

Plugin Output

tcp/2080

```
Port 2080/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: 2019/03/06

Plugin Output

tcp/2082

```
Port 2082/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: 2019/03/06

Plugin Output

tcp/2083

```
Port 2083/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: 2019/03/06

Plugin Output

tcp/2086

```
Port 2086/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: 2019/03/06

Plugin Output

tcp/2087

```
Port 2087/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: 2019/03/06

Plugin Output

tcp/2095

```
Port 2095/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: 2019/03/06

Plugin Output

tcp/2096

```
Port 2096/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: 2019/03/06

Plugin Output

tcp/2222

```
Port 2222/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: 2019/03/06

Plugin Output

tcp/3306

```
Port 3306/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.
- Whether credentialed or third-party patch management checks are possible.
- 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: 2019/03/06

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 8.4.0
Plugin feed version : 201905271142
Scanner edition used : Nessus Home
Scan type : Normal
Scan policy used : Web Application Tests
Scanner IP : 192.168.1.34
Port scanner(s) : nessus_syn_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
```

```
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
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
Scan Start Date : 2019/5/28 19:33
Scan duration : 85533 sec
```

40665 - Protected Web Page Detection

Synopsis

Some web pages require authentication.

Description

The remote web server requires HTTP authentication for the following pages. Several authentication schemes are available :

- Basic is the simplest, but the credentials are sent in cleartext.

- NTLM provides an SSO in a Microsoft environment, but it cannot be used on both the proxy and the web server. It is also weaker than Digest.

- Digest is a cryptographically strong scheme. Credentials are never sent in cleartext, although they may still be cracked by a dictionary attack.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/08/21, Modified: 2016/10/04

Plugin Output

tcp/2078

```
The following pages are protected by the Basic authentication scheme :

/
```

40665 - Protected Web Page Detection

Synopsis

Some web pages require authentication.

Description

The remote web server requires HTTP authentication for the following pages. Several authentication schemes are available :

- Basic is the simplest, but the credentials are sent in cleartext.

- NTLM provides an SSO in a Microsoft environment, but it cannot be used on both the proxy and the web server. It is also weaker than Digest.

- Digest is a cryptographically strong scheme. Credentials are never sent in cleartext, although they may still be cracked by a dictionary attack.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/08/21, Modified: 2016/10/04

Plugin Output

tcp/2080

```

The following pages are protected by the Basic authentication scheme :

/

```

100669 - Web Application Cookies Are Expired

Synopsis

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

Description

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

See Also

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

Solution

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

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

Risk Factor

None

Plugin Information

Published: 2017/06/07, Modified: 2017/06/07

Plugin Output

tcp/80

```

The following cookies are expired :

Name : roundcube_sessauth
Path : /
Value : expired
Domain : www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : PPA_ID
Path : /
Value : expired
```

```
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : horde_secret_key
Path : /
Value : expired
Domain : .www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : imp_key
Path : /
Value : expired
Domain : www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : Horde
Path : /
Value : expired
Domain : .www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : cprelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : roundcube_sessid
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : whostmgrrelogin
```

```
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : webmailrelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : Horde
Path : /horde
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :
```

100669 - Web Application Cookies Are Expired

Synopsis

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

Description

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

See Also

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

Solution

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

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

Risk Factor

None

Plugin Information

Published: 2017/06/07, Modified: 2017/06/07

Plugin Output

tcp/443

```

The following cookies are expired :

Name : roundcube_sessauth
Path : /
Value : expired
Domain : www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : PPA_ID
Path : /
Value : expired
```

```
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : horde_secret_key
Path : /
Value : expired
Domain : .www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : imp_key
Path : /
Value : expired
Domain : www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : Horde
Path : /
Value : expired
Domain : .www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : cprelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : roundcube_sessid
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : whostmgrrelogin
```

```
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : webmailrelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : Horde
Path : /horde
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :
```

100669 - Web Application Cookies Are Expired

Synopsis

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

Description

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

See Also

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

Solution

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

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

Risk Factor

None

Plugin Information

Published: 2017/06/07, Modified: 2017/06/07

Plugin Output

tcp/2078

```

The following cookies are expired :

Name : roundcube_sessauth
Path : /
Value : expired
Domain : www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : PPA_ID
Path : /
Value : expired
```

```
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : horde_secret_key
Path : /
Value : expired
Domain : .www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : imp_key
Path : /
Value : expired
Domain : www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : Horde
Path : /
Value : expired
Domain : .www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : cprelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : roundcube_sessid
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : whostmgrrelogin
```

```
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : webmailrelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : Horde
Path : /horde
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :
```

100669 - Web Application Cookies Are Expired

Synopsis

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

Description

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

See Also

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

Solution

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

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

Risk Factor

None

Plugin Information

Published: 2017/06/07, Modified: 2017/06/07

Plugin Output

tcp/2080

```

The following cookies are expired :

Name : roundcube_sessauth
Path : /
Value : expired
Domain : www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : PPA_ID
Path : /
Value : expired
```

```
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : horde_secret_key
Path : /
Value : expired
Domain : .www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : imp_key
Path : /
Value : expired
Domain : www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : Horde
Path : /
Value : expired
Domain : .www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : cprelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : roundcube_sessid
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : whostmgrrelogin
```

```
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : webmailrelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : Horde
Path : /horde
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :
```

100669 - Web Application Cookies Are Expired

Synopsis

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

Description

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

See Also

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

Solution

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

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

Risk Factor

None

Plugin Information

Published: 2017/06/07, Modified: 2017/06/07

Plugin Output

tcp/2083

```
The following cookies are expired :

Name : roundcube_sessauth
Path : /
Value : expired
Domain : www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : PPA_ID
Path : /
Value : expired
```

```
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : horde_secret_key
Path : /
Value : expired
Domain : .www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : imp_key
Path : /
Value : expired
Domain : www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : Horde
Path : /
Value : expired
Domain : .www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : cprelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : roundcube_sessid
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : whostmgrrelogin
```

```
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : webmailrelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : Horde
Path : /horde
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :
```

100669 - Web Application Cookies Are Expired

Synopsis

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

Description

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

See Also

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

Solution

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

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

Risk Factor

None

Plugin Information

Published: 2017/06/07, Modified: 2017/06/07

Plugin Output

tcp/2087

```
The following cookies are expired :

Name : roundcube_sessauth
Path : /
Value : expired
Domain : www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : PPA_ID
Path : /
Value : expired
```

```
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : horde_secret_key
Path : /
Value : expired
Domain : .www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : imp_key
Path : /
Value : expired
Domain : www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : Horde
Path : /
Value : expired
Domain : .www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : cprelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : roundcube_sessid
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : whostmgrrelogin
```

```
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : webmailrelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : Horde
Path : /horde
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :
```

100669 - Web Application Cookies Are Expired

Synopsis

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

Description

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

See Also

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

Solution

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

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

Risk Factor

None

Plugin Information

Published: 2017/06/07, Modified: 2017/06/07

Plugin Output

tcp/2096

```

The following cookies are expired :

Name : roundcube_sessauth
Path : /
Value : expired
Domain : www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : PPA_ID
Path : /
Value : expired
```

```
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : horde_secret_key
Path : /
Value : expired
Domain : .www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : imp_key
Path : /
Value : expired
Domain : www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : Horde
Path : /
Value : expired
Domain : .www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : cprelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : roundcube_sessid
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : whostmgrrelogin
```

```
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : webmailrelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : Horde
Path : /horde
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :
```

85601 - Web Application Cookies Not Marked HttpOnly

Synopsis

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

Description

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

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

See Also

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

Solution

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

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

Risk Factor

None

References

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

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

Plugin Information

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

Plugin Output

tcp/80

```
The following cookies do not set the HttpOnly cookie flag :

Name : PHPSESSID
Path : /
Value : lm1ntkhjqclkeni40ho1g4mmn7
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


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


Name : port
Path : /
Value : 2096
Domain :
Version : 1
Expires :
Comment :
Secure : 1
Httponly : 0
Port :
```

85601 - Web Application Cookies Not Marked HttpOnly

Synopsis

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

Description

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

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

See Also

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

Solution

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

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

Risk Factor

None

References

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

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

Plugin Information

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

Plugin Output

tcp/443

```

The following cookies do not set the HttpOnly cookie flag :

Name : PHPSESSID
Path : /
Value : lm1ntkhjqclkeni40ho1g4mmn7
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


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


Name : port
Path : /
Value : 2096
Domain :
Version : 1
Expires :
Comment :
Secure : 1
Httponly : 0
Port :

```

85601 - Web Application Cookies Not Marked HttpOnly

Synopsis

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

Description

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

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

See Also

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

Solution

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

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

Risk Factor

None

References

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

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

Plugin Information

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

Plugin Output

tcp/2078

```
The following cookies do not set the HttpOnly cookie flag :

Name : PHPSESSID
Path : /
Value : lm1ntkhjqclkeni40ho1g4mmn7
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


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


Name : port
Path : /
Value : 2096
Domain :
Version : 1
Expires :
Comment :
Secure : 1
Httponly : 0
Port :
```

85601 - Web Application Cookies Not Marked HttpOnly

Synopsis

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

Description

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

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

See Also

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

Solution

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

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

Risk Factor

None

References

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

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

Plugin Information

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

Plugin Output

tcp/2080

```
The following cookies do not set the HttpOnly cookie flag :

Name : PHPSESSID
Path : /
Value : lm1ntkhjqclkeni40ho1g4mmn7
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


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


Name : port
Path : /
Value : 2096
Domain :
Version : 1
Expires :
Comment :
Secure : 1
Httponly : 0
Port :
```

85601 - Web Application Cookies Not Marked HttpOnly

Synopsis

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

Description

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

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

See Also

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

Solution

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

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

Risk Factor

None

References

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

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

Plugin Information

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

Plugin Output

tcp/2083

```

The following cookies do not set the HttpOnly cookie flag :

Name : PHPSESSID
Path : /
Value : lm1ntkhjqclkeni40ho1g4mmn7
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


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


Name : port
Path : /
Value : 2096
Domain :
Version : 1
Expires :
Comment :
Secure : 1
Httponly : 0
Port :
```

85601 - Web Application Cookies Not Marked HttpOnly

Synopsis

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

Description

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

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

See Also

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

Solution

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

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

Risk Factor

None

References

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

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

Plugin Information

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

Plugin Output

tcp/2087

```

The following cookies do not set the HttpOnly cookie flag :

Name : PHPSESSID
Path : /
Value : lm1ntkhjqclkeni40ho1g4mmn7
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


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


Name : port
Path : /
Value : 2096
Domain :
Version : 1
Expires :
Comment :
Secure : 1
Httponly : 0
Port :

```

85601 - Web Application Cookies Not Marked HttpOnly

Synopsis

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

Description

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

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

See Also

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

Solution

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

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

Risk Factor

None

References

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

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

Plugin Information

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

Plugin Output

tcp/2096

```

The following cookies do not set the HttpOnly cookie flag :

Name : PHPSESSID
Path : /
Value : lm1ntkhjqclkeni40ho1g4mmn7
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


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


Name : port
Path : /
Value : 2096
Domain :
Version : 1
Expires :
Comment :
Secure : 1
Httponly : 0
Port :
```

85602 - Web Application Cookies Not Marked Secure

Synopsis

HTTP session cookies might be transmitted in cleartext.

Description

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

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

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

See Also

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

Solution

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

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

Risk Factor

None

References

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

Plugin Information

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

Plugin Output

tcp/80

```
The following cookies do not set the secure cookie flag :

Name : roundcube_sessauth
Path : /
Value : expired
Domain : www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : PPA_ID
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : horde_secret_key
Path : /
Value : expired
Domain : .www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : imp_key
Path : /
Value : expired
Domain : www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : Horde
Path : /
Value : expired
Domain : .www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : PHPSESSID
Path : /
Value : lm1ntkhjqclkeni40ho1g4mmn7
Domain :
Version : 1
Expires :
```

```
Comment :
Secure : 0
Httponly : 0
Port :


Name : whostmgrsession
Path : /
Value : %3awwfGpdX_7wTFaso3%2cfcc6c21641ef9c31f1012a63c7a52d90
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 1
Port :


Name : cprelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : cpsession
Path : /
Value : %3agURl00PyKPhBOIBa%2c0f31af60eb9a8dafb0bd295f8624ee3f
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 1
Port :


Name : roundcube_sessid
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : roundcube_cookies
Path : /
Value : enabled
Domain :
Version : 1
Expires : Wed, 27-May-2020 17:35:14 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : whostmgrrelogin
Path : /
Value : no
Domain :
```

```
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : webmailrelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01 [...]
```

85602 - Web Application Cookies Not Marked Secure

Synopsis

HTTP session cookies might be transmitted in cleartext.

Description

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

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

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

See Also

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

Solution

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

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

Risk Factor

None

References

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

Plugin Information

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

Plugin Output

tcp/443

```
The following cookies do not set the secure cookie flag :

Name : roundcube_sessauth
Path : /
Value : expired
Domain : www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : PPA_ID
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : horde_secret_key
Path : /
Value : expired
Domain : .www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : imp_key
Path : /
Value : expired
Domain : www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : Horde
Path : /
Value : expired
Domain : .www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : PHPSESSID
Path : /
Value : lm1ntkhjqclkeni40ho1g4mmn7
Domain :
Version : 1
Expires :
```

```
Comment :
Secure : 0
Httponly : 0
Port :


Name : whostmgrsession
Path : /
Value : %3awwfGpdX_7wTFaso3%2cfcc6c21641ef9c31f1012a63c7a52d90
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 1
Port :


Name : cprelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : cpsession
Path : /
Value : %3agURl00PyKPhBOIBa%2c0f31af60eb9a8dafb0bd295f8624ee3f
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 1
Port :


Name : roundcube_sessid
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : roundcube_cookies
Path : /
Value : enabled
Domain :
Version : 1
Expires : Wed, 27-May-2020 17:35:14 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : whostmgrrelogin
Path : /
Value : no
Domain :
```

```
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : webmailrelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01 [...]
```

85602 - Web Application Cookies Not Marked Secure

Synopsis

HTTP session cookies might be transmitted in cleartext.

Description

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

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

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

See Also

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

Solution

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

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

Risk Factor

None

References

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

Plugin Information

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

Plugin Output

tcp/2078

```
The following cookies do not set the secure cookie flag :

Name : roundcube_sessauth
Path : /
Value : expired
Domain : www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : PPA_ID
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : horde_secret_key
Path : /
Value : expired
Domain : .www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : imp_key
Path : /
Value : expired
Domain : www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : Horde
Path : /
Value : expired
Domain : .www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : PHPSESSID
Path : /
Value : lm1ntkhjqclkeni40ho1g4mmn7
Domain :
Version : 1
Expires :
```

```
Comment :
Secure : 0
Httponly : 0
Port :


Name : whostmgrsession
Path : /
Value : %3awwfGpdX_7wTFaso3%2cfcc6c21641ef9c31f1012a63c7a52d90
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 1
Port :


Name : cprelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : cpsession
Path : /
Value : %3agURl00PyKPhBOIBa%2c0f31af60eb9a8dafb0bd295f8624ee3f
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 1
Port :


Name : roundcube_sessid
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : roundcube_cookies
Path : /
Value : enabled
Domain :
Version : 1
Expires : Wed, 27-May-2020 17:35:14 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : whostmgrrelogin
Path : /
Value : no
Domain :
```

```
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : webmailrelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01 [...]
```

85602 - Web Application Cookies Not Marked Secure

Synopsis

HTTP session cookies might be transmitted in cleartext.

Description

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

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

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

See Also

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

Solution

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

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

Risk Factor

None

References

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

Plugin Information

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

Plugin Output

tcp/2080

```
The following cookies do not set the secure cookie flag :

Name : roundcube_sessauth
Path : /
Value : expired
Domain : www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : PPA_ID
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : horde_secret_key
Path : /
Value : expired
Domain : .www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : imp_key
Path : /
Value : expired
Domain : www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : Horde
Path : /
Value : expired
Domain : .www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : PHPSESSID
Path : /
Value : lm1ntkhjqclkeni40ho1g4mmn7
Domain :
Version : 1
Expires :
```

```
Comment :
Secure : 0
Httponly : 0
Port :


Name : whostmgrsession
Path : /
Value : %3awwfGpdX_7wTFaso3%2cfcc6c21641ef9c31f1012a63c7a52d90
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 1
Port :


Name : cprelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : cpsession
Path : /
Value : %3agURl00PyKPhBOIBa%2c0f31af60eb9a8dafb0bd295f8624ee3f
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 1
Port :


Name : roundcube_sessid
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : roundcube_cookies
Path : /
Value : enabled
Domain :
Version : 1
Expires : Wed, 27-May-2020 17:35:14 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : whostmgrrelogin
Path : /
Value : no
Domain :
```

```
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : webmailrelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01 [...]
```

85602 - Web Application Cookies Not Marked Secure

Synopsis

HTTP session cookies might be transmitted in cleartext.

Description

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

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

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

See Also

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

Solution

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

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

Risk Factor

None

References

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

Plugin Information

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

Plugin Output

tcp/2083

```
The following cookies do not set the secure cookie flag :

Name : roundcube_sessauth
Path : /
Value : expired
Domain : www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : PPA_ID
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : horde_secret_key
Path : /
Value : expired
Domain : .www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : imp_key
Path : /
Value : expired
Domain : www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : Horde
Path : /
Value : expired
Domain : .www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : PHPSESSID
Path : /
Value : lm1ntkhjqclkeni40ho1g4mmn7
Domain :
Version : 1
Expires :
```

```
Comment :
Secure : 0
Httponly : 0
Port :


Name : whostmgrsession
Path : /
Value : %3awwfGpdX_7wTFaso3%2cfcc6c21641ef9c31f1012a63c7a52d90
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 1
Port :


Name : cprelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : cpsession
Path : /
Value : %3agURl00PyKPhBOIBa%2c0f31af60eb9a8dafb0bd295f8624ee3f
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 1
Port :


Name : roundcube_sessid
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : roundcube_cookies
Path : /
Value : enabled
Domain :
Version : 1
Expires : Wed, 27-May-2020 17:35:14 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : whostmgrrelogin
Path : /
Value : no
Domain :
```

```
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : webmailrelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01 [...]
```

85602 - Web Application Cookies Not Marked Secure

Synopsis

HTTP session cookies might be transmitted in cleartext.

Description

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

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

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

See Also

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

Solution

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

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

Risk Factor

None

References

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

Plugin Information

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

Plugin Output

tcp/2087

```
The following cookies do not set the secure cookie flag :

Name : roundcube_sessauth
Path : /
Value : expired
Domain : www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : PPA_ID
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : horde_secret_key
Path : /
Value : expired
Domain : .www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : imp_key
Path : /
Value : expired
Domain : www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : Horde
Path : /
Value : expired
Domain : .www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : PHPSESSID
Path : /
Value : lm1ntkhjqclkeni40ho1g4mmn7
Domain :
Version : 1
Expires :
```

```
Comment :
Secure : 0
Httponly : 0
Port :


Name : whostmgrsession
Path : /
Value : %3awwfGpdX_7wTFaso3%2cfcc6c21641ef9c31f1012a63c7a52d90
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 1
Port :


Name : cprelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : cpsession
Path : /
Value : %3agURl00PyKPhBOIBa%2c0f31af60eb9a8dafb0bd295f8624ee3f
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 1
Port :


Name : roundcube_sessid
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : roundcube_cookies
Path : /
Value : enabled
Domain :
Version : 1
Expires : Wed, 27-May-2020 17:35:14 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : whostmgrrelogin
Path : /
Value : no
Domain :
```

```
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : webmailrelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01 [...]
```

85602 - Web Application Cookies Not Marked Secure

Synopsis

HTTP session cookies might be transmitted in cleartext.

Description

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

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

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

See Also

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

Solution

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

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

Risk Factor

None

References

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

Plugin Information

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

Plugin Output

tcp/2096

```
The following cookies do not set the secure cookie flag :

Name : roundcube_sessauth
Path : /
Value : expired
Domain : www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : PPA_ID
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : horde_secret_key
Path : /
Value : expired
Domain : .www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : imp_key
Path : /
Value : expired
Domain : www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : Horde
Path : /
Value : expired
Domain : .www.tatilcity.net
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : PHPSESSID
Path : /
Value : lm1ntkhjqclkeni40ho1g4mmn7
Domain :
Version : 1
Expires :
```

```
Comment :
Secure : 0
Httponly : 0
Port :


Name : whostmgrsession
Path : /
Value : %3awwfGpdX_7wTFaso3%2cfcc6c21641ef9c31f1012a63c7a52d90
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 1
Port :


Name : cprelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : cpsession
Path : /
Value : %3agURl00PyKPhBOIBa%2c0f31af60eb9a8dafb0bd295f8624ee3f
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 1
Port :


Name : roundcube_sessid
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : roundcube_cookies
Path : /
Value : enabled
Domain :
Version : 1
Expires : Wed, 27-May-2020 17:35:14 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : whostmgrrelogin
Path : /
Value : no
Domain :
```

```
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : webmailrelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01 [...]
```

40773 - Web Application Potentially Sensitive CGI Parameter Detection

Synopsis

An application was found that may use CGI parameters to control sensitive information.

Description

According to their names, some CGI parameters may control sensitive data (e.g., ID, privileges, commands, prices, credit card data, etc.). In the course of using an application, these variables may disclose sensitive data or be prone to tampering that could result in privilege escalation. These parameters should be examined to determine what type of data is controlled and if it poses a security risk.

** This plugin only reports information that may be useful for auditors

** or pen-testers, not a real flaw.

Solution

Ensure sensitive data is not disclosed by CGI parameters. In addition, do not use CGI parameters to control access to resources or privileges.

Risk Factor

None

Plugin Information

Published: 2009/08/25, Modified: 2012/08/17

Plugin Output

tcp/443

```
Potentially sensitive parameters for CGI /wp-login.php :

pwd : Possibly a clear or hashed password, vulnerable to dictionary attack
```

91815 - Web Application Sitemap

Synopsis

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

Description

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/80

```

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

  - http://www.tatilcity.net/controlpanel
  - http://www.tatilcity.net/css/
  - http://www.tatilcity.net/css/colorbox.css
  - http://www.tatilcity.net/css/myStyles.css
  - http://www.tatilcity.net/css/testapicss.css
  - http://www.tatilcity.net/form/
  - http://www.tatilcity.net/form/form.css
  - http://www.tatilcity.net/form/jquery.css
  - http://www.tatilcity.net/form/ucak.js
  - http://www.tatilcity.net/pipermail/

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

```

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

  - https://www.tatilcity.net/
  - https://www.tatilcity.net/accommodation
  - https://www.tatilcity.net/accommodation/
  - https://www.tatilcity.net/accommodation/feed/
  - https://www.tatilcity.net/accommodation/page/2
  - https://www.tatilcity.net/accommodation/page/2/
  - https://www.tatilcity.net/arac-kiralama/fiat-egea
  - https://www.tatilcity.net/arac-kiralama/fiat-egea/
  - https://www.tatilcity.net/arac/alfa-romeo-mito
  - https://www.tatilcity.net/arac/alfa-romeo-mito/
  - https://www.tatilcity.net/arac/bmw-5-series
  - https://www.tatilcity.net/arac/bmw-5-series/
  - https://www.tatilcity.net/arac/bmw-mini
  - https://www.tatilcity.net/arac/bmw-mini/
  - https://www.tatilcity.net/arac/citroen-ds3
  - https://www.tatilcity.net/arac/citroen-ds3/
  - https://www.tatilcity.net/arac/fiat-500
  - https://www.tatilcity.net/arac/fiat-500/
  - https://www.tatilcity.net/arac/holden-sv6
  - https://www.tatilcity.net/arac/holden-sv6/
  - https://www.tatilcity.net/arac/renault-grand-scenic
  - https://www.tatilcity.net/arac/renault-grand-scenic/
```

```
    - https://www.tatilcity.net/arac/vokswagen-polo
    - https://www.tatilcity.net/arac/vokswagen-polo/
    - https://www.tatilcity.net/author/buse
    - https://www.tatilcity.net/author/buse/
    - https://www.tatilcity.net/car
    - https://www.tatilcity.net/car/
    - https://www.tatilcity.net/car/feed/
    - https://www.tatilcity.net/comments/feed/
    - https://www.tatilcity.net/controlpanel
    - https://www.tatilcity.net/cruise
    - https://www.tatilcity.net/cruise/
    - https://www.tatilcity.net/cruise/feed/
    - https://www.tatilcity.net/css/
    - https://www.tatilcity.net/etiket/bursa
    - https://www.tatilcity.net/etiket/bursa/
    - https://www.tatilcity.net/etiket/istanbul
    - https://www.tatilcity.net/etiket/istanbul/
    - https://www.tatilcity.net/feed/
    - https://www.tatilcity.net/gezi-rehberi/antalya-gezi-rehberi
    - https://www.tatilcity.net/gezi-rehberi/antalya-gezi-rehberi/
    - https://www.tat [...]
```

42057 - Web Server Allows Password Auto-Completion

Synopsis

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

Description

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

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

Solution

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

Risk Factor

None

Plugin Information

Published: 2009/10/07, Modified: 2016/06/16

Plugin Output

tcp/443

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

Page : /login
Destination Page: /wp-login.php

Page : /accommodation/
Destination Page: /wp-login.php

Page : /accommodation
Destination Page: /wp-login.php

Page : /ucak-bileti/
Destination Page: /wp-login.php

Page : /ucak-bileti
Destination Page: /wp-login.php

Page : /tour/
Destination Page: /wp-login.php

Page : /tour
Destination Page: /wp-login.php

Page : /cruise/
Destination Page: /wp-login.php
```

```
Page : /cruise
Destination Page: /wp-login.php

Page : /car/
Destination Page: /wp-login.php

Page : /car
Destination Page: /wp-login.php

Page : /vize-islemleri/
Destination Page: /wp-login.php

Page : /vize-islemleri
Destination Page: /wp-login.php

Page : /tatil-city-iletisim/
Destination Page: /wp-login.php

Page : /tatil-city-iletisim
Destination Page: /wp-login.php

Page : /ucak-bileti/bursa-istanbul-ucak-bileti-fiyatlari/
Destination Page: /wp-login.php

Page : /ucak-bileti/bursa-istanbul-ucak-bileti-fiyatlari
Destination Page: /wp-login.php

Page : /ucak-bileti/balikesir-erzurum-ucak-bileti-fiyatlari
Destination Page: /wp-login.php

Page : /ucak-bileti/istanbul-sanliurfa-ucak-bileti-fiyat/
Destination Page: /wp-login.php

Page : /ucak-bileti/istanbul-sanliurfa-ucak-bileti-fiyat
Destination Page: /wp-login.php

Page : /ucak-bileti/istanbul-mersin-ucak-bileti-fiyat/
Destination Page: /wp-login.php

Page : /ucak-bileti/istanbul-mersin-ucak-bileti-fiyat
Destination Page: /wp-login.php

Page : /ucak-bileti/balikesir-van-ucak-bileti-fiyatlari/
Destination Page: /wp-login.php

Page : /ucak-bileti/balikesir-van-ucak-bileti-fiyatlari
Destination Page: /wp-login.php

Page : /ucak-bileti/ucuz-giresun-sivas-ucak-bileti-fiyatlari/
Destination Page: /wp-login.php

Page : /ucak-bileti/ucuz-giresun-sivas-ucak-bileti-fiyatlari
Destination Page: /wp-login.php

Page : /ucak-bileti/adiyaman-kastamonu-ucak-bileti-fiyatlari/
Destination Page: /wp-login.php

Page : /ucak-bileti/adiyaman-kastamonu-ucak-bileti-fiyatlari
Destination Page: /wp-login.php

Page : /ucak-bileti/eskisehir-tokat-uc [...]
```

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: 2018/11/15

Plugin Output

tcp/80

```
The following directories were discovered:
/pipermail, /controlpanel, /css, /form

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: 2018/11/15

Plugin Output

tcp/443

```
The following directories were discovered:
/login, /pipermail, /controlpanel, /css

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

10386 - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/04/28, Modified: 2015/10/13

Plugin Output

tcp/80

```
CGI scanning will be disabled for this host because the host responds
to requests for non-existent URLs with HTTP code 301
rather than 404. The requested URL was :

    http://www.tatilcity.net/uuW_MlFYdJEK.html
```

10386 - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/04/28, Modified: 2015/10/13

Plugin Output

tcp/443

```
CGI scanning will be disabled for this host because the host responds
to requests for non-existent URLs with HTTP code 301
rather than 404. The requested URL was :

    https://www.tatilcity.net/uuW_MlFYdJEK.html
```

51080 - Web Server Uses Basic Authentication over HTTPS

Synopsis

The remote web server seems to transmit credentials using Basic Authentication.

Description

The remote web server contains web pages that are protected by 'Basic' authentication over HTTPS.

While this is not in itself a security flaw, in some organizations, the use of 'Basic' authentication is discouraged as, depending on the underlying implementation, it may be vulnerable to account brute-forcing or may encourage Man-in-The-Middle (MiTM) attacks.

Solution

Make sure that the use of HTTP 'Basic' authentication is in line with your organization's security policy.

Risk Factor

None

Plugin Information

Published: 2010/12/08, Modified: 2011/03/18

Plugin Output

tcp/2078

```

The following pages are protected :

/:/  realm="Restricted Area"
```

51080 - Web Server Uses Basic Authentication over HTTPS

Synopsis

The remote web server seems to transmit credentials using Basic Authentication.

Description

The remote web server contains web pages that are protected by 'Basic' authentication over HTTPS.

While this is not in itself a security flaw, in some organizations, the use of 'Basic' authentication is discouraged as, depending on the underlying implementation, it may be vulnerable to account brute-forcing or may encourage Man-in-The-Middle (MiTM) attacks.

Solution

Make sure that the use of HTTP 'Basic' authentication is in line with your organization's security policy.

Risk Factor

None

Plugin Information

Published: 2010/12/08, Modified: 2011/03/18

Plugin Output

tcp/2080

```
The following pages are protected :

/:/  realm="Restricted Area"
```

10302 - Web Server robots.txt Information Disclosure

Synopsis

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

Description

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

See Also

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/80

```
Contents of robots.txt :

User-agent: *
Disallow: /wp-admin/
Allow: /wp-admin/admin-ajax.php
Dissallow: /my-account
Dissallow: /coming-soon/
Dissallow: /destinations/
Dissallow: /destination/
Dissallow: /testimonials-category/
Dissallow: /tour-item/
Dissallow: /elements/
```

10302 - Web Server robots.txt Information Disclosure

Synopsis

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

Description

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

See Also

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/443

```
Contents of robots.txt :

User-agent: *
Disallow: /wp-admin/
Allow: /wp-admin/admin-ajax.php
Dissallow: /my-account
Dissallow: /coming-soon/
Dissallow: /destinations/
Dissallow: /destination/
Dissallow: /testimonials-category/
Dissallow: /tour-item/
Dissallow: /elements/
```

10302 - Web Server robots.txt Information Disclosure

Synopsis

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

Description

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

See Also

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2083

```
Contents of robots.txt :

User-agent: *
Disallow: /
```

10302 - Web Server robots.txt Information Disclosure

Synopsis

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

Description

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

See Also

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2087

```
Contents of robots.txt :

User-agent: *
Disallow: /
```

10302 - Web Server robots.txt Information Disclosure

Synopsis

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

Description

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

See Also

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2096

```
Contents of robots.txt :

User-agent: *
Disallow: /
```

10662 - Web mirroring

Synopsis

Nessus can crawl the remote website.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/05/04, Modified: 2019/03/18

Plugin Output

tcp/80

```
Webmirror performed 17 queries in 17s (1.000 queries per second)

The following CGIs have been discovered :

Directory index found at /css/
Directory index found at /form/
```

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: 2019/03/18

Plugin Output

tcp/443

```

Webmirror performed 437 queries in 1201s (0.0363 queries per second)

The following CGIs have been discovered :


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


+ CGI : /wp-login.php
  Methods : POST
  Argument : log
  Argument : pwd
  Argument : redirect_to
   Value: https://www.tatilcity.net/dashboard/
  Argument : rememberme
   Value: forever


+ CGI : /
  Methods : GET
  Argument : adults
   Value: 30
  Argument : car_types
   Value: 433
```

```
    Argument : cruise_lines
     Value: 917
    Argument : cruise_types
     Value: 916
    Argument : date_from
    Argument : date_to
    Argument : max_price
    Argument : order
     Value: ASC
    Argument : order_by
     Value: name
    Argument : p
     Value: 23216
    Argument : passengers
     Value: 10
    Argument : post_type
     Value: post
    Argument : rooms
     Value: 30
    Argument : s
    Argument : tour_types
     Value: 376
    Argument : view
     Value: list


  + CGI : /login/
    Methods : GET
    Argument : action
     Value: register
    Argument : pdf
     Value: 745


  + CGI : /accommodation/
    Methods : GET
    Argument : adults
     Value: 30
    Argument : child_ages[]
     Value: 0
    Argument : date_from
    Argument : date_to
    Argument : kids
     Value: 0
    Argument : order
     Value: DESC
    Argument : order_by
     Value: rating
    Argument : page
     Value: 12
    Argument : rooms
     Value: 30
    Argument : s
    Argument : view
     Value: block


  + CGI : /oteller/antalya/side/adalya-grand-art-side/
    Methods : GET,POST
    Argument :
     Value: date_to
    Argument : _wpnonce
     Value: 1cb4235ec9
    Argument : accommodation_id
     Value: 10689
    Argument : action
     Value: acc_submit_review
    Argument : adults
     Value: 30
    Argument : booking_no
```

```
   Argument : child_ages[]
    Value: 0
   Argument : date_from
   Argument : date_to
   Argument : kids
    Value: 0
   Argument : pin_code
   Argument : post_id
    Value: 10689
   Argument : review_rating
    Value: 0
   Argument : review_rating_detail[]
   Argument : review_text
   Argument : review_title
   Argument : rooms
    Value: 30
   Argument : trip_type
    Value: 0
  [...]
```

11424 - WebDAV Detection

Synopsis

The remote server is running with WebDAV enabled.

Description

WebDAV is an industry standard extension to the HTTP specification.
It adds a capability for authorized users to remotely add and manage the content of a web server.

If you do not use this extension, you should disable it.

Solution

http://support.microsoft.com/default.aspx?kbid=241520

Risk Factor

None

Plugin Information

Published: 2003/03/20, Modified: 2011/03/14

Plugin Output

tcp/2078

18297 - WordPress Detection

Synopsis

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

Description

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

See Also

https://wordpress.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/05/18, Modified: 2018/11/15

Plugin Output

tcp/443

```
URL     : https://www.tatilcity.net/
Version : 4.9.9
```