gbkh server

Report generated by Nessus™ Fri, 04 Oct 2019 19:14:27 GMT+0800

TABLE OF CONTENTS

Vulnerabilities by Plugin

Vulnerabilities by Plugin

42424 (1) - CGI Generic SQL Injection (blind)

Synopsis

A CGI application hosted on the remote web server is potentially prone to SQL injection attack.

Description

By sending specially crafted parameters to one or more CGI scripts hosted on the remote web server, Nessus was able to get a very different response, which suggests that it may have been able to modify the behavior of the application and directly access the underlying database.

An attacker may be able to exploit this issue to bypass authentication, read confidential data, modify the remote database, or even take control of the remote operating system.

Note that this script is experimental and may be prone to false positives.

See Also

http://www.securiteam.com/securityreviews/5DP0N1P76E.html

http://www.nessus.org/u?ed792cf5

http://projects.webappsec.org/w/page/13246963/SQL%20Injection

Solution

Modify the affected CGI scripts so that they properly escape arguments.

Risk Factor

High

CVSS Base Score

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

References

XREF	CWE:20
XREF	CWE:77
XREF	CWE:801
XREF	CWE:810
XREF	CWE:89
XREF	CWE:91
XREF	CWE:203
XREF	CWE:643
XREF	CWE:713
XREF	CWE:722

XREF	CWE:727
XREF	CWE:751
XREF	CWE:928
XREF	CWE:929

Plugin Information

Published: 2009/11/06, Modified: 2018/11/15

Plugin Output

192.168.1.112 (tcp/80)

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

+ The following resources may be vulnerable to blind SQL injection :

+ The 'Account' parameter of the /person/update_dept_user.php CGI :

/person/update_dept_user.php?city=&Account=916538+or+1=1

-------- output --------
    <label class="layui-form-label">............</label>
<div class="layui-input-inline">
    <input type="text" id="UserName" required lay-verify="required" valu
e="" autocomplete="off" class="layui-input">
</div>
  </div>
-------- vs --------
    <label class="layui-form-label">............</label>
<div class="layui-input-inline">
    <input type="text" id="UserName" required lay-verify="required" valu
e="........." autocomplete="off" class="layui-input">
</div>
  </div>
------------------------

/person/update_dept_user.php?city=&Account=916538+or+1=1 {2}

-------- output --------
    <label class="layui-form-label">............</label>
<div class="layui-input-inline">
    <input type="text" id="UserName" required lay-verify="required" valu
e="" autocomplete="off" class="layui-input">
</div>
  </div>
-------- vs --------
    <label class="layui-form-label">............</label>
<div class="layui-input-inline">
    <input type="text" id="UserName" required lay-verify="required" valu
e="........." autocomplete="off" class="layui-input">
</div>
  </div>
------------------------

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

http://192.168.1.112/person/update_dept_user.php?city=&Account=916538+or+1=1
```

33926 (1) - Adobe Dreamweaver dwsync.xml Remote Information Disclosure

Synopsis

The remote web server discloses the location of files and directories.

Description

Adobe's Dreamweaver is known to produce 'dwsync.xml' files. These contain synchronization information that may include the list of files and directories synchronised. This can lead to information disclosure.

Solution

Disable the 'Maintain synchronization information' option from the Remote Info category of the advanced view of the Site Definition dialog box. In addition, remove the offending files if already created by the system.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

5.0 (CVSS:3.0/E:F/RL:T/RC:X)

CVSS Base Score

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

CVSS Temporal Score

4.3 (CVSS2#E:F/RL:TF/RC:ND)

Plugin Information

Published: 2008/08/18, Modified: 2018/06/14

Plugin Output

192.168.1.112 (tcp/80)

```
\nThe following dwsync.xml files where discovered :\n\nhttp://192.168.1.112/include/_notes/
dwsync.xml:
\tconfig.php\nhttp://192.168.1.112/css/_notes/dwsync.xml:
\tLogin.css\n\tvotecss.css\n\tvote.css\n\tbootstrap.min.css\n\try-framwork.css\n\tbuy-list.css\n
\teasyui.css\n\timpowerApp3696b4.css\n\tpersonal-base.css\n\try-login.css\n\ttestcss.css\n\try-
center.css\n\tmodify-pwd.css\nhttp://192.168.1.112/images/_notes/dwsync.xml:
```

```
\thncj.png\n\tweixin_ewm_76.gif\n\tLogomin1103.png\n\tkxwzz.png\n\tcert.jpg\n
\t20180224020136347_23.jpg\n\tdui.jpg\n\t1.gif\n\tfavicon.ico\n\tqrcode.jpg\n\thead-student.png\n
\t1.jpg\n\t2.jpeg\n\t3.jpeg\n\t4.jpg\n\tbackground.jpg\n\timg_par.png\n\timg_stu.png\n\timg_tea.png
\n\tleft.jpg\n\tleft.png\n\tload.gif\n\ttimg1.png\n\ttop.jpg\n\ttop.png\n\ttop4.jpg\n\tyuan.jpg
\nhttp://192.168.1.112/lib/layui245/css/_notes/dwsync.xml:
\tlayui.css\n\tlayui.mobile.css\nhttp://192.168.1.112/lib/menu/css/_notes/dwsync.xml:
\tfont.css\n\tweadmin.css\n\tweadmin.less\nhttp://192.168.1.112/person/_notes/dwsync.xml:
\tadd_user.php\n\tupdate_dept_user.php\n\tdel_dept_user.php\n\tdept_user_data.php\n\tsave_user.php
\n\tupdate_user_data.php\n\tview.php\n\tview_user.php\nhttp://192.168.1.112/voteinformation/_notes/
dwsync.xml:
\tadmin_view.php\n\tview.php\nhttp://192.168.1.112/lib/layui245/_notes/dwsync.xml:
\tlayui.all.js\n\tlayui.js\nhttp://192.168.1.112/lib/layui230/css/_notes/dwsync.xml:
\tlayui.css\n\tlayui.mobile.css\nhttp://192.168.1.112/lib/layui230/_notes/dwsync.xml:
\tlayui.all.js\n\tlayui.js\nhttp://192.168.1.112/upload/_notes/dwsync.xml:
\t1.jpg\n\t2.jpeg\n\t4.jpg\n\tdui.jpg\n\thead-student.png\n\timg_par.png\n\timg_stu.png
\n\timg_tea.png\n\tload.gif\n\tqrcode.jpg\n\tThumbs.db\n\ttop2.jpg\n\tyuan.jpg\n
\t..................jpg\n\t.........png\n\t.........2.png\nhttp://192.168.1.112/pages/_notes/
dwsync.xml:
\twelcome.html\nhttp://192.168.1.112/lib/_notes/dwsync.xml:
\tjquery-3.2.1.js\n\tconfig.php\n\tcommon.js\n\tJSEncrypt.js\n\tLogin.js\n\tjquery.cookie.js\n
```

85582 (1) - 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

192.168.1.112 (tcp/80)

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

  - http://192.168.1.112/
  - http://192.168.1.112/index.php
  - http://192.168.1.112/person/add_user.php
  - http://192.168.1.112/person/update_dept_user.php
  - http://192.168.1.112/voteinformation/view.php
```

26194 (1) - Web Server Transmits Cleartext Credentials

Synopsis

The remote web server might transmit credentials in cleartext.

Description

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

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

Solution

Make sure that every sensitive form transmits content over HTTPS.

Risk Factor

Low

CVSS Base Score

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

References

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

Plugin Information

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

Plugin Output

192.168.1.112 (tcp/80)

```
Page : /
Destination Page: /

Page : /index.php
Destination Page: /index.php
```

11219 (2) - 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: 2019/08/20

Plugin Output

192.168.1.112 (tcp/22)

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

192.168.1.112 (tcp/80)

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

10107 (1) - 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: 2019/06/07

Plugin Output

192.168.1.112 (tcp/80)

```
The remote web server type is :

Apache/2.4.18 (Ubuntu)
```

10662 (1) - Web mirroring

Synopsis

Nessus can crawl the remote website.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/05/04, Modified: 2019/08/20

Plugin Output

192.168.1.112 (tcp/80)

```
Webmirror performed 59 queries in 1s (59.000 queries per second)

The following CGIs have been discovered :


+ CGI : /
  Methods :
  Argument : usertype
   Value: 2


+ CGI : /index.php
  Methods :
  Argument : usertype
   Value: 2


+ CGI : /person/update_dept_user.php
  Methods : GET
  Argument : Account
  Argument : city


+ CGI : /person/add_user.php
  Methods : POST
  Argument : account
  Argument : dept
```

```
    Argument : level
     Value: 6
    Argument : username
```

11032 (1) - 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

192.168.1.112 (tcp/80)

```
The following directories were discovered:
/include, /css, /icons, /images, /js, /lib, /pages, /upload

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
```

18261 (1) - Apache Banner Linux Distribution Disclosure

Synopsis

The name of the Linux distribution running on the remote host was found in the banner of the web server.

Description

Nessus was able to extract the banner of the Apache web server and determine which Linux distribution the remote host is running.

Solution

If you do not wish to display this information, edit 'httpd.conf' and set the directive 'ServerTokens Prod' and restart Apache.

n/a

Risk Factor

None

Plugin Information

Published: 2005/05/15, Modified: 2019/10/01

Plugin Output

192.168.1.112 (tcp/0)

```
The Linux distribution detected was :
 - Ubuntu 16.04 (xenial)
 - Ubuntu 16.10 (yakkety)
```

19506 (1) - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

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

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- 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

192.168.1.112 (tcp/0)

```
Information about this scan :

Nessus version : 8.7.1
Plugin feed version : 201910040120
Scanner edition used : Nessus Home
Scan type : Normal
Scan policy used : Web Application Tests
Scanner IP : 192.168.1.254
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Thorough tests : yes
Experimental tests : no
Paranoia level : 1
```

```
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : enabled
Web application tests : enabled
Web app tests -  Test mode : all_pairs
Web app tests -  Try all HTTP methods : yes
Web app tests -  Maximum run time : 10 minutes.
Web app tests -  Stop at first flaw : param
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : Detected
Allow post-scan editing: Yes
Scan Start Date : 2019/10/4 19:14
Scan duration : 1112 sec
```

24260 (1) - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive 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

192.168.1.112 (tcp/80)

```
Response Code : HTTP/1.1 200 OK

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

  Date: Fri, 04 Oct 2019 11:20:53 GMT
  Server: Apache/2.4.18 (Ubuntu)
  Cache-control: no-cache,no-store,must-revalidate
  Pragma: no-cache
  Expires: 0
  Vary: Accept-Encoding
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Transfer-Encoding: chunked
  Content-Type: text/html;charset=utf-8

Response Body :


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/
xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
```

```
<meta name="renderer" content="webkit">
<meta http-equiv="X-UA-Compatible" content="ie=edge,Chrome=1">
<meta http-equiv="pragma" content="no-cache">
<meta http-equiv="Cache-Control" content="no-cache, must-revalidate, no-store">
<meta http-equiv="expires" content="0">
<meta name="format-detection" content="telephone=no">
<title>.....</title>
<link rel="stylesheet" type="text/css" href="css/Login.css"/>
<script type="text/javascript" src="lib/common.js"></script>
<script type="text/javascript" src="lib/JSEncrypt.js"></script>
<script type="text/javascript" src="lib/jquery-3.2.1.js"></script>
<script type="text/javascript" src="lib/jquery.cookie.js"></script>
<script type="text/javascript" src="js/lib/aes.js"></script>
<link rel="stylesheet" type="text/css" href="lib/layui245/css/layui.css"/>
<script type="text/javascript" src="lib/layui245/layui.js"></script>
<style>
#code{
                font-family:Arial;
                font-style:italic;
                font-weight:bold;
                border:0;
                letter-spacing:2px;
                color:#0000fff;
            }
.a {
background-image:url(images/timg1.png);
background-size:100% 100%;
background-repeat:no-repeat;
}
</style>
</head>
<body class="layui-main" > [...]
```

33817 (1) - 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

192.168.1.112 (tcp/80)

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

arbitrary command execution (time based) : S=48         SP=114       AP=114       SC=156
 AC=156
format string                            : S=16         SP=38        AP=38        SC=52        AC=52

cross-site scripting (comprehensive test): S=136        SP=323       AP=323       SC=442
 AC=442
injectable parameter                     : S=16         SP=38        AP=38        SC=52        AC=52

arbitrary command execution              : S=176        SP=418       AP=418       SC=572
 AC=572
local file inclusion                     : S=32         SP=76        AP=76        SC=104
 AC=104
directory traversal                      : S=232        SP=551       AP=551       SC=754
 AC=754
web code injection                       : S=8          SP=19        AP=19        SC=26        AC=26

blind SQL injection (4 requests)         : S=32         SP=76        AP=76        SC=104
 AC=104
persistent XSS                           : S=32         SP=76        AP=76        SC=104
 AC=104
```

```
directory traversal (write access)       : S=16         SP=38        AP=38        SC=52        AC=52

XML injection                            : S=8          SP=19        AP=19        SC=26        AC=26

blind SQL injection                      : S=96         SP=228       AP=228       SC=312
 AC=312
SQL injection                            : S=224        SP=532       AP=532       SC=728
 AC=728
directory traversal (extended test)      : S=408        SP=969       AP=969       SC=1326
 AC=1326
SSI injection                            : S=24         SP=57        AP=57        SC=78        AC=78

unseen parameters                        : S=280        SP=665       AP=665       SC=910
 AC=910
SQL injection (2nd order)              [...]
```

42057 (1) - 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

192.168.1.112 (tcp/80)

```
Page : /
Destination Page: /

Page : /index.php
Destination Page: /index.php
```

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

Synopsis

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

Description

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

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

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

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

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

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

See Also

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

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

192.168.1.112 (tcp/80)

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

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

    /css
    /icons
    /images
    /include
    /js
    /lib
    /lib/layui230
    /lib/layui230/css
    /lib/layui245
    /lib/layui245/css
    /lib/menu
    /lib/menu/css
    /pages
    /person
    /upload
    /voteinformation


Based on tests of each method :

  - HTTP methods GET HEAD OPTIONS POST are allowed on :

    /
    /css
    /icons
    /images
    /include
    /js
    /lib
    /lib/layui230
    /lib/layui230/css
    /lib/layui245
    /lib/layui245/css
    /lib/menu
    /lib/menu/css
    /pages
    /person
    /upload
    /voteinformation
```

48204 (1) - Apache HTTP Server Version

Synopsis

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

Description

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

See Also

https://httpd.apache.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/07/30, Modified: 2019/06/04

Plugin Output

192.168.1.112 (tcp/80)

```
URL        : http://192.168.1.112/
Version    : 2.4.99
backported : 1
os         : ConvertedUbuntu
```

50344 (1) - 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

192.168.1.112 (tcp/80)

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

  - http://192.168.1.112/
  - http://192.168.1.112/AdminMenu.php
  - http://192.168.1.112/index.php
  - http://192.168.1.112/noteinfo.php
  - http://192.168.1.112/person/add_user.php
  - http://192.168.1.112/person/update_dept_user.php
  - http://192.168.1.112/person/view_user.php
  - http://192.168.1.112/voteinformation/view.php
```

```
- http://192.168.1.112/welcome.php
```

50345 (1) - Missing or Permissive X-Frame-Options HTTP Response Header

Synopsis

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

Description

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

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

See Also

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

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

Solution

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

Risk Factor

None

Plugin Information

Published: 2010/10/26, Modified: 2017/05/16

Plugin Output

192.168.1.112 (tcp/80)

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

  - http://192.168.1.112/
  - http://192.168.1.112/AdminMenu.php
  - http://192.168.1.112/index.php
  - http://192.168.1.112/noteinfo.php
  - http://192.168.1.112/person/add_user.php
  - http://192.168.1.112/person/update_dept_user.php
  - http://192.168.1.112/person/view_user.php
  - http://192.168.1.112/voteinformation/view.php
  - http://192.168.1.112/welcome.php
```

85601 (1) - 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

192.168.1.112 (tcp/80)

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

Name : PHPSESSID
Path : /
Value : rofm43fv1d25uhnr974uoscuc3
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :
```

85602 (1) - 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

192.168.1.112 (tcp/80)

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

Name : PHPSESSID
Path : /
Value : rofm43fv1d25uhnr974uoscuc3
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :
```

91815 (1) - 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

192.168.1.112 (tcp/80)

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

  - http://192.168.1.112/
  - http://192.168.1.112/AdminMenu.php
  - http://192.168.1.112/css/Login.css
  - http://192.168.1.112/css/bootstrap.min.css
  - http://192.168.1.112/css/ry-center.css
  - http://192.168.1.112/css/ry-framwork.css
  - http://192.168.1.112/images/favicon.ico
  - http://192.168.1.112/index.php
  - http://192.168.1.112/lib/layui230/css/layui.css
  - http://192.168.1.112/lib/layui245/css/layui.css
  - http://192.168.1.112/lib/menu/css/font.css
  - http://192.168.1.112/lib/menu/css/weadmin.css
  - http://192.168.1.112/noteinfo.php
  - http://192.168.1.112/person/add_user.php
  - http://192.168.1.112/person/update_dept_user.php
  - http://192.168.1.112/person/view_user.php
  - http://192.168.1.112/voteinformation/view.php
  - http://192.168.1.112/welcome.php

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

106658 (1) - JQuery Detection

Synopsis

The web server on the remote host uses JQuery.

Description

Nessus was able to detect JQuery on the remote host.

See Also

https://jquery.com/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/02/07, Modified: 2019/09/25

Plugin Output

192.168.1.112 (tcp/80)

```
URL     : http://192.168.1.112/lib/jquery-3.2.1.js
Version : 3.2.1
```