CS230 Site

Report generated by Nessus™ | Tue, 03 Nov 2020 17:37:59 EST

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

52.201.250.219

0	0	5	1	22
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Tue Nov 3 17:16:26 2020
End time:	Tue Nov 3 17:37:59 2020

Host Information

DNS Name:	ec2-52-201-250-219.compute-1.amazonaws.com
IP:	52.201.250.219
OS:	KYOCERA Printer

Vulnerabilities

10756 - Apple Mac OS X Find-By-Content .DS_Store Web Directory Listing

Synopsis

It is possible to get the list of files present in the remote directory.

Description

It is possible to read a '.DS_Store' file on the remote web server.

This file is created by MacOS X Finder; it is used to remember the icons position on the desktop, among other things, and contains the list of files and directories present in the remote directory.

Note that deleted files may still be present in this .DS_Store file.

See Also

https://support.apple.com/en-us/HT1629

https://helpx.adobe.com/dreamweaver/kb/remove-ds-store-files-mac.html

http://www.greci.cc/?p=10

Solution

- Configure your web server so as to prevent the download of .DS_Store files
- Mac OS X users should configure their workstation to disable the creation of .DS_Store files on network shares.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

BID	3316
BID	3325
CVE	CVE-2001-1446
XREF	CERT:177243

Plugin Information

Published: 2001/09/14, Modified: 2018/11/15

Plugin Output

tcp/80/www

```
http://ec2-52-201-250-219.compute-1.amazonaws.com/.DS_Store
reveals the following entries:
 metadata
 gallery.php
 includes
 images
 html
 login.php
 uploads
 about.php
 css
 admin.php
 entry.php
 Sandbox
 main.php
 display-reviews.php
```

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 information 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: 2020/04/27

Plugin Output

tcp/80/www

```
The following directories are browsable :

http://ec2-52-201-250-219.compute-1.amazonaws.com/css/
http://ec2-52-201-250-219.compute-1.amazonaws.com/html/
http://ec2-52-201-250-219.compute-1.amazonaws.com/images/
http://ec2-52-201-250-219.compute-1.amazonaws.com/includes/
http://ec2-52-201-250-219.compute-1.amazonaws.com/js/
http://ec2-52-201-250-219.compute-1.amazonaws.com/phpMyAdmin/
http://ec2-52-201-250-219.compute-1.amazonaws.com/phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc/
http://ec2-52-201-250-219.compute-1.amazonaws.com/phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc/
html/_sources/
```

```
http://ec2-52-201-250-219.compute-1.amazonaws.com/phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc/
html/_static/
http://ec2-52-201-250-219.compute-1.amazonaws.com/phpMyAdmin/phpMyAdmin-5.0.4-all-languages/themes/
http://ec2-52-201-250-219.compute-1.amazonaws.com/phpMyAdmin/phpMyAdmin-5.0.4-all-languages/themes/
metro/
http://ec2-52-201-250-219.compute-1.amazonaws.com/phpMyAdmin/phpMyAdmin-5.0.4-all-languages/themes/
metro/css/
http://ec2-52-201-250-219.compute-1.amazonaws.com/phpMyAdmin/phpMyAdmin-5.0.4-all-languages/themes/
metro/fonts/
http://ec2-52-201-250-219.compute-1.amazonaws.com/phpMyAdmin/phpMyAdmin-5.0.4-all-languages/themes/
metro/img/
http://ec2-52-201-250-219.compute-1.amazonaws.com/phpMyAdmin/phpMyAdmin-5.0.4-all-languages/themes/
metro/jquery/
http://ec2-52-201-250-219.compute-1.amazonaws.com/phpMyAdmin/phpMyAdmin-5.0.4-all-languages/themes/
metro/scss/
http://ec2-52-201-250-219.compute-1.amazonaws.com/phpMyAdmin/phpMyAdmin-5.0.4-all-languages/themes/
original/
http://ec2-52-201-250-219.compute-1.amazonaws.com/phpMyAdmin/phpMyAdmin-5.0.4-all-languages/themes/
original/css/
http://ec2-52-201-250-219.compute-1.amazonaws.com/phpMyAdmin/phpMyAdmin-5.0.4-all-languages/themes/
original/img/
http://ec2-52-201-250-219.compute-1.amazonaws.com/phpMyAdmin/phpMyAdmin-5.0.4-all-languages/themes/
original/jquery/
http://ec2-52-201-250-219.compute-1.amazonaws.com/phpMyAdmin/phpMyAdmin-5.0.4-all-languages/themes/
original/scss/
http://ec2-52-2 [...]
```

65702 - Git Repository Served by Web Server

Synopsis

The remote web server may disclose information due to a configuration weakness.

Description

The web server on the remote host allows read access to a Git repository. This potential flaw can be used to download content from the Web server that might otherwise be private.

See Also

https://blog.skullsecurity.org/2012/using-git-clone-to-get-pwn3d

http://www.nessus.org/u?b573eafc

Solution

Verify that the listed Git repositories are served intentionally.

Risk Factor

Medium

CVSS Base Score

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

Plugin Information

Published: 2013/03/27, Modified: 2018/11/15

Plugin Output

tcp/80/www

```

The following repositories were found on the remote web server :

  Repository : http://ec2-52-201-250-219.compute-1.amazonaws.com/.git
  Type       : Non-Bare
  Transport  : Not configured for cloning
```

140532 - PHP 7.2.x / 7.3.x < 7.3.22 Memory Leak Vulnerability

Synopsis

The version of PHP running on the remote web server is affected by a memory leak vulnerability.

Description

According to its self-reported version number, the version of PHP running on the remote web server is 7.2.x or 7.3.x prior to 7.3.21. It is, therefore affected by a memory leak vulnerability in the LDAP component. An unauthenticated, remote attacker could exploit this issue to cause a denial-of-service condition.

See Also

https://www.php.net/ChangeLog-7.php#7.3.22

Solution

Upgrade to PHP version 7.3.22 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

STIG Severity

I

References

XREF	IAVA:2020-A-0420-S

Plugin Information

Published: 2020/09/11, Modified: 2020/10/09

Plugin Output

tcp/80/www

```
 URL               : http://ec2-52-201-250-219.compute-1.amazonaws.com/ (7.2.34 under Server:
Apache/2.4.46 (Amazon) PHP/7.2.34, X-Powered-By: PHP/7.2.34)
 Installed version : 7.2.34
 Fixed version     : 7.3.22
```

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/80/www

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

  - http://ec2-52-201-250-219.compute-1.amazonaws.com/about.php
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/html/profile.html
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/login.php
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc/
html/
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc/
html/bookmarks.html
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc/
html/charts.html
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc/
html/copyright.html
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc/
html/credits.html
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc/
html/developers.html
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc/
html/genindex.html
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc/
html/glossary.html
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc/
html/import_export.html
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc/
html/index.html
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc/
html/intro.html
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc/
html/other.html
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc/
html/privileges.html
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc/
html/relations.html
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/phpMyAdmin/phpMyAdmin-5.0.4-all-lan [...]
```

26194 - Web Server Transmits Cleartext Credentials

Synopsis

The remote web server might transmit credentials in cleartext.

Description

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

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

Solution

Make sure that every sensitive form transmits content over HTTPS.

Risk Factor

Low

CVSS Base Score

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

References

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

Plugin Information

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

Plugin Output

tcp/80/www

```
Page : /login.php
Destination Page: /includes/login-helper.php

Page : /signup.php
Destination Page: /includes/signup-helper.php

Page : /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/
```

```
Destination Page: /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/index.php

Page : /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/index.php
Destination Page: /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/index.php
```

48204 - Apache HTTP Server Version

Synopsis

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

Description

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

See Also

https://httpd.apache.org/

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0530

Plugin Information

Published: 2010/07/30, Modified: 2020/09/22

Plugin Output

tcp/80/www

```
URL        : http://ec2-52-201-250-219.compute-1.amazonaws.com/
Version    : 2.4.46
backported : 0
modules    : PHP/7.2.34
os         : Amazon
```

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: 2020/06/12

Plugin Output

tcp/80/www

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

+ The following resources may be vulnerable to injectable parameter :

+ The 'db' parameter of the /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/index.php CGI :

/phpMyAdmin/phpMyAdmin-5.0.4-all-languages/index.php?db=%00lxydpv

-------- output --------
<script data-cfasync="false" type="text/javascript">
// <![CDATA[
[...] ang:"en",server:"1",table:"",db:"lxydpv",token:"4b6f587733763e376d2b3663 [...]
ConsoleEnterExecutes=false
------------------------
```

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: 2020/06/12

Plugin Output

tcp/80/www

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

on site request forgery                  : S=1          SP=1         AP=1         SC=1         AC=1

SQL injection                            : S=552        SP=552       AP=2376      SC=24
 AC=9936
unseen parameters                        : S=805        SP=805       AP=3465      SC=35
 AC=14490
local file inclusion                     : S=23         SP=23        AP=99        SC=1
 AC=414
web code injection                       : S=23         SP=23        AP=99        SC=1
 AC=414
XML injection                            : S=23         SP=23        AP=99        SC=1
 AC=414
format string                            : S=46         SP=46        AP=198       SC=2
 AC=828
script injection                         : S=1          SP=1         AP=1         SC=1         AC=1

cross-site scripting (comprehensive test): S=92         SP=92        AP=396       SC=4
 AC=1656
injectable parameter                     : S=46         SP=46        AP=198       SC=2
 AC=828
```

```
cross-site scripting (extended patterns) : S=6          SP=6         AP=6         SC=6         AC=6

directory traversal (write access)       : S=46         SP=46        AP=198       SC=2
 AC=828
SSI injection                            : S=69         SP=69        AP=297       SC=3
 AC=1242
header injection                         : S=2          SP=2         AP=2         SC=2         AC=2

HTML injection                           : S=5          SP=5         AP=5         SC=5         AC=5

directory traversal                      : S=575        SP=575       AP=2475      SC=25
 AC=10350
arbitrary command execution (time based) : S=138        SP=138       AP=594       SC=6
 AC=2484
persistent XSS                         [...]
```

49704 - External URLs

Synopsis

Links to external sites were gathered.

Description

Nessus gathered HREF links to external sites by crawling the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/10/04, Modified: 2011/08/19

Plugin Output

tcp/80/www

```

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


http://sphinx-doc.org/                  - /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc/html/
index.html
http://www.fpdf.org/                    - /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc/html/
credits.html
http://www.jqplot.com/                  - /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc/html/
charts.html
http://www.php-editors.com/articles/sql_phpmyadmin.php - /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/
doc/html/other.html
http://www.scriptalicious.com/blog/2009/04/complete-inserts-or-extended-inserts-in-phpmyadmin/ - /
phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc/html/import_export.html
https://apps.apple.com/us/app/google-authenticator/id388497605 - /phpMyAdmin/phpMyAdmin-5.0.4-all-
languages/doc/html/two_factor.html
https://authy.com/                      - /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc/html/
two_factor.html
https://cihar.com/publications/linuxsoft/ - /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc/html/
other.html
https://classic.yarnpkg.com/en/docs/install - /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc/html/
setup.html
https://codeload.github.com/phpmyadmin/phpmyadmin/zip/master - /phpMyAdmin/phpMyAdmin-5.0.4-all-
languages/doc/html/setup.html
https://demo.phpmyadmin.net/master/setup/ - /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc/html/
setup.html
https://dev.mysql.com/doc/refman/5.7/en/packet-too-large.html - /phpMyAdmin/phpMyAdmin-5.0.4-all-
languages/doc/html/import_export.html
https://dev.mysql.com/doc/refman/5.7/en/storage-engines.html - /phpMyAdmin/phpMyAdmin-5.0.4-all-
languages/doc/html/glossary.html
```

```
https://en.wikipedia.org/wiki/.htaccess - /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc/html/
glossary.html
https://en.wikipedia.org/wiki/Apache_HTTP_Server - /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc/
html/glossary.html
https://en.wikipedia.org/wiki/Blowfish_(cipher) - /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc/
html/glossary.html
https://en.wikipedia.org/wiki/Brute- [...]
```

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/www

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

      /css
      /html
      /icons
      /images
      /includes
      /js
      /phpMyAdmin
      /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc
      /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc/html
      /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc/html/_sources
      /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc/html/_static
      /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/themes
      /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/themes/metro
      /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/themes/metro/css
      /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/themes/metro/fonts
      /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/themes/metro/img
      /uploads


  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 UNCHECKOUT UNLOCK
      UNSUBSCRIBE UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on :

      /cgi-bin

    - HTTP methods GET HEAD OPTIONS POST are allowed on :

      /
      /css
      /html
      /icons
      /images
      /includes
      /js
      /phpMyAdmin
      /phpMyAdmin/phpMyAdmin-5.0.4-all-languages
      /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc
      /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc/html
      /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc/html/_sources
      /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc/html/_static
      /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/themes
      /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/themes/metro
      /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/themes/metro/css
      /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/themes/metro/fonts
      /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/themes/metro/img
      /uploads

    - Invalid/unknown HTTP methods are allowed on :

      /cgi-bin
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/80/www

```
The remote web server type is :

Apache/2.4.46 (Amazon) PHP/7.2.34
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/80/www

```

Response Code : HTTP/1.1 200 OK

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

  Date: Tue, 03 Nov 2020 22:26:33 GMT
  Server: Apache/2.4.46 (Amazon) PHP/7.2.34
  X-Powered-By: PHP/7.2.34
  Expires: Thu, 19 Nov 1981 08:52:00 GMT
  Cache-Control: no-store, no-cache, must-revalidate
  Pragma: no-cache
  Content-Length: 6773
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html; charset=UTF-8

Response Body :


<link rel="stylesheet" href="css/main.css">
<main>
    <div class="navbar">

<head>
```

```
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <title></title>
    <meta name="description" content="">
    <meta name="viewport" content="width=device-width, initial-scale=1">

    <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/
bootstrap.min.css" integrity="sha384-Gn5384xqQ1aoWXA+058RXPxPg6fy4IWvTNh0E263XmFcJlSAwiGgFAW/
dAiS6JXm" crossorigin="anonymous">
    <script src="https://code.jquery.com/jquery-3.5.1.js" integrity="sha256-
QWo7LDvxbWT2tbbQ97B53yJnYU3WhH/C8ycbRAkjPDc=" crossorigin="anonymous"></script>
    <script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js"
 integrity="sha384-ApNbgh9B+Y1QKtv3Rn7W3mgPxhU9K/ScQsAP7hUibX39j7fakFPskvXusvfa0b4Q"
 crossorigin="anonymous"></script>
    <script src="https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js"
 integrity="sha384-JZR6Spejh4U02d8jOt6vLEHfe/JQGiRRSQQxSfFWpi1MquVdAyjUar5+76PVCmYl"
 crossorigin="anonymous"></script>
    <script src="https://kit.fontawesome.com/0809ee8fa6.js" crossorigin="anonymous"></script>
    <script src="https://ajax.googleapis.com/ajax/libs/jquery/3.5.1/jquery.min.js"></script>
</head>
<header>
    <nav class="navbar navbar-expand-lg navbar-dark bg-dark">
        <div class="d-md-flex d-block flex-row mx-md-auto mx-0">
            <a class="navbar-brand" href="index.php">GAMRFAX</a>
            <button class="navbar-toggler" type="button"  [...]
```

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/www

```

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

  - http://ec2-52-201-250-219.compute-1.amazonaws.com/
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/about.php
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/css/
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/html/
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/html/profile.html
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/images/
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/includes/
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/includes/dbhandler.php
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/includes/gallery-helper.php
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/includes/get-ratings.php
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/includes/header.php
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/includes/review-helper.php
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/includes/upload-helper.php
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/index.php
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/js/
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/login.php
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/phpMyAdmin/
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/phpMyAdmin/phpMyAdmin-5.0.4-all-languages/
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc/
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc/
html/
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc/
html/_sources/
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc/
html/_static/
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc/
html/bookmarks.html
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc/
html/charts.htm [...]
```

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/www

```

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

  - http://ec2-52-201-250-219.compute-1.amazonaws.com/
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/about.php
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/css/
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/html/
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/html/profile.html
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/images/
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/includes/
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/includes/dbhandler.php
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/includes/gallery-helper.php
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/includes/get-ratings.php
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/includes/header.php
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/includes/review-helper.php
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/includes/upload-helper.php
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/index.php
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/js/
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/login.php
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/phpMyAdmin/
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc/
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc/
html/
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc/
html/_sources/
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc/
html/_static/
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc/
html/bookmarks.html
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc/
html/charts.html
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc/
html/copyright.html [...]
```

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: 2020/09/14

Plugin Output

tcp/22/ssh

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2020/09/14

Plugin Output

tcp/80/www

```
Port 80/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.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2020/08/27

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 8.12.1
Plugin feed version : 202011031732
Scanner edition used : Nessus Home
Scan type : Normal
Scan policy used : Web Application Tests
Scanner IP : 10.0.2.15
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
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
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : enabled
Web application tests : enabled
Web app tests -  Test mode : single
Web app tests -  Try all HTTP methods : no
Web app tests -  Maximum run time : 5 minutes.
Web app tests -  Stop at first flaw : CGI
Max hosts : 2
Max checks : 2
Recv timeout : 15
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2020/11/3 17:16 EST
Scan duration : 1284 sec
```

48243 - PHP Version Detection

Synopsis

It was possible to obtain the version number of the remote PHP installation.

Description

Nessus was able to determine the version of PHP available on the remote web server.

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0936

Plugin Information

Published: 2010/08/04, Modified: 2020/09/22

Plugin Output

tcp/80/www

```
Nessus was able to identify the following PHP version information :

  Version : 7.2.34
  Source  : Server: Apache/2.4.46 (Amazon) PHP/7.2.34
  Source  : X-Powered-By: PHP/7.2.34
```

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/www

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

Name : PHPSESSID
Path : /
Value : rqgsknmh5qacv4dgj6t3apq9en
Domain :
Version : 1
Expires :
Comment :
Secure : 0
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/www

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

Name : phpMyAdmin
Path : /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/
Value : ionrkv6f04okpr50m7saqc7fgn
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 1
Port :


Name : pma_lang
Path : /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/
Value : en
Domain :
Version : 1
Expires : Thu, 03-Dec-2020 22:22:09 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : PHPSESSID
Path : /
Value : rqgsknmh5qacv4dgj6t3apq9en
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :
```

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: 2020/06/12

Plugin Output

tcp/80/www

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

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

Potentially sensitive parameters for CGI /includes/signup-helper.php :

pwd : Possibly a clear or hashed password, vulnerable to sniffing or 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/www

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

  - http://ec2-52-201-250-219.compute-1.amazonaws.com/
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/about.php
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/css/
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/css/about.css
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/css/admin.css
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/css/all.css
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/css/gallery.css
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/css/login.css
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/css/main.css
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/css/signup.css
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/html/
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/html/profile.html
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/images/
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/images/PS.jpg
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/images/carouselimg1.png
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/images/carouselimg2.png
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/images/carouselimg3.png
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/images/cfo.png
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/images/coolbg.jpg
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/images/coolbg_black.jpg
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/images/darkbg.jpeg
  - http://ec2-52-201-250-219.compute-1.amazonaws.com/images/darkbg2.jpg
```

```
    - http://ec2-52-201-250-219.compute-1.amazonaws.com/images/defaultpfp.png
    - http://ec2-52-201-250-219.compute-1.amazonaws.com/images/lawyer.png
    - http://ec2-52-201-250-219.compute-1.amazonaws.com/images/login-background.png
    - http://ec2-52-201-250-219.compute-1.amazonaws.com/images/loginbg.jpg
    - http://ec2-52-201-250-219.compute-1.amazonaws.com/images/morpheus.jpg
    - http://ec2-52-201-250-219.compute-1.amazonaws.com/images/ninswitc [...]
```

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: 2020/06/12

Plugin Output

tcp/80/www

```
Page : /login.php
Destination Page: /includes/login-helper.php

Page : /signup.php
Destination Page: /includes/signup-helper.php

Page : /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/
Destination Page: /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/index.php

Page : /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/index.php
Destination Page: /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/index.php
```

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: 2020/06/12

Plugin Output

tcp/80/www

```

The following directories were discovered:
/cgi-bin, /includes, /css, /html, /icons, /images, /js, /phpMyAdmin, /uploads

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

49705 - Web Server Harvested Email Addresses

Synopsis

Email addresses were harvested from the web server.

Description

Nessus harvested HREF mailto: links and extracted email addresses by crawling the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/10/04, Modified: 2018/05/24

Plugin Output

tcp/80/www

```

The following email address has been gathered :


- 'security%40phpmyadmin.net', referenced from :
   /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc/html/security.html
```

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: 2020/09/14

Plugin Output

tcp/80/www

```
Webmirror performed 847 queries in 159s (5.0327 queries per second)

The following CGIs have been discovered :


+ CGI : /includes/login-helper.php
  Methods : POST
  Argument : pwd
  Argument : uname


+ CGI : /includes/signup-helper.php
  Methods : POST
  Argument : con-pwd
  Argument : email
  Argument : fname
  Argument : lname
  Argument : pwd
  Argument : uname


+ CGI : /html/includes/upload-helper.php
  Methods : POST
  Argument : bio
  Argument : prof-image
```

```
+ CGI : /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/url.php
  Methods : GET
  Argument : url
   Value: https%3A%2F%2Fwww.phpmyadmin.net%2F


+ CGI : /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/index.php
  Methods : GET,POST
  Argument : db
  Argument : lang
   Value: vi
  Argument : pma_password
  Argument : pma_username
  Argument : server
   Value: 1
  Argument : set_session
   Value: ionrkv6f04okpr50m7saqc7fgn
  Argument : table
  Argument : target
   Value: index.php
  Argument : token
   Value: 296a39572e67572c39795859475e7674


+ CGI : /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc/html/search.html
  Methods : GET
  Argument : area
   Value: default
  Argument : check_keywords
   Value: yes
  Argument : q

Directory index found at /includes/
Directory index found at /css/
Directory index found at /html/
Directory index found at /uploads/
Directory index found at /phpMyAdmin/
Directory index found at /js/
Directory index found at /images/
Directory index found at /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/themes/pmahomme/jquery/
Directory index found at /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/themes/pmahomme/
Directory index found at /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/themes/
Directory index found at /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/themes/pmahomme/css/
Directory index found at /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/doc/
Directory index found at /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/themes/pmahomme/img/
Directory index found at /phpMyAdmin/phpMyAdmin-5.0.4-all-languages/themes/pmahomme/scss/
Directory index found at  [...]
```

17219 - phpMyAdmin Detection

Synopsis

The remote web server hosts a database management application written in PHP.

Description

The remote host is running phpMyAdmin, a web-based MySQL administration tool written in PHP.

See Also

https://www.phpmyadmin.net/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/02/25, Modified: 2019/11/22

Plugin Output

tcp/80/www

```

The following instance of phpMyAdmin was detected on the remote host :

  Version : 5.0.4
  URL     : http://ec2-52-201-250-219.compute-1.amazonaws.com/phpMyAdmin/phpMyAdmin-5.0.4-all-
languages/
```