nessus-web-all-ports-complex

Report generated by Nessus™ Thu, 01 Jun 2023 13:23:50 EDT

Nessus Essentials

TABLE OF CONTENTS

Vulnerabilities by Host

Nessus Essentials

Nessus Essentials

Vulnerabilities by Host

10.0.2.4

0	1	3	0	16
CRITICAL	HIGH	MEDIUM	LOW	INFO

Host Information

IP:	10.0.2.4
MAC Address:	08:00:27:0F:15:FD
OS:	Linux Kernel 2.6

Vulnerabilities

42423 - CGI Generic SSI Injection (HTTP headers)

Synopsis

It may be possible to execute arbitrary code through a CGI script hosted on the remote web server.

Description

The remote web server hosts one or more CGI scripts that fail to adequately sanitize request strings and seem to be vulnerable to an 'SSI injection' attack. By leveraging this issue, an attacker may be able to execute arbitrary commands on the remote host.

See Also

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

https://www.owasp.org/index.php/Server-Side_Includes_(SSI)_Injection

http://projects.webappsec.org/w/page/13246964/SSI%20Injection

Solution

Disable Server Side Includes if you do not use them.

Otherwise, restrict access to the vulnerable application or contact the vendor for a patch / upgrade.

Risk Factor

High

CVSS v2.0 Base Score

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

Nessus Essentials

References

XREF	CWE:97
XREF	CWE:96
XREF	CWE:94
XREF	CWE:74
XREF	CWE:727
XREF	CWE:632
XREF	CWE:75
XREF	CWE:752
XREF	CWE:713

Plugin Information

Published: 2009/11/06, Modified: 2021/01/19

Plugin Output

tcp/80/www

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

+ The following resources may be vulnerable to SSI injection (on HTTP headers) :

/manual/de/howto/ssi.html

-------- request --------
POST /manual/de/howto/ssi.html HTTP/1.1
Host: 10.0.2.4
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Close
Content-Length: 71
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
<!--#include file="nessus784690508.html"-->=1&/manual/de/howto/ssi.html
------------------------

-------- output --------
you get the message</p>
<div class="example"><p><code>
[an error occurred while processing this directive]
</code></p></div>
------------------------

/manual/tr/howto/ssi.html

-------- request --------
POST /manual/tr/howto/ssi.html HTTP/1.1
Host: 10.0.2.4
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Close
Content-Length: 71
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
```

```
<!--#include file="nessus784690508.html"-->=1&/manual/tr/howto/ssi.html
------------------------

-------- output --------
you get the message</p>
<div class="example"><p><code>
[an error occurred while processing this directive]
</code></p></div>
------------------------

/manual/zh-cn/howto/ssi.html

-------- request --------
POST /manual/zh-cn/howto/ssi.html HTTP/1.1
Host: 10.0.2.4
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Close
Content-Length: 74
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
<!--#include file="nessus784690508.html"-->=1&/manual/zh-cn/howto/ssi.html
------------------------

-------- output --------
you get the message</p>
<div class="example"><p><code>
[an er [...]
```

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 v2.0 Base Score

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

Plugin Information

Published: 2009/09/15, Modified: 2021/01/19

Plugin Output

tcp/80/www

```
The following directories are browsable :

http://10.0.2.4/css/
http://10.0.2.4/img/
http://10.0.2.4/js/
http://10.0.2.4/manual/images/
http://10.0.2.4/manual/style/
http://10.0.2.4/manual/style/css/
```

57640 - Web Application Information Disclosure

Synopsis

The remote web application discloses path information.

Description

At least one web application hosted on the remote web server discloses the physical path to its directories when a malformed request is sent to it.

Leaking this kind of information may help an attacker fine-tune attacks against the application and its backend.

Solution

Filter error messages containing path information.

Risk Factor

Medium

CVSS v2.0 Base Score

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

Plugin Information

Published: 2012/01/25, Modified: 2021/01/19

Plugin Output

tcp/80/www

```
The request POST /manual/zh-cn/howto/ssi.html HTTP/1.1
Host: 10.0.2.4
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Close
Content-Length: 74
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
<!--#include file="nessus784690508.html"-->=1&/manual/zh-cn/howto/ssi.html

produces the following path information :
<p>Here's something else that you can do with the <code>exec</code>
function. You can actually have SSI execute a command using the
shell (<code>/bin/sh</code>, to be precise - or the DOS shell,
if you're on Win32). The following, for example, will give you
a directory listing.</p>

The request POST /manual/en/howto/ssi.html HTTP/1.1
Host: 10.0.2.4
```

```
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Close
Content-Length: 71
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
<!--#include file="nessus784690508.html"-->=1&/manual/en/howto/ssi.html

produces the following path information :
<p>Here's something else that you can do with the <code>exec</code>
function. You can actually have SSI execute a command using the
shell (<code>/bin/sh</code>, to be precise - or the DOS shell,
if you're on Win32). The following, for example, will give you
a directory listing.</p>

The request POST /manual/tr/howto/ssi.html HTTP/1.1
Host: 10.0.2.4
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Close
Content-Length: 71
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
<!--#include file="nessus784690508.html"-->=1&/manual/tr/howto/ssi.html

produces the following path information :
<p>Here's something else that you can do with the <code>exec</code>
function [...]
```

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 v2.0 Base Score

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

References

XREF	CWE:693

Plugin Information

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

Plugin Output

tcp/80/www

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

  - http://10.0.2.4/
  - http://10.0.2.4/manual/da/
  - http://10.0.2.4/manual/da/index.html
  - http://10.0.2.4/manual/de/
  - http://10.0.2.4/manual/de/index.html
  - http://10.0.2.4/manual/en/
  - http://10.0.2.4/manual/en/index.html
  - http://10.0.2.4/manual/es/
  - http://10.0.2.4/manual/es/index.html
  - http://10.0.2.4/manual/fr/
  - http://10.0.2.4/manual/fr/index.html
  - http://10.0.2.4/manual/ja/
  - http://10.0.2.4/manual/ja/index.html
  - http://10.0.2.4/manual/ko/
  - http://10.0.2.4/manual/ko/index.html
  - http://10.0.2.4/manual/pt-br/
  - http://10.0.2.4/manual/pt-br/index.html
  - http://10.0.2.4/manual/tr/
  - http://10.0.2.4/manual/tr/index.html
  - http://10.0.2.4/manual/zh-cn/
  - http://10.0.2.4/manual/zh-cn/index.html
```

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: 2023/05/24

Plugin Output

tcp/80/www

```
URL        : http://10.0.2.4/
Version    : 2.4.99
Source     : Server: Apache/2.4.38 (Debian)
backported : 1
os         : ConvertedDebian
```

33817 - CGI Generic Tests Load Estimation (all tests)

Synopsis

Load estimation for web application tests.

Description

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

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/80/www

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

arbitrary command execution (time based) : S=6          SP=6         AP=6         SC=6         AC=6

format string                            : S=2          SP=2         AP=2         SC=2         AC=2

cross-site scripting (comprehensive test): S=17         SP=17        AP=17        SC=17        AC=17

injectable parameter                     : S=2          SP=2         AP=2         SC=2         AC=2

arbitrary command execution              : S=22         SP=22        AP=22        SC=22        AC=22

local file inclusion                     : S=4          SP=4         AP=4         SC=4         AC=4

directory traversal                      : S=29         SP=29        AP=29        SC=29        AC=29

web code injection                       : S=1          SP=1         AP=1         SC=1         AC=1

blind SQL injection (4 requests)         : S=4          SP=4         AP=4         SC=4         AC=4
```

```
persistent XSS                          : S=4          SP=4          AP=4          SC=4          AC=4
directory traversal (write access)      : S=2          SP=2          AP=2          SC=2          AC=2
XML injection                           : S=1          SP=1          AP=1          SC=1          AC=1
blind SQL injection                     : S=12         SP=12         AP=12         SC=12         AC=12
SQL injection                           : S=28         SP=28         AP=28         SC=28         AC=28
directory traversal (extended test)     : S=51         SP=51         AP=51         SC=51         AC=51
SSI injection                           : S=3          SP=3          AP=3          SC=3          AC=3
unseen parameters                       : S=35         SP=35         AP=35         SC=35         AC=35
SQL injection (2nd order)              [...]
```

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

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


http://apache.webthing.com/mod_diagnostics/ - /manual/en/mod/mod_filter.html
http://apache.webthing.com/mod_proxy_html/ - /manual/ja/urlmapping.html
http://apachetoday.com/news_story.php3?ltsn=2000-06-14-002-01-PS - /manual/ko/env.html
http://apr.apache.org                   - /manual/en/mod/mod_ldap.html
http://apr.apache.org/                  - /manual/en/glossary.html
http://apr.apache.org/docs/apr-util/trunk/group___a_p_r___util___bucket___brigades.html - /manual/
en/developer/output-filters.html
http://apr.apache.org/docs/apr/1.4/group__apr__pools.html#ga85f1e193c31d109affda72f9a92c6915 - /
manual/en/developer/modguide.html
http://apr.apache.org/docs/apr/1.4/group__apr__pools.html#gaf61c098ad258069d64cdf8c0a9369f9e - /
manual/en/developer/modguide.html
http://apr.apache.org/docs/apr/1.4/group__apr__strings.html#ga3eca76b8d293c5c3f8021e45eda813d8 - /
manual/en/developer/modguide.html
http://apr.apache.org/docs/apr/1.4/group__apr__strings.html#gabc79e99ff19abbd7cfd18308c5f85d47 - /
manual/en/developer/modguide.html
http://aspell.sourceforge.net/          - /manual/en/developer/thread_safety.html
http://bahumbug.wordpress.com/2006/10/12/mod_proxy_html-revisited/ - /manual/en/mod/mod_xml2enc.html
http://bitnami.com/stack/wamp           - /manual/en/platform/windows.html
http://blog.haproxy.com/haproxy/proxy-protocol/ - /manual/en/mod/mod_remoteip.html
http://bugs.apache.org/index/full/467   - /manual/en/misc/perf-tuning.html
http://caniuse.com/#search=http2        - /manual/en/howto/http2.html
http://cgi-spec.golux.com               - /manual/ja/env.html
http://cgi-spec.golux.com/              - /manual/de/glossary.html
http://cgiwrap.sourceforge.net/         - /manual/en/misc/security_tips.html
http://cgiwrap.unixtools.org/           - /manual/ko/misc/security_tips.html
http://ci.apache.org/projects/httpd/trunk/doxygen/ - /manual/en/developer/index.html
```

```
http://ci.apache.org/projects/httpd/trunk/doxygen/group_ [...]
```

43111 - HTTP Methods Allowed (per directory)

Synopsis

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

Description

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

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

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

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

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

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

See Also

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

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/80/www

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

  - HTTP methods GET HEAD OPTIONS POST are allowed on :

    /
    /css
    /icons
    /img
    /js
    /manual
    /manual/da
    /manual/da/developer
    /manual/da/faq
    /manual/da/howto
    /manual/da/misc
    /manual/da/mod
    /manual/da/platform
    /manual/da/programs
    /manual/da/rewrite
    /manual/da/ssl
    /manual/da/vhosts
    /manual/de


Based on tests of each method :

  - HTTP methods GET HEAD OPTIONS POST are allowed on :

    /
    /css
    /icons
    /img
    /js
    /manual
    /manual/da
    /manual/da/developer
    /manual/da/faq
    /manual/da/howto
    /manual/da/misc
    /manual/da/mod
    /manual/da/platform
    /manual/da/programs
    /manual/da/rewrite
    /manual/da/ssl
    /manual/da/vhosts
    /manual/de
```

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/2.4.38 (Debian)
```

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: Thu, 01 Jun 2023 17:07:52 GMT
  Server: Apache/2.4.38 (Debian)
  Last-Modified: Thu, 22 Apr 2021 02:12:14 GMT
  ETag: "7d1-5c086352f5b80"
  Accept-Ranges: bytes
  Content-Length: 2001
  Vary: Accept-Encoding
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html

Response Body :

<head>
    <link rel="stylesheet" type="text/css" href="css/style.css">
    <script type="text/javascript" src="js/main.js"></script>
    <title>Momentum | Index </title>
</head>
<body>
```

```
<br><br>
<h1>Momentum</h1>
<p id="prova"></p>
<br><br>
<a href="#img1">
    <img class="thumb" src="img/c.jpg">
</a>
<!-- lightbox container hidden with CSS -->
<div class="lightbox" id="img1">
    <a href="#img3" class="light-btn btn-prev">prev</a>
        <a href="#_" class="btn-close">X</a>
         <img src="img/c.jpg" onclick="viewDetails('demon')" />
    <a href="#img2" class="light-btn btn-next">next</a>
</div>
<a href="#img2">
  <img class="thumb" src="img/b.jpg">
</a>
<!-- lightbox container hidden with CSS -->
<div class="lightbox" id="img2">
    <a href="#img1" class="light-btn btn-prev">prev</a>
        <a href="#_" class="btn-close">X</a>
        <img src="img/b.jpg" onclick="viewDetails('angel')" />
    <a href="#img3" class="light-btn btn-next">next</a>
</div>
<a href="#img3">
  <img class="thumb" src="img/a.jpg">
</a>
<!-- lightbox container hidden with CSS -->
<div class="lightbox" id="img3">
    <a href="#img2" class="light-btn btn-prev">prev</a>
        <a href="#_" class="btn-close">X</a>
        <img src="img/a.jpg" onclick="viewDetails('guard')" />
    <a href="#img4" class="light-btn btn-next">next</a>
</div>
<a href="#img4">
  <img class="thumb" src="img/d.jpg">
</  [...]
```

50344 - Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header

Synopsis

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

Description

The remote web server in some responses sets a permissive Content-Security-Policy (CSP) frame-ancestors response header or does not set one at all.

The CSP frame-ancestors header has been proposed by the W3C Web Application Security Working Group as a way to mitigate cross-site scripting and clickjacking attacks.

See Also

http://www.nessus.org/u?55aa8f57

http://www.nessus.org/u?07cc2a06

https://content-security-policy.com/

https://www.w3.org/TR/CSP2/

Solution

Set a non-permissive Content-Security-Policy frame-ancestors header for all requested resources.

Risk Factor

None

Plugin Information

Published: 2010/10/26, Modified: 2021/01/19

Plugin Output

tcp/80/www

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

  - http://10.0.2.4/
  - http://10.0.2.4/css/
  - http://10.0.2.4/img/
  - http://10.0.2.4/js/
  - http://10.0.2.4/manual/
  - http://10.0.2.4/manual/da/
  - http://10.0.2.4/manual/da/bind.html
  - http://10.0.2.4/manual/da/caching.html
  - http://10.0.2.4/manual/da/configuring.html
  - http://10.0.2.4/manual/da/content-negotiation.html
  - http://10.0.2.4/manual/da/custom-error.html
```

```
- http://10.0.2.4/manual/da/developer/index.html
- http://10.0.2.4/manual/da/dns-caveats.html
- http://10.0.2.4/manual/da/dso.html
- http://10.0.2.4/manual/da/expr.html
- http://10.0.2.4/manual/da/faq/index.html
- http://10.0.2.4/manual/da/filter.html
- http://10.0.2.4/manual/da/glossary.html
- http://10.0.2.4/manual/da/handler.html
- http://10.0.2.4/manual/da/howto/access.html
- http://10.0.2.4/manual/da/howto/auth.html
- http://10.0.2.4/manual/da/howto/cgi.html
- http://10.0.2.4/manual/da/howto/htaccess.html
- http://10.0.2.4/manual/da/howto/http2.html
- http://10.0.2.4/manual/da/howto/index.html
- http://10.0.2.4/manual/da/howto/public_html.html
- http://10.0.2.4/manual/da/howto/reverse_proxy.html
- http://10.0.2.4/manual/da/howto/ssi.html
- http://10.0.2.4/manual/da/index.html
- http://10.0.2.4/manual/da/install.html
- http://10.0.2.4/manual/da/invoking.html
- http://10.0.2.4/manual/da/license.html
- http://10.0.2.4/manual/da/logs.html
- http://10.0.2.4/manual/da/misc/index.html
- http://10.0.2.4/manual/da/misc/perf-tuning.html
- http://10.0.2.4/manual/da/misc/security_tips.html
- http://10.0.2.4/manual/da/mod/
- http://10.0.2.4/manual/da/mod/directive-dict.html
- http://10.0.2.4/manual/da/mod/directives.html
- http://10.0.2.4/manual/da/mod/event.html
- http://10.0.2.4/manual/da/mod/index.html
- http://10.0.2.4/manual/da/mod/mod_access_compat.html
- http://10.0.2.4/manual/da/mod/mod_actions.html
- http://10.0.2.4/manual/da/mod/mod_alias.html
- htt [...]
```

50345 - Missing or Permissive X-Frame-Options HTTP Response Header

Synopsis

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

Description

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

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

See Also

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

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

Solution

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

Risk Factor

None

Plugin Information

Published: 2010/10/26, Modified: 2021/01/19

Plugin Output

tcp/80/www

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

  - http://10.0.2.4/
  - http://10.0.2.4/css/
  - http://10.0.2.4/img/
  - http://10.0.2.4/js/
  - http://10.0.2.4/manual/
  - http://10.0.2.4/manual/da/
  - http://10.0.2.4/manual/da/bind.html
  - http://10.0.2.4/manual/da/caching.html
  - http://10.0.2.4/manual/da/configuring.html
  - http://10.0.2.4/manual/da/content-negotiation.html
  - http://10.0.2.4/manual/da/custom-error.html
  - http://10.0.2.4/manual/da/developer/index.html
  - http://10.0.2.4/manual/da/dns-caveats.html
  - http://10.0.2.4/manual/da/dso.html
  - http://10.0.2.4/manual/da/expr.html
  - http://10.0.2.4/manual/da/faq/index.html
```

```
- http://10.0.2.4/manual/da/filter.html
- http://10.0.2.4/manual/da/glossary.html
- http://10.0.2.4/manual/da/handler.html
- http://10.0.2.4/manual/da/howto/access.html
- http://10.0.2.4/manual/da/howto/auth.html
- http://10.0.2.4/manual/da/howto/cgi.html
- http://10.0.2.4/manual/da/howto/htaccess.html
- http://10.0.2.4/manual/da/howto/http2.html
- http://10.0.2.4/manual/da/howto/index.html
- http://10.0.2.4/manual/da/howto/public_html.html
- http://10.0.2.4/manual/da/howto/reverse_proxy.html
- http://10.0.2.4/manual/da/howto/ssi.html
- http://10.0.2.4/manual/da/index.html
- http://10.0.2.4/manual/da/install.html
- http://10.0.2.4/manual/da/invoking.html
- http://10.0.2.4/manual/da/license.html
- http://10.0.2.4/manual/da/logs.html
- http://10.0.2.4/manual/da/misc/index.html
- http://10.0.2.4/manual/da/misc/perf-tuning.html
- http://10.0.2.4/manual/da/misc/security_tips.html
- http://10.0.2.4/manual/da/mod/
- http://10.0.2.4/manual/da/mod/directive-dict.html
- http://10.0.2.4/manual/da/mod/directives.html
- http://10.0.2.4/manual/da/mod/event.html
- http://10.0.2.4/manual/da/mod/index.html
- http://10.0.2.4/manual/da/mod/mod_access_compat.html
- http://10.0.2.4/manual/da/mod/mod_actions.html
- http://10.0.2.4/manual/da/mod/mod_alias.html
- http://10.0.2.4/manual/da/m [...]
```

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: 2023/05/31

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: 2023/05/31

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.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2023/04/27

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.5.2
Nessus build : 20009
Plugin feed version : 202306011205
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : ubuntu1404-x86-64
Scan type : Normal
Scan name : nessus-web-all-ports
```

```
Scan policy used : Web Application Tests
Scanner IP : 10.0.2.15
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Ping RTT : 230.264 ms
Thorough tests : yes
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : enabled
Web application tests : enabled
Web app tests -  Test mode : 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 : 2023/6/1 13:03 EDT
Scan duration : 1232 sec
Scan for malware : no
```

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: 2021/01/19

Plugin Output

tcp/80/www

```
Potentially sensitive parameters for CGI /js/opus-details.php :

id : Potential horizontal or vertical privilege escalation
```

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://10.0.2.4/
  - http://10.0.2.4/css/
  - http://10.0.2.4/css/style.css
  - http://10.0.2.4/img/
  - http://10.0.2.4/img/a.jpg
  - http://10.0.2.4/img/b.jpg
  - http://10.0.2.4/img/c.jpg
  - http://10.0.2.4/img/d.jpg
  - http://10.0.2.4/js/
  - http://10.0.2.4/js/main.js
  - http://10.0.2.4/manual/
  - http://10.0.2.4/manual/da/
  - http://10.0.2.4/manual/da/bind.html
  - http://10.0.2.4/manual/da/caching.html
  - http://10.0.2.4/manual/da/configuring.html
  - http://10.0.2.4/manual/da/content-negotiation.html
  - http://10.0.2.4/manual/da/custom-error.html
  - http://10.0.2.4/manual/da/developer/index.html
  - http://10.0.2.4/manual/da/dns-caveats.html
  - http://10.0.2.4/manual/da/dso.html
  - http://10.0.2.4/manual/da/expr.html
  - http://10.0.2.4/manual/da/faq/index.html
```

```
- http://10.0.2.4/manual/da/filter.html
- http://10.0.2.4/manual/da/glossary.html
- http://10.0.2.4/manual/da/handler.html
- http://10.0.2.4/manual/da/howto/access.html
- http://10.0.2.4/manual/da/howto/auth.html
- http://10.0.2.4/manual/da/howto/cgi.html
- http://10.0.2.4/manual/da/howto/htaccess.html
- http://10.0.2.4/manual/da/howto/http2.html
- http://10.0.2.4/manual/da/howto/index.html
- http://10.0.2.4/manual/da/howto/public_html.html
- http://10.0.2.4/manual/da/howto/reverse_proxy.html
- http://10.0.2.4/manual/da/howto/ssi.html
- http://10.0.2.4/manual/da/index.html
- http://10.0.2.4/manual/da/install.html
- http://10.0.2.4/manual/da/invoking.html
- http://10.0.2.4/manual/da/license.html
- http://10.0.2.4/manual/da/logs.html
- http://10.0.2.4/manual/da/misc/index.html
- http://10.0.2.4/manual/da/misc/perf-tuning.html
- http://10.0.2.4/manual/da/misc/security_tips.html
- http://10.0.2.4/manual/da/mod/
- http://10.0.2.4/manual/da/mod/directive-dict.html
- http://10.0.2.4/manual/da/mod/directives.html
- http://10.0.2.4/manual/da/mod/event.html
- http://10.0.2.4/manual/da/mod/index.html
- http:/ [...]
```

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: 2021/08/17

Plugin Output

tcp/80/www

```
The following directories were discovered:
/css, /icons, /img, /js, /manual

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 addresses have been gathered :


- 'raj@cup.hp.com', referenced from :
   /manual/en/platform/perf-hp.html
   /manual/da/platform/perf-hp.html

- 'users@httpd.apache.org', referenced from :
   /manual/en/ssl/ssl_faq.html
   /manual/da/ssl/ssl_faq.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: 2023/05/31

Plugin Output

tcp/80/www

```
Webmirror performed 1000 queries in 242s (4.0132 queries per second)

The following CGIs have been discovered :


+ CGI : /js/opus-details.php
  Methods : GET
  Argument : id

Directory index found at /js/
Directory index found at /img/
Directory index found at /css/
Directory index found at /manual/style/css/
Directory index found at /manual/style/
Directory index found at /manual/images/
```