qlvbdh.hungyen.dcs.vn

Report generated by Nessus™ Fri, 25 Aug 2023 09:18:41 +07

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

qlvbdh.hungyen.dcs.vn

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	8	4	63

Scan Information

Start time: Fri Aug 25 08:53:09 2023
End time: Fri Aug 25 09:18:41 2023

Host Information

DNS Name: qlvbdh.hungyen.dcs.vn
IP: 113.160.132.205
OS: Microsoft Windows 10

Vulnerabilities

44136 - CGI Generic Cookie Injection Scripting

Synopsis

The remote web server is prone to cookie injection attacks.

Description

The remote web server hosts at least one CGI script that fails to adequately sanitize request strings with malicious JavaScript.

By leveraging this issue, an attacker may be able to inject arbitrary cookies. Depending on the structure of the web application, it may be possible to launch a 'session fixation' attack using this mechanism.

Please note that :

- Nessus did not check if the session fixation attack is feasible.

- This is not the only vector of session fixation.

See Also

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

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

http://www.acros.si/papers/session_fixation.pdf

http://projects.webappsec.org/w/page/13246960/Session%20Fixation

Solution

Restrict access to the vulnerable application. Contact the vendor for a patch or upgrade.

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:472
XREF	CWE:642
XREF	CWE:715
XREF	CWE:722

Plugin Information

Published: 2010/01/25, Modified: 2022/04/11

Plugin Output

tcp/80/www

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

+ The following resources may be vulnerable to cookie manipulation :

+ The 'DcAv5B1aRzPm' parameter of the /qlvbdh/main CGI :

/qlvbdh/main?DcAv5B1aRzPm=<script>document.cookie="testjlhz=6784;"</scri
pt>

-------- output --------
</a>,
<a target="_blank" style=" color: white; " href="https://itunes.ap [...]
[...] Pm' value ='<script>document.cookie="testjlhz=6784;"</script>'><INPUT typ [...]
<div class="button-actions" style="text-align: center; display: no [...]
<span class="icon fa fa-user"></span></div><label class="help-erro [...]
------------------------
```

49067 - CGI Generic HTML Injections (quick test)

Synopsis

The remote web server may be prone to HTML injections.

Description

The remote web server hosts CGI scripts that fail to adequately sanitize request strings with malicious JavaScript. By leveraging this issue, an attacker may be able to cause arbitrary HTML to be executed in a user's browser within the security context of the affected site.

The remote web server may be vulnerable to IFRAME injections or cross-site scripting attacks :

- IFRAME injections allow 'virtual defacement' that might scare or anger gullible users. Such injections are sometimes implemented for 'phishing' attacks.

- XSS are extensively tested by four other scripts.

- Some applications (e.g. web forums) authorize a subset of HTML without any ill effect. In this case, ignore this warning.

See Also

http://www.nessus.org/u?602759bc

Solution

Either restrict access to the vulnerable application or contact the vendor for an update.

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:80
XREF	CWE:86

Plugin Information

Published: 2010/09/01, Modified: 2021/01/19

Plugin Output

tcp/80/www

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

+ The following resources may be vulnerable to HTML injection :

+ The 'DcAv5B1aRzPm' parameter of the /qlvbdh/main CGI :

/qlvbdh/main?DcAv5B1aRzPm=<"lhkmbw%0A>

-------- output --------
</a>,
<a target="_blank" style=" color: white; " href="https://itunes.ap [...]
[...] in_failed='10'><INPUT type='hidden' name='DcAv5B1aRzPm' value ='<"lhkmbw
>'><INPUT type='hidden' name='+4y9k5cbd5cbi5O..' value ='CEt1CzAwJ [...]
<div class="button-actions" style="text-align: center; display: no [...]
------------------------

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

http://qlvbdh.hungyen.dcs.vn/qlvbdh/main?DcAv5B1aRzPm=<"lhkmbw%0A>
```

39466 - CGI Generic XSS (quick test)

Synopsis

The remote web server is prone to cross-site scripting attacks.

Description

The remote web server hosts CGI scripts that fail to adequately sanitize request strings with malicious JavaScript. By leveraging this issue, an attacker may be able to cause arbitrary HTML and script code to be executed in a user's browser within the security context of the affected site.

These XSS are likely to be 'non persistent' or 'reflected'.

See Also

https://en.wikipedia.org/wiki/Cross_site_scripting#Non-persistent

http://www.nessus.org/u?ea9a0369

http://projects.webappsec.org/w/page/13246920/Cross%20Site%20Scripting

Solution

Restrict access to the vulnerable application. Contact the vendor for a patch or upgrade to address any cross-site scripting vulnerabilities.

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:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:80
XREF	CWE:81
XREF	CWE:83
XREF	CWE:86
XREF	CWE:116
XREF	CWE:442
XREF	CWE:692
XREF	CWE:712
XREF	CWE:722

XREF	CWE:725
XREF	CWE:751
XREF	CWE:801
XREF	CWE:811
XREF	CWE:928
XREF	CWE:931

Plugin Information

Published: 2009/06/19, Modified: 2022/04/11

Plugin Output

tcp/80/www

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

+ The following resources may be vulnerable to cross-site scripting (quick test) :

+ The 'DcAv5B1aRzPm' parameter of the /qlvbdh/main CGI :

/qlvbdh/main?DcAv5B1aRzPm=<IMG%20SRC="javascript:alert(104);">

-------- output --------
</a>,
<a target="_blank" style=" color: white; " href="https://itunes.ap [...]
[...] v5B1aRzPm' value ='<IMG SRC="javascript:alert(104);">'><INPUT type='hidd [...]
<div class="button-actions" style="text-align: center; display: no [...]
<span class="icon fa fa-user"></span></div><label class="help-erro [...]
------------------------
```

136929 - JQuery 1.2 < 3.5.0 Multiple XSS

Synopsis

The remote web server is affected by multiple cross site scripting vulnerability.

Description

According to the self-reported version in the script, the version of JQuery hosted on the remote web server is greater than or equal to 1.2 and prior to 3.5.0. It is, therefore, affected by multiple cross site scripting vulnerabilities.

Note, the vulnerabilities referenced in this plugin have no security impact on PAN-OS, and/or the scenarios required for successful exploitation do not exist on devices running a PAN-OS release.

See Also

https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/

https://security.paloaltonetworks.com/PAN-SA-2020-0007

Solution

Upgrade to JQuery version 3.5.0 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

5.5 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

5.7

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.4 (CVSS2#E:POC/RL:OF/RC:C)

STIG Severity

II

References

CVE	CVE-2020-11022
CVE	CVE-2020-11023
XREF	IAVB:2020-B-0030
XREF	CEA-ID:CEA-2021-0004
XREF	CEA-ID:CEA-2021-0025

Plugin Information

Published: 2020/05/28, Modified: 2022/12/05

Plugin Output

tcp/8080/www

```
URL              : http://qlvbdh.hungyen.dcs.vn:8080/Scripts/jquery-1.10.2.min.js
Installed version : 1.10.2
Fixed version     : 3.5.0
```

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/90/www

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

  - http://qlvbdh.hungyen.dcs.vn:90/cgi-bin/MANGA/index.cgi
```

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/8080/www

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

  - http://qlvbdh.hungyen.dcs.vn:8080/Account/
  - http://qlvbdh.hungyen.dcs.vn:8080/Account/Login
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/admin/
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/admin/dist/
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/admin/dist/css/
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/admin/dist/css/skins/
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/admin/plugins/
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/admin/plugins/iCheck/
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/admin/plugins/iCheck/square/
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/bootstrap/
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/bootstrap/css/
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/font-awesome/
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/font-awesome/css/
  - http://qlvbdh.hungyen.dcs.vn:8080/account/
  - http://qlvbdh.hungyen.dcs.vn:8080/content/
  - http://qlvbdh.hungyen.dcs.vn:8080/content/admin/
  - http://qlvbdh.hungyen.dcs.vn:8080/content/admin/dist/
  - http://qlvbdh.hungyen.dcs.vn:8080/content/admin/dist/css/
  - http://qlvbdh.hungyen.dcs.vn:8080/content/admin/dist/css/skins/
  - http://qlvbdh.hungyen.dcs.vn:8080/content/admin/plugins/
  - http://qlvbdh.hungyen.dcs.vn:8080/content/admin/plugins/iCheck/
  - http://qlvbdh.hungyen.dcs.vn:8080/content/admin/plugins/iCheck/square/
  - http://qlvbdh.hungyen.dcs.vn:8080/content/bootstrap/
  - http://qlvbdh.hungyen.dcs.vn:8080/content/bootstrap/css/
  - http://qlvbdh.hungyen.dcs.vn:8080/content/font-awesome/
  - http://qlvbdh.hungyen.dcs.vn:8080/content/font-awesome/css/
  - http://qlvbdh.hungyen.dcs.vn:8080/error
  - http://qlvbdh.hungyen.dcs.vn:8080/reports/
  - http://qlvbdh.hungyen.dcs.vn:8080/scripts/
  - http://qlvbdh.hungyen.dcs.vn:8080/uploads/
```

134220 - nginx < 1.17.7 Information Disclosure

Synopsis

The remote web server is affected by an information disclosure vulnerability.

Description

According to its Server response header, the installed version of nginx is prior to 1.17.7. It is, therefore, affected by an information disclosure vulnerability.

See Also

http://www.nessus.org/u?fd026623

Solution

Upgrade to nginx version 1.17.7 or later.

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

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

2.2

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2019-20372
XREF	IAVB:2020-B-0013-S

Plugin Information

Published: 2020/03/05, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
URL              : http://qlvbdh.hungyen.dcs.vn/
Installed version : 1.12.2
Fixed version     : 1.17.7
```

134220 - nginx < 1.17.7 Information Disclosure

Synopsis

The remote web server is affected by an information disclosure vulnerability.

Description

According to its Server response header, the installed version of nginx is prior to 1.17.7. It is, therefore, affected by an information disclosure vulnerability.

See Also

http://www.nessus.org/u?fd026623

Solution

Upgrade to nginx version 1.17.7 or later.

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

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

2.2

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2019-20372
XREF	IAVB:2020-B-0013-S

Plugin Information

Published: 2020/03/05, Modified: 2022/04/11

Plugin Output

tcp/90/www

```
URL              : http://qlvbdh.hungyen.dcs.vn:90/
Installed version : 1.2.6
Fixed version     : 1.17.7
```

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

Low

Plugin Information

Published: 2009/10/07, Modified: 2023/07/17

Plugin Output

tcp/8080/www

```
Page : /Account/Login
Destination Page: /Account/Login
```

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 v2.0 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 : /qlvbdh/main
Destination Page: /qlvbdh/main
```

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 v2.0 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/90/www

```
Page : /cgi-bin/MANGA/index.cgi
Destination Page: /cgi-bin/MANGA/index.cgi
```

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 v2.0 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/8080/www

```
Page : /Account/Login
Destination Page: /Account/Login
```

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: 2021/01/19

Plugin Output

tcp/80/www

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

+ The following resources may be vulnerable to injectable parameter :

+ The 'DcAv5B1aRzPm' parameter of the /qlvbdh/main CGI :

/qlvbdh/main?DcAv5B1aRzPm=yrqnce

-------- output --------
</a>,
<a target="_blank" style=" color: white; " href="https://itunes.ap [...]
[...] den' name='DcAv5B1aRzPm' value ='yrqnce'><INPUT type='hidden' name='+4y9 [...]
<div class="button-actions" style="text-align: center; display: no [...]
<span class="icon fa fa-user"></span></div><label class="help-erro [...]
------------------------

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

```
http://qlvbdh.hungyen.dcs.vn/qlvbdh/main?DcAv5B1aRzPm=yrqnce
```

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: 2021/01/19

Plugin Output

tcp/8080/www

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

+ The following resources may be vulnerable to injectable parameter :

+ The 'ReturnURL' parameter of the /Account/Login CGI :

/Account/Login?ReturnURL=yrqnce

-------- output --------
</head>
<body class="hold-transition login-page">
<form method="post" action="./Login?ReturnURL=yrqnce" onsubmit="javascri
pt:return WebForm_OnSubmit();" id="form1">
<div class="aspNetHidden">
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
------------------------

+ The 'search' parameter of the /error CGI :
```

```
/error?search=yrqnce

-------- output --------
</head>
<body class="hold-transition login-page">
<form method="post" action="./error?search=yrqnce" id="form1">
<div class="aspNetHidden">
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="rB [...]
-----------------------

+ The '403%3bhttp%3a%2f%2fqlvbdh.hungyen.dcs.vn%3a8080%2faccount%2f' parameter of the /account/
 CGI :

/account/?403%3bhttp%3a%2f%2fqlvbdh.hungyen.dcs.vn%3a8080%2faccount%2f=y
rqnce

-------- output --------
</head>
<body class="hold-transition login-page">
<form method="post" action="./?403%3bhttp%3a%2f%2fqlvbdh.hungyen.dcs.vn%
3a8080%2faccount%2f%3f403%3bhttp%3a%2f%2fqlvbdh.hungyen.dcs.vn%3a8080%2f
account%2f=yrqnce" id="form1">
<div class="aspNetHidden">
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="az [...]
-----------------------

+ The '403%3bhttp%3a%2f%2fqlvbdh.hungyen.dcs.vn%3a8080%2fcontent%2f' parameter of the /content/
 CGI :

/content/?403%3bhttp%3a%2f%2fqlvbdh.hungyen.dcs.vn%3a8080%2fcontent%2f=y
rqnce

-------- output --------
</head>
<body class="hold-transition login-page">
<form method="post" action="./?403%3bhttp%3a%2f%2fqlvbdh.hungyen.dcs.vn%
3a8080%2fcontent%2f%3f403%3bhttp%3a%2f%2fqlvbdh.hungyen.dcs.vn%3a8080%2f
content%2f=yrqnce" id="form1">
<div class="aspNetHidden">
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="44 [...]
-----------------------

+ The '403%3bhttp%3a%2f%2fqlvbdh.hungyen.dcs.vn%3a8080%2fContent%2fb [...]
```

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]

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

SQL injection                            : S=216        SP=216       AP=1176      SC=0
 AC=4992
unseen parameters                        : S=315        SP=315       AP=1715      SC=0
 AC=7280
local file inclusion                     : S=9          SP=9         AP=49        SC=0
 AC=208
cookie manipulation                      : S=18         SP=18        AP=98        SC=0
 AC=416
web code injection                       : S=9          SP=9         AP=49        SC=0
 AC=208
XML injection                            : S=9          SP=9         AP=49        SC=0
 AC=208
format string                            : S=18         SP=18        AP=98        SC=0
 AC=416
script injection                         : S=1          SP=1         AP=1         SC=1         AC=1
```

```
injectable parameter                     : S=18         SP=18        AP=98        SC=0
 AC=416
cross-site scripting (comprehensive test): S=36         SP=36        AP=196       SC=0
 AC=832
cross-site scripting (extended patterns) : S=6          SP=6         AP=6         SC=6         AC=6

directory traversal (write access)       : S=18         SP=18        AP=98        SC=0
 AC=416
SSI injection                            : S=27         SP=27        AP=147       SC=0
 AC=624
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=225        SP=225       AP=1225      SC=0
 AC=5200
cross-site scripting (quick test)      [...]
```

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/90/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]

SSI injection                           : S=15         SP=15        AP=33        SC=3         AC=39

blind SQL injection                     : S=60         SP=60        AP=132       SC=12
 AC=156
directory traversal (write access)      : S=10         SP=10        AP=22        SC=2         AC=26

persistent XSS                          : S=20         SP=20        AP=44        SC=4         AC=52

SQL injection                           : S=120        SP=120       AP=264       SC=24
 AC=312
cross-site scripting (comprehensive test): S=20        SP=20        AP=44        SC=4         AC=52

arbitrary command execution             : S=80         SP=80        AP=176       SC=16
 AC=208
SQL injection (2nd order)               : S=5          SP=5         AP=11        SC=1         AC=13

local file inclusion                    : S=5          SP=5         AP=11        SC=1         AC=13
```

```
XML injection                              : S=5          SP=5          AP=11         SC=1          AC=13

directory traversal (extended test)        : S=255        SP=255        AP=561        SC=51
 AC=663
injectable parameter                       : S=10         SP=10         AP=22         SC=2          AC=26

blind SQL injection (4 requests)           : S=20         SP=20         AP=44         SC=4          AC=52

unseen parameters                          : S=175        SP=175        AP=385        SC=35
 AC=455
format string                              : S=10         SP=10         AP=22         SC=2          AC=26

arbitrary command execution (time based) : S=30         SP=30         AP=66         SC=6          AC=78

web code injection                         : S=5          SP=5          AP=11         SC=1          AC=13

directory traversal                      [...]
```

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/8080/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]

SSI injection                           : S=384        SP=384       AP=1008      SC=0
 AC=1395
arbitrary command execution (time based) : S=768        SP=768       AP=2016      SC=0
 AC=2790
cross-site scripting (comprehensive test): S=512        SP=512       AP=1344      SC=0
 AC=1860
HTTP response splitting                 : S=279        SP=279       AP=279       SC=279
 AC=279
web code injection                      : S=128        SP=128       AP=336       SC=0
 AC=465
format string                           : S=256        SP=256       AP=672       SC=0
 AC=930
header injection                        : S=62         SP=62        AP=62        SC=62        AC=62

on site request forgery                 : S=31         SP=31        AP=31        SC=31        AC=31

SQL injection (2nd order)               : S=128        SP=128       AP=336       SC=0
 AC=465
```

```
directory traversal                     : S=3200       SP=3200      AP=8400      SC=0
 AC=11625
persistent XSS                          : S=512        SP=512       AP=1344      SC=0
 AC=1860
blind SQL injection                     : S=1536       SP=1536      AP=4032      SC=0
 AC=5580
script injection                        : S=31         SP=31        AP=31        SC=31        AC=31

blind SQL injection (4 requests)        : S=512        SP=512       AP=1344      SC=0
 AC=1860
XML injection                           : S=128        SP=128       AP=336       SC=0
 AC=465
directory traversal (write access)      : S=256        SP=256       AP=672       SC=0
 AC=930
arbitrary command execution             : S=2048       SP=2048      AP=5376      SC=0
 AC=7440
unseen parameters                      [...]
```

39470 - CGI Generic Tests Timeout

Synopsis

Some generic CGI attacks ran out of time.

Description

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

Solution

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

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

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

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

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

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/80/www

```
The following tests timed out without finding any flaw :
- SQL injection
```

39470 - CGI Generic Tests Timeout

Synopsis

Some generic CGI attacks ran out of time.

Description

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

Solution

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

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

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

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

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

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/90/www

```
The following tests timed out without finding any flaw :
- SQL injection
```

39470 - CGI Generic Tests Timeout

Synopsis

Some generic CGI attacks ran out of time.

Description

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

Solution

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

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

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

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

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

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8080/www

```
The following tests timed out without finding any flaw :
- SQL injection
```

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

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


https://fonts.googleapis.com/css?family=Roboto:300,400,500,600,700|Roboto
+Condensed:400,700&subset=vietnamese - /qlvbdh/main
https://itunes.apple.com/us/app/vnpt-e-office/id1319829992?ls=1&mt=8 - /qlvbdh/main
https://kontum.vnptioffice.vn           - /qlvbdh/main
https://play.google.com/store/apps/details?id=vn.com.vnpt.vinaphone.vnptsoftware.vnptoffice&hl=vi
 - /qlvbdh/main
```

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/8082/www

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


https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.min.css - /
https://netdna.bootstrapcdn.com/bootstrap/4.4.1/css/bootstrap.min.css - /
```

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  DELETE  HEAD  OPTIONS  POST  PUT GET
    are allowed on :

    /qlvbdh
    /qlvbdh/login
    /qlvbdh/mycss
    /qlvbdh/mycss/custom
    /qlvbdh/smart_admin
    /qlvbdh/smart_admin/css


Based on tests of each method :

  - HTTP methods GET HEAD OPTIONS POST are allowed on :

    /qlvbdh
    /qlvbdh/login
    /qlvbdh/mycss
    /qlvbdh/mycss/custom
    /qlvbdh/smart_admin
    /qlvbdh/smart_admin/css

  - HTTP methods GET HEAD POST are allowed on :

    /
```

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/90/www

```
Based on tests of each method :

  - HTTP methods ACL BCOPY BDELETE BMOVE BPROPFIND BPROPPATCH CHECKIN
    CHECKOUT CONNECT 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 are allowed on :

    /cgi-bin/MANGA

  - HTTP methods GET HEAD POST are allowed on :

    /
    /cgi-bin
    /en
    /images

  - Invalid/unknown HTTP methods are allowed on :

    /cgi-bin/MANGA
```

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/8080/www

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

  - HTTP methods  HEAD  OPTIONS  TRACE GET are allowed on :

    /
    /Account
    /Content
    /Content/admin
    /Content/admin/dist
    /Content/admin/dist/css
    /Content/admin/dist/css/skins
    /Content/admin/plugins
    /Content/admin/plugins/iCheck
    /Content/admin/plugins/iCheck/square
    /Content/bootstrap
    /Content/bootstrap/css
    /Content/font-awesome
    /Content/font-awesome/css
    /account
    /content
    /content/admin
    /reports
    /scripts
    /uploads


Based on tests of each method :

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

    /
    /Account
    /Content
    /Content/admin
    /Content/admin/dist
    /Content/admin/dist/css
    /Content/admin/dist/css/skins
    /Content/admin/plugins
    /Content/admin/plugins/iCheck
    /Content/admin/plugins/iCheck/square
    /Content/bootstrap
    /Content/bootstrap/css
    /Content/font-awesome
    /Content/font-awesome/css
    /account
    /content
    /content/admin
    /error
    /reports
    /scripts
    /uploads

  - Invalid/unknown HTTP methods are allowed on :

    /
    /Account
    /Content
    /Content/admin
    /Content/admin/dist
    /Content/admin/dist/css
    /Content/admin/dist/css/skins
    /Content/admin/plugins
    /Content/admin/plugins/iCheck
    /Content/admin/plugins/iCheck/square
```

```
    /Content/bootstrap
    /Content/bootstrap/css
    /Content/font-awesome
    /Content/font-awesome/css
    /account
    /content
    /content/admin
    /error
    /reports
    /scripts
    /uploads
```

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/8081/www

```
Based on tests of each method :

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

    /

  - Invalid/unknown HTTP methods are allowed on :

    /
```

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/8082/www

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

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

    /
    /help
    /src
    /src/src
    /src/src/src
    /src/src/src/src
    /src/src/src/src/src


Based on tests of each method :

  - HTTP methods GET HEAD OPTIONS are allowed on :

    /
    /help
    /src
    /src/src
    /src/src/src
    /src/src/src/src
    /src/src/src/src/src
```

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 :

nginx/1.12.2
```

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/90/www

```
The remote web server type is :

nginx/1.2.6
```

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/8080/www

```
The remote web server type is :

Microsoft-IIS/10.0
```

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/8081/www

```
The remote web server type is :

Microsoft-IIS/10.0
```

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/8082/www

```
The remote web server type is :

Microsoft-IIS/10.0
```

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/1.1 301 Moved Permanently

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

  Server: nginx/1.12.2
  Date: Fri, 25 Aug 2023 01:48:30 GMT
  Content-Type: text/html
  Content-Length: 185
  Connection: keep-alive
  Location: http://qlvbdh.hungyen.dcs.vn/qlvbdh/
  X-Frame-Options: SAMEORIGIN

Response Body :

<html>
<head><title>301 Moved Permanently</title></head>
<body bgcolor="white">
<center><h1>301 Moved Permanently</h1></center>
<hr><center>nginx/1.12.2</center>
</body>
</html>
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/90/www

```
Response Code : HTTP/1.1 200 OK

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

  Server: nginx/1.2.6
  Date: Fri, 25 Aug 2023 01:57:03 GMT
  Content-Type: text/html
  Content-Length: 347
  Last-Modified: Thu, 24 Jul 2014 01:14:24 GMT
  Connection: keep-alive
  Accept-Ranges: bytes

Response Body :

<html>
<head>
<title>Web Administration Interface</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<noscript>
<meta http-equiv="refresh" content="0;URL=unsupported.html">
</noscript>
<meta http-equiv="refresh" content="0;URL=cgi-bin/MANGA/index.cgi">
</head>
```

```
<body bgcolor="#FFFFFF" text="#000000">
</body>
</html>
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8080/www

```
Response Code : HTTP/1.1 302 Found

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

  Cache-Control: private
  Content-Type: text/html; charset=utf-8
  Location: /Account/Login?ReturnURL=%2fdefault.aspx
  Server: Microsoft-IIS/10.0
  X-AspNet-Version: 4.0.30319
  X-UA-Compatible: IE=edge
  X-Powered-By: ASP.NET
  Date: Fri, 25 Aug 2023 01:57:02 GMT
  Content-Length: 157

Response Body :

<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href="/Account/Login?ReturnURL=%2fdefault.aspx">here</a>.</h2>
</body></html>
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8081/www

```
Response Code : HTTP/1.1 404 Not Found

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

  Transfer-Encoding: chunked
  Server: Microsoft-IIS/10.0
  X-Powered-By: ASP.NET
  Date: Fri, 25 Aug 2023 01:57:02 GMT

Response Body :
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8082/www

```
Response Code : HTTP/1.1 200 OK

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

  Content-Type: text/html
  Last-Modified: Tue, 02 Nov 2021 07:07:06 GMT
  Accept-Ranges: bytes
  ETag: "0897c3eb8cfd71:0"
  Server: Microsoft-IIS/10.0
  X-Powered-By: ASP.NET
  Date: Fri, 25 Aug 2023 01:57:02 GMT
  Content-Length: 13305

Response Body :

<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>H# th#ng thông tin</title>
    <link rel="apple-touch-icon" sizes="57x57" href="/apple-icon-57x57.png">
    <link rel="apple-touch-icon" sizes="60x60" href="/apple-icon-60x60.png">
    <link rel="apple-touch-icon" sizes="72x72" href="/apple-icon-72x72.png">
```

```
    <link rel="apple-touch-icon" sizes="76x76" href="/apple-icon-76x76.png">
    <link rel="apple-touch-icon" sizes="114x114" href="/apple-icon-114x114.png">
    <link rel="apple-touch-icon" sizes="120x120" href="/apple-icon-120x120.png">
    <link rel="apple-touch-icon" sizes="144x144" href="/apple-icon-144x144.png">
    <link rel="apple-touch-icon" sizes="152x152" href="/apple-icon-152x152.png">
    <link rel="apple-touch-icon" sizes="180x180" href="/apple-icon-180x180.png">
    <link rel="icon" type="image/png" sizes="192x192"  href="/android-icon-192x192.png">
    <link rel="icon" type="image/png" sizes="32x32" href="/favicon-32x32.png">
    <link rel="icon" type="image/png" sizes="96x96" href="/favicon-96x96.png">
    <link rel="icon" type="image/png" sizes="16x16" href="/favicon-16x16.png">
    <link rel="manifest" href="/manifest.json">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <meta name="msapplication-TileColor" content="#ffffff">
    <meta name="msapplication-TileImage" content="/ms-icon-144x144.png">
    <meta name="theme-color" content="#ffffff">
    <link rel="stylesheet" src="./src/addtohomescreen.scss">
    <script src="./src/mobile-detect.min.js"></script>
    <link rel="stylesheet" href="https://netdna.bootstrapcdn.com/bootstrap/4.4.1/css/boot [...]
```

91634 - HyperText Transfer Protocol (HTTP) Redirect Information

Synopsis

The remote web server redirects requests to the root directory.

Description

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

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/80/www

```
Request         : http://qlvbdh.hungyen.dcs.vn/
HTTP response   : HTTP/1.1 301 Moved Permanently
Redirect to     : http://qlvbdh.hungyen.dcs.vn/qlvbdh/
Redirect type   : 30x redirect

Final page      : http://qlvbdh.hungyen.dcs.vn/qlvbdh/
HTTP response   : HTTP/1.1 200 OK
```

91634 - HyperText Transfer Protocol (HTTP) Redirect Information

Synopsis

The remote web server redirects requests to the root directory.

Description

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

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/90/www

```
Request         : http://qlvbdh.hungyen.dcs.vn:90/
HTTP response   : HTTP/1.1 200 OK
Redirect to     : http://qlvbdh.hungyen.dcs.vn:90/cgi-bin/MANGA/index.cgi
Redirect type   : meta redirect

Final page      : http://qlvbdh.hungyen.dcs.vn:90/cgi-bin/MANGA/index.cgi
HTTP response   : HTTP/1.1 200 OK
```

91634 - HyperText Transfer Protocol (HTTP) Redirect Information

Synopsis

The remote web server redirects requests to the root directory.

Description

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

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8080/www

```
Request         : http://qlvbdh.hungyen.dcs.vn:8080/
HTTP response   : HTTP/1.1 302 Found
Redirect to     : http://qlvbdh.hungyen.dcs.vn:8080/Account/Login?ReturnURL=%2fdefault.aspx
Redirect type   : 30x redirect

Final page      : http://qlvbdh.hungyen.dcs.vn:8080/Account/Login?ReturnURL=%2fdefault.aspx
HTTP response   : HTTP/1.1 200 OK
```

106658 - 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: 2023/05/24

Plugin Output

tcp/8080/www

```
URL     : http://qlvbdh.hungyen.dcs.vn:8080/Scripts/jquery-1.10.2.min.js
Version : 1.10.2
```

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://qlvbdh.hungyen.dcs.vn/qlvbdh/
  - http://qlvbdh.hungyen.dcs.vn/qlvbdh/main
```

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/90/www

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

  - http://qlvbdh.hungyen.dcs.vn:90/
  - http://qlvbdh.hungyen.dcs.vn:90/cgi-bin/
  - http://qlvbdh.hungyen.dcs.vn:90/cgi-bin/MANGA/index.cgi
  - http://qlvbdh.hungyen.dcs.vn:90/unsupported.html
```

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

Synopsis

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

Description

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

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

See Also

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

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

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

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8080/www

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

  - http://qlvbdh.hungyen.dcs.vn:8080/Account/
  - http://qlvbdh.hungyen.dcs.vn:8080/Account/Login
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/admin/
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/admin/dist/
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/admin/dist/css/
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/admin/dist/css/skins/
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/admin/plugins/
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/admin/plugins/iCheck/
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/admin/plugins/iCheck/square/
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/bootstrap/
```

```
    - http://qlvbdh.hungyen.dcs.vn:8080/Content/bootstrap/css/
    - http://qlvbdh.hungyen.dcs.vn:8080/Content/font-awesome/
    - http://qlvbdh.hungyen.dcs.vn:8080/Content/font-awesome/css/
    - http://qlvbdh.hungyen.dcs.vn:8080/account/
    - http://qlvbdh.hungyen.dcs.vn:8080/content/
    - http://qlvbdh.hungyen.dcs.vn:8080/content/admin/
    - http://qlvbdh.hungyen.dcs.vn:8080/content/admin/dist/
    - http://qlvbdh.hungyen.dcs.vn:8080/content/admin/dist/css/
    - http://qlvbdh.hungyen.dcs.vn:8080/content/admin/dist/css/skins/
    - http://qlvbdh.hungyen.dcs.vn:8080/content/admin/plugins/
    - http://qlvbdh.hungyen.dcs.vn:8080/content/admin/plugins/iCheck/
    - http://qlvbdh.hungyen.dcs.vn:8080/content/admin/plugins/iCheck/square/
    - http://qlvbdh.hungyen.dcs.vn:8080/content/bootstrap/
    - http://qlvbdh.hungyen.dcs.vn:8080/content/bootstrap/css/
    - http://qlvbdh.hungyen.dcs.vn:8080/content/font-awesome/
    - http://qlvbdh.hungyen.dcs.vn:8080/content/font-awesome/css/
    - http://qlvbdh.hungyen.dcs.vn:8080/error
    - http://qlvbdh.hungyen.dcs.vn:8080/reports/
    - http://qlvbdh.hungyen.dcs.vn:8080/scripts/
    - http://qlvbdh.hungyen.dcs.vn:8080/uploads/
```

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/8082/www

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

  - http://qlvbdh.hungyen.dcs.vn:8082/
  - http://qlvbdh.hungyen.dcs.vn:8082/%3A
  - http://qlvbdh.hungyen.dcs.vn:8082/backListReport
  - http://qlvbdh.hungyen.dcs.vn:8082/home
  - http://qlvbdh.hungyen.dcs.vn:8082/info
  - http://qlvbdh.hungyen.dcs.vn:8082/report-list
  - http://qlvbdh.hungyen.dcs.vn:8082/reportList
  - http://qlvbdh.hungyen.dcs.vn:8082/src/%3A
  - http://qlvbdh.hungyen.dcs.vn:8082/src/addtohomescreen.scss
  - http://qlvbdh.hungyen.dcs.vn:8082/src/backListReport
  - http://qlvbdh.hungyen.dcs.vn:8082/src/home
```

```
- http://qlvbdh.hungyen.dcs.vn:8082/src/report-list
- http://qlvbdh.hungyen.dcs.vn:8082/src/reportList
- http://qlvbdh.hungyen.dcs.vn:8082/src/src
- http://qlvbdh.hungyen.dcs.vn:8082/src/src/%3A
- http://qlvbdh.hungyen.dcs.vn:8082/src/src/addtohomescreen.scss
- http://qlvbdh.hungyen.dcs.vn:8082/src/src/backListReport
- http://qlvbdh.hungyen.dcs.vn:8082/src/src/home
- http://qlvbdh.hungyen.dcs.vn:8082/src/src/report-list
- http://qlvbdh.hungyen.dcs.vn:8082/src/src/reportList
- http://qlvbdh.hungyen.dcs.vn:8082/src/src/src
- http://qlvbdh.hungyen.dcs.vn:8082/src/src/src/%3A
- http://qlvbdh.hungyen.dcs.vn:8082/src/src/src/addtohomescreen.scss
- http://qlvbdh.hungyen.dcs.vn:8082/src/src/src/backListReport
- http://qlvbdh.hungyen.dcs.vn:8082/src/src/src/home
- http://qlvbdh.hungyen.dcs.vn:8082/src/src/src/report-list
- http://qlvbdh.hungyen.dcs.vn:8082/src/src/src/reportList
- http://qlvbdh.hungyen.dcs.vn:8082/src/src/src/src
- http://qlvbdh.hungyen.dcs.vn:8082/src/src/src/src/%3A
- http://qlvbdh.hungyen.dcs.vn:8082/src/src/src/src/addtohomescreen.scss
- http://qlvbdh.hungyen.dcs.vn:8082/src/src/src/src/backListReport
- http://qlvbdh.hungyen.dcs.vn:8082/src/src/src/src/home
- http://qlvbdh.hungyen.dcs.vn:8082/src/src/src/src/report-list
- http://qlvbdh.hungyen.dcs.vn:8082/src/src/src/src/reportList
- http://qlvbdh.hungyen.dcs.vn:8082 [...]
```

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/90/www

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

  - http://qlvbdh.hungyen.dcs.vn:90/
  - http://qlvbdh.hungyen.dcs.vn:90/cgi-bin/
  - http://qlvbdh.hungyen.dcs.vn:90/cgi-bin/MANGA/index.cgi
  - http://qlvbdh.hungyen.dcs.vn:90/unsupported.html
```

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/8080/www

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

  - http://qlvbdh.hungyen.dcs.vn:8080/Account/
  - http://qlvbdh.hungyen.dcs.vn:8080/Account/Login
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/admin/
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/admin/dist/
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/admin/dist/css/
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/admin/dist/css/skins/
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/admin/plugins/
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/admin/plugins/iCheck/
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/admin/plugins/iCheck/square/
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/bootstrap/
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/bootstrap/css/
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/font-awesome/
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/font-awesome/css/
  - http://qlvbdh.hungyen.dcs.vn:8080/account/
  - http://qlvbdh.hungyen.dcs.vn:8080/content/
```

```
    - http://qlvbdh.hungyen.dcs.vn:8080/content/admin/
    - http://qlvbdh.hungyen.dcs.vn:8080/content/admin/dist/
    - http://qlvbdh.hungyen.dcs.vn:8080/content/admin/dist/css/
    - http://qlvbdh.hungyen.dcs.vn:8080/content/admin/dist/css/skins/
    - http://qlvbdh.hungyen.dcs.vn:8080/content/admin/plugins/
    - http://qlvbdh.hungyen.dcs.vn:8080/content/admin/plugins/iCheck/
    - http://qlvbdh.hungyen.dcs.vn:8080/content/admin/plugins/iCheck/square/
    - http://qlvbdh.hungyen.dcs.vn:8080/content/bootstrap/
    - http://qlvbdh.hungyen.dcs.vn:8080/content/bootstrap/css/
    - http://qlvbdh.hungyen.dcs.vn:8080/content/font-awesome/
    - http://qlvbdh.hungyen.dcs.vn:8080/content/font-awesome/css/
    - http://qlvbdh.hungyen.dcs.vn:8080/error
    - http://qlvbdh.hungyen.dcs.vn:8080/reports/
    - http://qlvbdh.hungyen.dcs.vn:8080/scripts/
    - http://qlvbdh.hungyen.dcs.vn:8080/uploads/
```

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/8082/www

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

  - http://qlvbdh.hungyen.dcs.vn:8082/
  - http://qlvbdh.hungyen.dcs.vn:8082/%3A
  - http://qlvbdh.hungyen.dcs.vn:8082/backListReport
  - http://qlvbdh.hungyen.dcs.vn:8082/home
  - http://qlvbdh.hungyen.dcs.vn:8082/info
  - http://qlvbdh.hungyen.dcs.vn:8082/report-list
  - http://qlvbdh.hungyen.dcs.vn:8082/reportList
  - http://qlvbdh.hungyen.dcs.vn:8082/src/%3A
  - http://qlvbdh.hungyen.dcs.vn:8082/src/addtohomescreen.scss
  - http://qlvbdh.hungyen.dcs.vn:8082/src/backListReport
  - http://qlvbdh.hungyen.dcs.vn:8082/src/home
  - http://qlvbdh.hungyen.dcs.vn:8082/src/report-list
  - http://qlvbdh.hungyen.dcs.vn:8082/src/reportList
  - http://qlvbdh.hungyen.dcs.vn:8082/src/src
  - http://qlvbdh.hungyen.dcs.vn:8082/src/src/%3A
  - http://qlvbdh.hungyen.dcs.vn:8082/src/src/addtohomescreen.scss
```

```
- http://qlvbdh.hungyen.dcs.vn:8082/src/src/backListReport
- http://qlvbdh.hungyen.dcs.vn:8082/src/src/home
- http://qlvbdh.hungyen.dcs.vn:8082/src/src/report-list
- http://qlvbdh.hungyen.dcs.vn:8082/src/src/reportList
- http://qlvbdh.hungyen.dcs.vn:8082/src/src/src
- http://qlvbdh.hungyen.dcs.vn:8082/src/src/src/%3A
- http://qlvbdh.hungyen.dcs.vn:8082/src/src/src/addtohomescreen.scss
- http://qlvbdh.hungyen.dcs.vn:8082/src/src/src/backListReport
- http://qlvbdh.hungyen.dcs.vn:8082/src/src/src/home
- http://qlvbdh.hungyen.dcs.vn:8082/src/src/src/report-list
- http://qlvbdh.hungyen.dcs.vn:8082/src/src/src/reportList
- http://qlvbdh.hungyen.dcs.vn:8082/src/src/src/src
- http://qlvbdh.hungyen.dcs.vn:8082/src/src/src/src/%3A
- http://qlvbdh.hungyen.dcs.vn:8082/src/src/src/src/addtohomescreen.scss
- http://qlvbdh.hungyen.dcs.vn:8082/src/src/src/src/backListReport
- http://qlvbdh.hungyen.dcs.vn:8082/src/src/src/src/home
- http://qlvbdh.hungyen.dcs.vn:8082/src/src/src/src/report-list
- http://qlvbdh.hungyen.dcs.vn:8082/src/src/src/src/reportList
- http://qlvbdh.hungyen.dcs.vn:8082/src/src/src/src/src
- [...]
```

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: 2023/06/20

Plugin Output

tcp/80/www

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/06/20

Plugin Output

tcp/90/www

```
Port 90/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: 2023/06/20

Plugin Output

tcp/8080/www

```
Port 8080/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: 2023/06/20

Plugin Output

tcp/8081/www

```
Port 8081/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: 2023/06/20

Plugin Output

tcp/8082/www

```
Port 8082/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: 2023/07/31

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.5.0
Nessus build : 20097
Plugin feed version : 202308241626
Scanner edition used : Nessus
Scanner OS : LINUX
Scanner distribution : es7-x86-64
Scan type : Normal
Scan name : qlvbdh.hungyen.dcs.vn
```

```
Scan policy used : Web Application Tests
Scanner IP : 10.156.10.20
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 12.726 ms
Thorough tests : no
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 : single
Web app tests -  Try all HTTP methods : no
Web app tests -  Maximum run time : 5 minutes.
Web app tests -  Stop at first flaw : CGI
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2023/8/25 8:53 +07
Scan duration : 1520 sec
Scan for malware : no
```

66334 - Patch Report

Synopsis

The remote host is missing several patches.

Description

The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.

Note: Because the 'Show missing patches that have been superseded' setting in your scan policy depends on this plugin, it will always run and cannot be disabled.

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information

Published: 2013/07/08, Modified: 2023/08/08

Plugin Output

tcp/0

```
. You need to take the following action :

[ nginx < 1.17.7 Information Disclosure (134220) ]

+ Action to take : Upgrade to nginx version 1.17.7 or later.
```

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 : JSESSIONID
Path : /qlvbdh/
Value : 8380D13C199A39D02E57E93A36E23F6C.TC1_1
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 1
Port :


Name : __AntiXsrfToken
Path : /
Value : b1193d53192d4931a4057fab492138ec
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 1
Port :


Name : bauth
Path : /
Value : YcagrwAfJqULdhLQq4j4g5F7OJvPuRysUBydabsLsexxv
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 1
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/90/www

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

Name : JSESSIONID
Path : /qlvbdh/
Value : 8380D13C199A39D02E57E93A36E23F6C.TC1_1
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 1
Port :


Name : __AntiXsrfToken
Path : /
Value : b1193d53192d4931a4057fab492138ec
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 1
Port :


Name : bauth
Path : /
Value : YcagrwAfJqULdhLQq4j4g5F7OJvPuRysUBydabsLsexxv
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 1
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/8080/www

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

Name : JSESSIONID
Path : /qlvbdh/
Value : 8380D13C199A39D02E57E93A36E23F6C.TC1_1
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 1
Port :


Name : __AntiXsrfToken
Path : /
Value : b1193d53192d4931a4057fab492138ec
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 1
Port :


Name : bauth
Path : /
Value : YcagrwAfJqULdhLQq4j4g5F7OJvPuRysUBydabsLsexxv
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 1
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/8081/www

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

Name : JSESSIONID
Path : /qlvbdh/
Value : 8380D13C199A39D02E57E93A36E23F6C.TC1_1
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 1
Port :


Name : __AntiXsrfToken
Path : /
Value : b1193d53192d4931a4057fab492138ec
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 1
Port :


Name : bauth
Path : /
Value : YcagrwAfJqULdhLQq4j4g5F7OJvPuRysUBydabsLsexxv
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 1
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/8082/www

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

Name : JSESSIONID
Path : /qlvbdh/
Value : 8380D13C199A39D02E57E93A36E23F6C.TC1_1
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 1
Port :


Name : __AntiXsrfToken
Path : /
Value : b1193d53192d4931a4057fab492138ec
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 1
Port :


Name : bauth
Path : /
Value : YcagrwAfJqULdhLQq4j4g5F7OJvPuRysUBydabsLsexxv
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 1
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: 2021/01/19

Plugin Output

tcp/90/www

```
Potentially sensitive parameters for CGI /cgi-bin/MANGA/index.cgi :

password : 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://qlvbdh.hungyen.dcs.vn/qlvbdh/
  - http://qlvbdh.hungyen.dcs.vn/qlvbdh/login/font-awesome.min.css
  - http://qlvbdh.hungyen.dcs.vn/qlvbdh/login/login.css
  - http://qlvbdh.hungyen.dcs.vn/qlvbdh/login/style.css
  - http://qlvbdh.hungyen.dcs.vn/qlvbdh/main
  - http://qlvbdh.hungyen.dcs.vn/qlvbdh/mycss/custom/favicon.ico
  - http://qlvbdh.hungyen.dcs.vn/qlvbdh/smart_admin/css/style_language.css

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

91815 - Web Application Sitemap

Synopsis

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

Description

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/90/www

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

  - http://qlvbdh.hungyen.dcs.vn:90/
  - http://qlvbdh.hungyen.dcs.vn:90/cgi-bin/
  - http://qlvbdh.hungyen.dcs.vn:90/cgi-bin/MANGA/connicon.cgi
  - http://qlvbdh.hungyen.dcs.vn:90/cgi-bin/MANGA/index.cgi
  - http://qlvbdh.hungyen.dcs.vn:90/jquery-ui.css
  - http://qlvbdh.hungyen.dcs.vn:90/unsupported.html

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

91815 - Web Application Sitemap

Synopsis

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

Description

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8080/www

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

  - http://qlvbdh.hungyen.dcs.vn:8080/Account/
  - http://qlvbdh.hungyen.dcs.vn:8080/Account/Login
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/Site.css
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/admin/
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/admin/dist/
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/admin/dist/css/
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/admin/dist/css/AdminLTE.min.css
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/admin/dist/css/skins/
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/admin/dist/css/skins/_all-skins.css
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/admin/plugins/
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/admin/plugins/iCheck/
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/admin/plugins/iCheck/square/
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/admin/plugins/iCheck/square/blue.css
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/bootstrap/
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/bootstrap/css/
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/bootstrap/css/bootstrap.min.css
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/favicon.ico
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/font-awesome/
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/font-awesome/css/
  - http://qlvbdh.hungyen.dcs.vn:8080/Content/font-awesome/css/font-awesome.min.css
  - http://qlvbdh.hungyen.dcs.vn:8080/account/
```

```
    - http://qlvbdh.hungyen.dcs.vn:8080/content/
    - http://qlvbdh.hungyen.dcs.vn:8080/content/Site.css
    - http://qlvbdh.hungyen.dcs.vn:8080/content/admin/
    - http://qlvbdh.hungyen.dcs.vn:8080/content/admin/dist/
    - http://qlvbdh.hungyen.dcs.vn:8080/content/admin/dist/css/
    - http://qlvbdh.hungyen.dcs.vn:8080/content/admin/dist/css/AdminLTE.min.css
    - http://qlvbdh.hungyen.dcs.vn:8080/content/admin/dist/css/skins/
    - http://qlvbdh.hungyen.dcs.vn:8080/content/admin/dist/css/skins/_all-skins.css
    - http://qlvbdh.hungyen.dcs.vn:8080/content/admin/plugins/ [...]
```

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/8082/www

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

  - http://qlvbdh.hungyen.dcs.vn:8082/
  - http://qlvbdh.hungyen.dcs.vn:8082/%3A
  - http://qlvbdh.hungyen.dcs.vn:8082/android-icon-192x192.png
  - http://qlvbdh.hungyen.dcs.vn:8082/apple-icon-114x114.png
  - http://qlvbdh.hungyen.dcs.vn:8082/apple-icon-120x120.png
  - http://qlvbdh.hungyen.dcs.vn:8082/apple-icon-144x144.png
  - http://qlvbdh.hungyen.dcs.vn:8082/apple-icon-152x152.png
  - http://qlvbdh.hungyen.dcs.vn:8082/apple-icon-180x180.png
  - http://qlvbdh.hungyen.dcs.vn:8082/apple-icon-57x57.png
  - http://qlvbdh.hungyen.dcs.vn:8082/apple-icon-60x60.png
  - http://qlvbdh.hungyen.dcs.vn:8082/apple-icon-72x72.png
  - http://qlvbdh.hungyen.dcs.vn:8082/apple-icon-76x76.png
  - http://qlvbdh.hungyen.dcs.vn:8082/backListReport
  - http://qlvbdh.hungyen.dcs.vn:8082/favicon-16x16.png
  - http://qlvbdh.hungyen.dcs.vn:8082/favicon-32x32.png
  - http://qlvbdh.hungyen.dcs.vn:8082/favicon-96x96.png
  - http://qlvbdh.hungyen.dcs.vn:8082/home
  - http://qlvbdh.hungyen.dcs.vn:8082/info
  - http://qlvbdh.hungyen.dcs.vn:8082/manifest.json
  - http://qlvbdh.hungyen.dcs.vn:8082/report-list
  - http://qlvbdh.hungyen.dcs.vn:8082/reportList
  - http://qlvbdh.hungyen.dcs.vn:8082/src/%3A
```

```
    - http://qlvbdh.hungyen.dcs.vn:8082/src/addtohomescreen.scss
    - http://qlvbdh.hungyen.dcs.vn:8082/src/backListReport
    - http://qlvbdh.hungyen.dcs.vn:8082/src/home
    - http://qlvbdh.hungyen.dcs.vn:8082/src/report-list
    - http://qlvbdh.hungyen.dcs.vn:8082/src/reportList
    - http://qlvbdh.hungyen.dcs.vn:8082/src/src
    - http://qlvbdh.hungyen.dcs.vn:8082/src/src/%3A
    - http://qlvbdh.hungyen.dcs.vn:8082/src/src/addtohomescreen.scss
    - http://qlvbdh.hungyen.dcs.vn:8082/src/src/backListReport
    - http://qlvbdh.hungyen.dcs.vn:8082/src/src/home
    - http://qlvbdh.hungyen.dcs.vn:8082/src/src/report-list
    - http://qlvbdh.hungyen.dcs.vn:8082/src/src/reportList
    - http://qlvbdh.hungyen.dcs.vn:8082/src/src/src
    - http://qlvbdh.hungyen.dcs.vn:8082/src/src/src/%3A
    -  [...]
```

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/90/www

```
The following directories were discovered:
/cgi-bin, /images, /en

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

11032 - Web Server Directory Enumeration

Synopsis

It is possible to enumerate directories on the web server.

Description

This plugin attempts to determine the presence of various common directories on the remote web server. By sending a request for a directory, the web server response code indicates if it is a valid directory or not.

See Also

http://projects.webappsec.org/w/page/13246953/Predictable%20Resource%20Location

Solution

n/a

Risk Factor

None

References

XREF OWASP:OWASP-CM-006

Plugin Information

Published: 2002/06/26, Modified: 2021/08/17

Plugin Output

tcp/8080/www

```
The following directories were discovered:
/account, /error, /reports, /scripts, /uploads, /content

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

11032 - Web Server Directory Enumeration

Synopsis

It is possible to enumerate directories on the web server.

Description

This plugin attempts to determine the presence of various common directories on the remote web server. By sending a request for a directory, the web server response code indicates if it is a valid directory or not.

See Also

http://projects.webappsec.org/w/page/13246953/Predictable%20Resource%20Location

Solution

n/a

Risk Factor

None

References

XREF OWASP:OWASP-CM-006

Plugin Information

Published: 2002/06/26, Modified: 2021/08/17

Plugin Output

tcp/8082/www

```
The following directories were discovered:
/help, /src

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

10386 - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/04/28, Modified: 2022/06/17

Plugin Output

tcp/8080/www

```
The following string will be used :
404
```

10386 - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/04/28, Modified: 2022/06/17

Plugin Output

tcp/8082/www

```
The following title tag will be used :
H# th#ng thông tin
```

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: 2023/07/17

Plugin Output

tcp/80/www

```
Webmirror performed 19 queries in 1s (19.000 queries per second)

The following CGIs have been discovered :


+ CGI : /qlvbdh/main
  Methods : POST
  Argument : +4y9k5cbd5cbi5O..
   Value: CEt1CzAwJyLZ4dKlTFpi3ynl5ybk
  Argument : DEtvDzTlDcO.
  Argument : DcAv5B1aRzPm
   Value: 0
  Argument : DcAwT3HkRE9d6B0.
   Value: 0
  Argument : DyAu6BtiOyAuTEbc6BLXTES.
  Argument : DybdCcAaQEtv6o..
  Argument : DzAYCBbw
   Value: S# d#ng token
  Argument : T3LbDc1XCBS.
  Argument : TFXwRBt44BLM6Etk
```

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: 2023/07/17

Plugin Output

tcp/90/www

```
Webmirror performed 17 queries in 1s (17.000 queries per second)

The following CGIs have been discovered :


+ CGI : /cgi-bin/MANGA/connicon.cgi
  Methods : GET
  Argument : type
   Value: favicon


+ CGI : /cgi-bin/MANGA/index.cgi
  Methods : POST
  Argument : mode
   Value: submit
  Argument : option
   Value: login
  Argument : password
  Argument : username
```

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: 2023/07/17

Plugin Output

tcp/8080/www

```
Webmirror performed 75 queries in 4s (18.0750 queries per second)

The following CGIs have been discovered :


+ CGI : /Account/Login
  Methods : GET,POST
  Argument : ReturnURL
   Value: %2fdefault.aspx
  Argument : __EVENTARGUMENT
  Argument : __EVENTTARGET
  Argument : __EVENTVALIDATION
  Argument : __VIEWSTATE
  Argument : __VIEWSTATEGENERATOR
   Value: CD85D8D2
  Argument : ctl00$MainContent$btnDangnhap
   Value: ##ng nh#p
  Argument : ctl00$MainContent$txtName
  Argument : ctl00$MainContent$txtPassword


+ CGI : /error
  Methods : POST
  Argument : __VIEWSTATE
  Argument : __VIEWSTATEGENERATOR
   Value: AB827D4F
  Argument : search
```

```
+ CGI : /account/
  Methods : POST
  Argument : 403%3bhttp%3a%2f%2fqlvbdh.hungyen.dcs.vn%3a8080%2faccount%2f
  Argument : __VIEWSTATE
  Argument : __VIEWSTATEGENERATOR
   Value: B1F71293
  Argument : search


+ CGI : /content/
  Methods : POST
  Argument : 403%3bhttp%3a%2f%2fqlvbdh.hungyen.dcs.vn%3a8080%2fcontent%2f
  Argument : __VIEWSTATE
  Argument : __VIEWSTATEGENERATOR
   Value: B1F71293
  Argument : search


+ CGI : /uploads/
  Methods : POST
  Argument : 403%3bhttp%3a%2f%2fqlvbdh.hungyen.dcs.vn%3a8080%2fuploads%2f
  Argument : __VIEWSTATE
  Argument : __VIEWSTATEGENERATOR
   Value: B1F71293
  Argument : search


+ CGI : /scripts/
  Methods : POST
  Argument : 403%3bhttp%3a%2f%2fqlvbdh.hungyen.dcs.vn%3a8080%2fscripts%2f
  Argument : __VIEWSTATE
  Argument : __VIEWSTATEGENERATOR
   Value: B1F71293
  Argument : search


+ CGI : /reports/
  Methods : POST
  Argument : 403%3bhttp%3a%2f%2fqlvbdh.hungyen.dcs.vn%3a8080%2freports%2f
  Argument : __VIEWSTATE
  Argument : __VIEWSTATEGENERATOR
   Value: B1F71293
  Argument : search


+ CGI : /Account/
  Methods : POST
  Argument : 403%3bhttp%3a%2f%2fqlvbdh.hungyen.dcs.vn%3a8080%2fAccount%2f
  Argument : __VIEWSTATE
  Argument : __VIEWSTATEGENERATOR
   Value: B1F71293
  Argument : search


+ CGI : /Content/
  Methods : POST
  Argument : 403%3bhttp%3a%2f%2fqlvbdh.hungyen.dcs.vn%3a8080%2fContent%2f
  Argument : __VIEWSTATE
  Argume [...]
```

106375 - nginx HTTP Server Detection

Synopsis

The nginx HTTP server was detected on the remote host.

Description

Nessus was able to detect the nginx HTTP server by looking at the HTTP banner on the remote host.

See Also

https://nginx.org/

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0677

Plugin Information

Published: 2018/01/26, Modified: 2023/05/24

Plugin Output

tcp/80/www

```
URL     : http://qlvbdh.hungyen.dcs.vn/
Version : 1.12.2
source  : Server: nginx/1.12.2
```

106375 - nginx HTTP Server Detection

Synopsis

The nginx HTTP server was detected on the remote host.

Description

Nessus was able to detect the nginx HTTP server by looking at the HTTP banner on the remote host.

See Also

https://nginx.org/

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0677

Plugin Information

Published: 2018/01/26, Modified: 2023/05/24

Plugin Output

tcp/90/www

```
URL     : http://qlvbdh.hungyen.dcs.vn:90/
Version : 1.2.6
source  : Server: nginx/1.2.6
```