hungyen.dcs.vn

Report generated by Nessus™ Fri, 25 Aug 2023 09:52:32 +07

TABLE OF CONTENTS

Vulnerabilities by Host

- hungyen.dcs.vn..... 4

Vulnerabilities by Host

hungyen.dcs.vn

0	0	3	0	50
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Fri Aug 25 08:52:28 2023
End time: Fri Aug 25 09:51:37 2023

Host Information

DNS Name: hungyen.dcs.vn
IP: 113.160.132.24
OS: FortiOS on Fortinet FortiGate

Vulnerabilities

11411 - Backup Files Disclosure

Synopsis

It is possible to retrieve file backups from the remote web server.

Description

By appending various suffixes (ie: .old, .bak, ~, etc...) to the names of various files on the remote host, it seems possible to retrieve their contents, which may result in disclosure of sensitive information.

See Also

http://www.nessus.org/u?8f3302c6

Solution

Ensure the files do not contain any sensitive information, such as credentials to connect to a database, and delete or protect those files that should not be accessible.

Risk Factor

Medium

CVSS v2.0 Base Score

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

Plugin Information

Published: 2003/03/17, Modified: 2023/07/10

Plugin Output

tcp/443/www

```
It is possible to read the following backup file :

  - File : /logout~
    URL  : https://hungyen.dcs.vn/logout~
```

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/80/www

```
URL              : http://hungyen.dcs.vn/javascripts/jquery-1.9.1.min.js
Installed version : 1.9.1
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/80/www

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

  - http://hungyen.dcs.vn/
  - http://hungyen.dcs.vn/1-nguoi-o-thi-xa-my-hao-bi-bong-nang-do-su-dung-dien-thoai-trong-luc-sac-
pin-c29977.html
  - http://hungyen.dcs.vn/12-nhiem-vu-giai-phap-trong-tam-cua-nganh-giao-duc-thuc-hien-trong-nam-
hoc-moi-c210002.html
  - http://hungyen.dcs.vn/12-nhiem-vu-giai-phap-trong-tam-cua-nganh-giao-duc-thuc-hien-trong-nam-
hoc-moi-c210003.html
  - http://hungyen.dcs.vn/15-bi-can-bi-khoi-to-lien-quan-vu-thao-tung-thi-truong-chung-khoan-
c29059.html
  - http://hungyen.dcs.vn/161-xa-phuong-thi-tran-thuoc-tinh-hung-yen-c2362.html
  - http://hungyen.dcs.vn/235-hec-ta-dien-tich-mat-nuoc-nuoi-tha-thuy-san-c29876.html
  - http://hungyen.dcs.vn/6-thang-dau-nam-toan-tinh-xay-ra-71-vu-tai-nan-giao-thong-c28996.html
  - http://hungyen.dcs.vn/aipa-va-dau-an-cua-viet-nam-tai-cac-dien-dan-lien-nghi-vien-c29792.html
  - http://hungyen.dcs.vn/an-thi-ghi-nhan-tu-dien-tap-chien-dau-phong-thu-cum-xa-c29984.html
  - http://hungyen.dcs.vn/an-thi-san-sang-phong-chong-ung-noi-dong-c29733.html
  - http://hungyen.dcs.vn/an-tuong-doi-bong-da-nhi-dong-u11-tinh-hung-yen-c29906.html
  - http://hungyen.dcs.vn/ba-dong-luc-de-tang-truong-kinh-te-cao-hon-trong-nua-cuoi-nam-c29724.html
  - http://hungyen.dcs.vn/bai-1-thu-doan-moi-cua-cac-the-luc-thu-dich-xuyen-tac-bo-doi-cu-ho-
c29485.html
  - http://hungyen.dcs.vn/bai-2-bai-hoc-ve-su-tu-bo-nguyen-tac-tu-phe-binh-va-phe-binh-trong-dang-
c29069.html
  - http://hungyen.dcs.vn/bai-2-de-nghi-quyet-cua-dang-tiep-tuc-di-vao-cuoc-song-c25764.html
  - http://hungyen.dcs.vn/bai-2-trong-kho-khan-bo-doi-cu-ho-cang-toa-sang-c29486.html
  - http://hungyen.dcs.vn/ban-bi-thu-trung-uong-dang-thi-hanh-ky-luat-to-chuc-dang-dang-vien-
c29112.html
  - http://hungyen.dcs.vn/ban-can-su-dang-ubnd-tinh-va-cac-thanh-vien-ubnd-tinh-xem-xet-cho-y-kien-
mot-so-noi-dung-quan-trong-c29576.html
  - http://hungyen.dcs.vn/ban-can-su-dang-ubnd-tinh-va-cac-thanh-vien-ubnd-tinh-xem-xet-cho-y-kien-
ve-ti [...]
```

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 'ctl00$ContentPlaceHolder1$ctl00$ddl_linhvuc' parameter of the /cate.aspx?uc=4 CGI :

/cate.aspx?uc=4?ctl00$ContentPlaceHolder1$ctl00$ddl_linhvuc=pffrui

-------- output --------
<meta name="title" content="##ng b# T#nh H#ng Yên" /><met [...]
<body>
<form method="post" action="./cate.aspx?uc=4%3fctl00%24ContentPlaceHolde
r1%24ctl00%24ddl_linhvuc%3dpffrui" id="aspnetForm">
<div class="aspNetHidden">
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="w4 [...]
------------------------

+ The 'ctl00$ContentPlaceHolder1$ctl00$ddl_linhvuc' parameter of the /cate.aspx?uc=3&page=1 CGI :
```

```
/cate.aspx?uc=3&page=1?ctl00$ContentPlaceHolder1$ctl00$ddl_linhvuc=pffru
i

-------- output --------
<meta name="title" content="##ng b# T#nh H#ng Yên" /><met [...]
<body>
<form method="post" action="./cate.aspx?uc=3&amp;page=1%3fctl00%24Conten
tPlaceHolder1%24ctl00%24ddl_linhvuc%3dpffrui" id="aspnetForm">
<div class="aspNetHidden">
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
------------------------

+ The 'ctl00$ContentPlaceHolder1$ctl00$ddlcap' parameter of the /cate_no_right.aspx?
uc=1&cateid=21&id=21 CGI :

/cate_no_right.aspx?uc=1&cateid=21&id=21?ctl00$ContentPlaceHolder1$ctl00
$ddlcap=pffrui

-------- output --------
</head>
<body>
<form method="post" action="./cate_no_right.aspx?uc=1&amp;cateid=21&amp;
id=21%3fctl00%24ContentPlaceHolder1%24ctl00%24ddlcap%3dpffrui" id="aspne
tForm">
<div class="aspNetHidden">
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
------------------------

+ The 'ctl00$ContentPlaceHolder1$ctl00$ddlcap' parameter of the /cate_no_right.aspx?
uc=1&cateid=22&id=22 CGI :

/cate_no_right.aspx?uc=1&cateid=22&id=22?ctl00$ContentPlaceHolder1$ctl00
$ddlcap=pffrui

-------- output --------
</head>
<body>
<form method="post" action="./cate_no_right.aspx?uc=1&amp;cateid=22&amp;
id=22%3fctl00%24ContentPlaceHolder1% [...]
```

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=145        SP=145       AP=145       SC=145
 AC=145
SQL injection                           : S=8256       SP=8256      AP=20976     SC=48
 AC=12256224
unseen parameters                       : S=12040      SP=12040     AP=30590     SC=70
 AC=17873660
local file inclusion                    : S=344        SP=344       AP=874       SC=2
 AC=510676
web code injection                      : S=344        SP=344       AP=874       SC=2
 AC=510676
XML injection                           : S=344        SP=344       AP=874       SC=2
 AC=510676
format string                           : S=688        SP=688       AP=1748      SC=4
 AC=1021352
script injection                        : S=145        SP=145       AP=145       SC=145
 AC=145
cross-site scripting (comprehensive test): S=1376       SP=1376      AP=3496      SC=8
 AC=2042704
```

```
injectable parameter                     : S=688        SP=688       AP=1748      SC=4
 AC=1021352
cross-site scripting (extended patterns) : S=870        SP=870       AP=870       SC=870
 AC=870
directory traversal (write access)       : S=688        SP=688       AP=1748      SC=4
 AC=1021352
SSI injection                            : S=1032       SP=1032      AP=2622      SC=6
 AC=1532028
header injection                         : S=290        SP=290       AP=290       SC=290
 AC=290
directory traversal                      : S=8600       SP=8600      AP=21850     SC=50
 AC=12766900
HTML injection                           : S=725        SP=725       AP=725       SC=725
 AC=725
arbitrary command execution (time based) : S=2064       SP=2064      AP=5244      SC=12
 AC=3064056
persistent XSS                          [...]
```

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/443/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]

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

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

cross-site scripting (comprehensive test): S=4          SP=4         AP=4         SC=4         AC=4

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

arbitrary command execution              : S=16         SP=16        AP=16        SC=16        AC=16

directory traversal (extended test)      : S=51         SP=51        AP=51        SC=51        AC=51

local file inclusion                     : S=1          SP=1         AP=1         SC=1         AC=1

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

SQL injection                            : S=24         SP=24        AP=24        SC=24        AC=24
```

```
unseen parameters                       : S=35          SP=35          AP=35          SC=35          AC=35
directory traversal (write access)      : S=2           SP=2           AP=2           SC=2           AC=2
format string                           : S=2           SP=2           AP=2           SC=2           AC=2
XML injection                           : S=1           SP=1           AP=1           SC=1           AC=1
directory traversal                     : S=25          SP=25          AP=25          SC=25          AC=25
persistent XSS                          : S=4           SP=4           AP=4           SC=4           AC=4
SSI injection                           : S=3           SP=3           AP=3           SC=3           AC=3
SQL injection (2nd order)               : S=1           SP=1           AP=1           SC=1           AC=1
blind SQL injection                   [...]
```

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/8443/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]

directory traversal                       : S=25         SP=25        AP=25        SC=25        AC=25

SQL injection (2nd order)                 : S=1          SP=1         AP=1         SC=1         AC=1

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

SSI injection                             : S=3          SP=3         AP=3         SC=3         AC=3

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

local file inclusion                      : S=1          SP=1         AP=1         SC=1         AC=1

arbitrary command execution               : S=16         SP=16        AP=16        SC=16        AC=16

XML injection                             : S=1          SP=1         AP=1         SC=1         AC=1

cross-site scripting (comprehensive test): S=4          SP=4         AP=4         SC=4         AC=4
```

```
directory traversal (extended test)      : S=51          SP=51          AP=51          SC=51          AC=51
arbitrary command execution (time based) : S=6           SP=6           AP=6           SC=6           AC=6
SQL injection                            : S=24          SP=24          AP=24          SC=24          AC=24
unseen parameters                        : S=35          SP=35          AP=35          SC=35          AC=35
format string                            : S=2           SP=2           AP=2           SC=2           AC=2
persistent XSS                           : S=4           SP=4           AP=4           SC=4           AC=4
web code injection                       : S=1           SP=1           AP=1           SC=1           AC=1
blind SQL injection                      : S=12          SP=12          AP=12          SC=12          AC=12
directory traversal (write access)     [...]
```

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 :
- web code injection
- SQL injection (on parameters names)
- SQL injection
- cross-site scripting (extended patterns)
- uncontrolled redirection
- cross-site scripting (comprehensive test)
- XSS (on parameters names)
- local file inclusion
- blind SQL injection
- blind SQL injection (time based)
- SQL injection (2nd order)
```

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/443/www

```
The following tests timed out without finding any flaw :
- blind SQL injection (time based)
- blind SQL injection
- XSS (on parameters names)
- SQL injection (on parameters names)
```

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

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


http://anthi.hungyen.dcs.vn             - /
http://ccb.hungyen.dcs.vn               - /
http://congan.hungyen.gov.vn/tintuc/tintuc03/wp-includes/css/dashicons.min.css?ver=4.4.2 - /
http://csdl.thutuchanhchinh.vn/dms/content/view/full/568463 - /cate-thu-tuc-hc-tt2-21.html
http://danvan.hungyen.dcs.vn            - /
http://dukcq.hungyen.dcs.vn             - /
http://khoaichau.hungyen.dcs.vn         - /
http://kimdong.hungyen.dcs.vn           - /
http://ldld.hungyen.dcs.vn              - /
http://mail1.hungyen.gov.vn/Names.nsf?Login&RedirectTo=/webmail.nsf/OpenMailFile.xsp - /
http://mttq.hungyen.dcs.vn              - /
http://myhao.hungyen.dcs.vn             - /
http://noichinh.hungyen.dcs.vn          - /
http://nongdan.hungyen.dcs.vn           - /
http://phucu.hungyen.dcs.vn/            - /
http://phunu.hungyen.dcs.vn             - /
http://qlvbdh.hungyen.dcs.vn/qlvbdh/main?lang=vi - /
http://thanhuy.hungyen.dcs.vn           - /
http://tienlu.hungyen.dcs.vn            - /
http://tinhdoan.hungyen.dcs.vn          - /
http://tochuc.hungyen.dcs.vn            - /
http://tuyengiao.hungyen.dcs.vn         - /
http://ubkt.hungyen.dcs.vn              - /
http://vangiang.hungyen.dcs.vn          - /
http://vanlam.hungyen.dcs.vn            - /
http://vi.wikipedia.org/w/index.php?title=Gi%C3%A1o_l%C3%BD&action=edit&redlink=1 - /huong-dan-chi-
tiet-chuyen-de-van-de-ton-giao-va-chinh-sach-ton-giao-c2319.html
```

```
http://vi.wikipedia.org/w/index.php?title=Kinh_%C4%91i%E1%BB%83n&action=edit&redlink=1 - /huong-dan-
chi-tiet-chuyen-de-van-de-ton-giao-va-chinh-sach-ton-giao-c2319.html
http://vi.wikipedia.org/w/index.php?title=T%C3%ADnh_ch%E1%BA%A5t_d%C3%A2n_gian&action=edit&redlink=1
 - /huong-dan-chi-tiet-chuyen-de-van-de-ton-giao-va-chinh-sach-ton-giao-c2319.html
http://vi.wikipedia.org/w/index.php?title=Th%C3%A1nh_%C4%91%C6%B0%E1%BB%9Dng&action=edit&redlink=1
 - /huong-dan-chi-tiet-chuyen-de-van-de-ton-giao-va-chinh-sach-ton-giao-c231 [...]
```

17367 - Fortinet FortiGate Web Console Management Detection

Synopsis

A firewall management console is running on the remote host.

Description

A Fortinet FortiGate Firewall is running on the remote host, and connections are allowed to its web-based console management port.

Letting attackers know that you are using this software will help them to focus their attack or will make them change their strategy. In addition to this, an attacker may set up a brute-force attack against the remote interface.

See Also

https://www.fortinet.com/products/fortigate/

Solution

Filter incoming traffic to this port.

Risk Factor

None

Plugin Information

Published: 2005/03/18, Modified: 2023/07/18

Plugin Output

tcp/443/www

```
The following instance of FortiOS Web Interface was detected on the remote host :

  Version : >= 5.4
  URL     : https://hungyen.dcs.vn/
```

84502 - HSTS Missing From HTTPS Server

Synopsis

The remote web server is not enforcing HSTS.

Description

The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

See Also

https://tools.ietf.org/html/rfc6797

Solution

Configure the remote web server to use HSTS.

Risk Factor

None

Plugin Information

Published: 2015/07/02, Modified: 2021/05/19

Plugin Output

tcp/8443/www

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

69826 - HTTP Cookie 'secure' Property Transport Mismatch

Synopsis

The remote web server sent out a cookie with a secure property that does not match the transport on which it was sent.

Description

The remote web server sends out cookies to clients with a 'secure'

property that does not match the transport, HTTP or HTTPS, over which they were received. This may occur in two forms :

1. The cookie is sent over HTTP, but has the 'secure'

property set, indicating that it should only be sent over a secure, encrypted transport such as HTTPS.

This should not happen.

2. The cookie is sent over HTTPS, but has no 'secure'

property set, indicating that it may be sent over both HTTP and HTTPS transports. This is common, but care should be taken to ensure that the 'secure' property not being set is deliberate.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/09/10, Modified: 2021/12/20

Plugin Output

tcp/443/www

```
The following cookie does not have the 'secure' property enabled, despite being served over HTTPS :

  Domain   :
  Path     : /
  Name     : ASP.NET_SessionId
  Value    : mfwwkki5qbku3uvf20zx3eqh
  Secure   : false
  HttpOnly : true
```

69826 - HTTP Cookie 'secure' Property Transport Mismatch

Synopsis

The remote web server sent out a cookie with a secure property that does not match the transport on which it was sent.

Description

The remote web server sends out cookies to clients with a 'secure'

property that does not match the transport, HTTP or HTTPS, over which they were received. This may occur in two forms :

1. The cookie is sent over HTTP, but has the 'secure'

property set, indicating that it should only be sent over a secure, encrypted transport such as HTTPS.

This should not happen.

2. The cookie is sent over HTTPS, but has no 'secure'

property set, indicating that it may be sent over both HTTP and HTTPS transports. This is common, but care should be taken to ensure that the 'secure' property not being set is deliberate.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/09/10, Modified: 2021/12/20

Plugin Output

tcp/8443/www

```
The following cookie does not have the 'secure' property enabled, despite being served over HTTPS :

  Domain   :
  Path     : /
  Name     : ASP.NET_SessionId
  Value    : mfwwkki5qbku3uvf20zx3eqh
  Secure   : false
  HttpOnly : true
```

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 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 :

    /
    /Images
    /ckfinder
    /ckfinder/userfiles
    /ckfinder/userfiles/files
    /ckfinder/userfiles/files/bantinnoino
    /ckfinder/userfiles/images
    /ckfinder/userfiles/images/Ban%20tin%20315
    /ckfinder/userfiles/images/Ban%20tin%20315/Ban%20tin316
    /ckfinder/userfiles/images/bantinchibo
    /ckfinder/userfiles/images/bantinchibo/bantinso1
    /ckfinder/userfiles/images/bantinchibo/so%20314
    /cms
    /cms/assets
    /cms/assets/css
    /css
    /css-js

  - Invalid/unknown HTTP methods are allowed on :

    /
    /Images
    /ckfinder
    /ckfinder/userfiles
    /ckfinder/userfiles/files
    /ckfinder/userfiles/files/bantinnoino
    /ckfinder/userfiles/images
    /ckfinder/userfiles/images/Ban%20tin%20315
    /ckfinder/userfiles/images/Ban%20tin%20315/Ban%20tin316
    /ckfinder/userfiles/images/bantinchibo
    /ckfinder/userfiles/images/bantinchibo/bantinso1
    /ckfinder/userfiles/images/bantinchibo/so%20314
    /cms
    /cms/assets
    /cms/assets/css
    /css
    /css-js
```

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/443/www

```
Based on tests of each method :
  - HTTP methods DELETE GET are allowed on :
    /dfc7d243c39529351a844cd6af29d8d0
  - HTTP methods DELETE GET OPTIONS POST PUT 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/8080/www

```
Based on tests of each method :
  - HTTP methods GET HEAD OPTIONS 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/8443/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 UNCHECKOUT UNLOCK
    UNSUBSCRIBE UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on :

    /manage
    /manage/account

  - HTTP methods GET HEAD OPTIONS POST are allowed on :

    /

  - Invalid/unknown HTTP methods are allowed on :

    /manage
    /manage/account
```

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 :

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/1.1 200 OK

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
  Server: Microsoft-IIS/10.0
  X-Powered-By: UrlRewriter.NET 1.7.0
  X-AspNet-Version: 4.0.30319
  X-Powered-By: ASP.NET
  X-UA-Compatible: IE=8
  Date: Fri, 25 Aug 2023 09:47:10 GMT
  Content-Length: 138614

Response Body :

<!DOCTYPE html>
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
    <script src="https://apis.google.com/js/platform.js" async defer></script>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8" /><title>
##ng b# T#nh H#ng Yên
```

```
</title><link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/
font-awesome.min.css" /><meta name="viewport" content="width=device-width, initial-scale=1, maximum-
scale=1" /><meta name="DC.Language" content="vi-vn" /><meta name="DC.Description" content="##ng
 b# t#nh H#ng Yên" /><meta name="DC.Title" content="##ng b# t#nh H#ng Yên, DANG BO TINH HUNG
 YEN" /><meta name="DC.Identifier" content="/" /><meta name="geo.region" content="VN-33" /><meta
 name="geo.placename" content="V#n phòng T#nh #y H#ng Yên - S# 12 ###ng Chùa Chuông - Ph##ng Hi#n
 Nam - Thành Ph# H#ng Yên" /><meta charset="utf-8" /><meta content="text/html;charset=utf-8" http-
equiv="Content-Type" /><meta content="vi" http-equiv="Content-Language" /><meta content="100"
 name="MobileOptimized" /><meta content="yes" name="apple-mobile-web-app-capsable" /><meta
 http-equiv="X-UA-Compatible" content="IE=edge" /><meta name="viewport" content="width=device-
width, initial-scale=1" /><link href="./Images/images.png" rel="icon" /><link href="css/
bootstrap-3.3.6/css/bootstrap.min.css" rel="stylesheet" /><link href="css/font-awesome-4.5.0/css/
font-awesome.min.css" rel="stylesheet" /><link href="css/congdoanvn.css" rel="stylesheet" /><link
 href="css/newslist.css" rel="stylesheet" /><link href="css/jqu [...]
```

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/443/www

```
Response Code : HTTP/1.1 200 OK

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

  Content-Encoding: gzip
  Content-Type: text/html
  ETag: dfc7d243c39529351a844cd6af29d8d0
  X-Frame-Options: SAMEORIGIN
  Content-Security-Policy: frame-ancestors 'self'
  X-XSS-Protection: 1; mode=block
  Strict-Transport-Security: max-age=15552000
  Date: Fri, 25 Aug 2023 02:06:03 GMT
  Connection: keep-alive
  Transfer-Encoding: chunked

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/8080/www

```
Response Code : HTTP/1.1 302

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : yes
Options allowed : GET, HEAD, POST, PUT, DELETE, OPTIONS
Headers :

  Location: /manage
  Content-Length: 0
  Date: Fri, 25 Aug 2023 01:47:17 GMT
  Keep-Alive: timeout=5
  Connection: keep-alive

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/8443/www

```
Response Code : HTTP/1.1 302

Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : yes
Options allowed : GET, HEAD, POST, PUT, DELETE, OPTIONS
Headers :

  Location: /manage
  Content-Length: 0
  Date: Fri, 25 Aug 2023 01:47:17 GMT
  Keep-Alive: timeout=60
  Connection: keep-alive

Response Body :
```

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://hungyen.dcs.vn:8080/
  HTTP response   : HTTP/1.1 302
  Redirect to     : http://hungyen.dcs.vn:8080/manage
  Redirect type   : 30x redirect

  Request         : http://hungyen.dcs.vn:8080/manage
  HTTP response   : HTTP/1.1 302
  Redirect to     : https://hungyen.dcs.vn:8443/manage
  Redirect type   : 30x redirect


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

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/8443/www

```
Request         : https://hungyen.dcs.vn:8443/
HTTP response   : HTTP/1.1 302
Redirect to     : https://hungyen.dcs.vn:8443/manage
Redirect type   : 30x redirect

Request         : https://hungyen.dcs.vn:8443/manage
HTTP response   : HTTP/1.1 302
Redirect to     : https://hungyen.dcs.vn:8443/manage/account/login?redirect=%2Fmanage
Redirect type   : 30x redirect

Final page      : https://hungyen.dcs.vn:8443/manage/account/login?redirect=%2Fmanage
HTTP response   : HTTP/1.1 200
```

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/80/www

```
URL     : http://hungyen.dcs.vn/javascripts/jquery-1.9.1.min.js
Version : 1.9.1
```

24242 - Microsoft .NET Handlers Enumeration

Synopsis

It is possible to enumerate the remote .NET handlers used by the remote web server.

Description

It is possible to obtain the list of handlers the remote ASP.NET web server supports.

See Also

https://support.microsoft.com/en-us/help/815145

Solution

None

Risk Factor

None

Plugin Information

Published: 2007/01/26, Modified: 2018/11/15

Plugin Output

tcp/80/www

```
The remote extensions are handled by the remote ASP.NET server :

 - .rem
 - .soap
```

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://hungyen.dcs.vn/
  - http://hungyen.dcs.vn/1-nguoi-o-thi-xa-my-hao-bi-bong-nang-do-su-dung-dien-thoai-trong-luc-sac-
pin-c29977.html
  - http://hungyen.dcs.vn/12-nhiem-vu-giai-phap-trong-tam-cua-nganh-giao-duc-thuc-hien-trong-nam-
hoc-moi-c210002.html
  - http://hungyen.dcs.vn/12-nhiem-vu-giai-phap-trong-tam-cua-nganh-giao-duc-thuc-hien-trong-nam-
hoc-moi-c210003.html
  - http://hungyen.dcs.vn/15-bi-can-bi-khoi-to-lien-quan-vu-thao-tung-thi-truong-chung-khoan-
c29059.html
  - http://hungyen.dcs.vn/161-xa-phuong-thi-tran-thuoc-tinh-hung-yen-c2362.html
  - http://hungyen.dcs.vn/235-hec-ta-dien-tich-mat-nuoc-nuoi-tha-thuy-san-c29876.html
```

```
  - http://hungyen.dcs.vn/6-thang-dau-nam-toan-tinh-xay-ra-71-vu-tai-nan-giao-thong-c28996.html
  - http://hungyen.dcs.vn/aipa-va-dau-an-cua-viet-nam-tai-cac-dien-dan-lien-nghi-vien-c29792.html
  - http://hungyen.dcs.vn/an-thi-ghi-nhan-tu-dien-tap-chien-dau-phong-thu-cum-xa-c29984.html
  - http://hungyen.dcs.vn/an-thi-san-sang-phong-chong-ung-noi-dong-c29733.html
  - http://hungyen.dcs.vn/an-tuong-doi-bong-da-nhi-dong-u11-tinh-hung-yen-c29906.html
  - http://hungyen.dcs.vn/ba-dong-luc-de-tang-truong-kinh-te-cao-hon-trong-nua-cuoi-nam-c29724.html
  - http://hungyen.dcs.vn/bai-1-thu-doan-moi-cua-cac-the-luc-thu-dich-xuyen-tac-bo-doi-cu-ho-
c29485.html
  - http://hungyen.dcs.vn/bai-2-bai-hoc-ve-su-tu-bo-nguyen-tac-tu-phe-binh-va-phe-binh-trong-dang-
c29069.html
  - http://hungyen.dcs.vn/bai-2-de-nghi-quyet-cua-dang-tiep-tuc-di-vao-cuoc-song-c25764.html
  - http://hungyen.dcs.vn/bai-2-trong-kho-khan-bo-doi-cu-ho-cang-toa-sang-c29486.html
  - http://hungyen.dcs.vn/ban-bi-thu-trung-uong-dang-thi-hanh-ky-luat-to-chuc-dang-dang-vien-
c29112.html
  - http://hungyen.dcs.vn/ban-can-su-dang-ubnd-tinh-va-cac-thanh-vien-ubnd-tinh-xem-xet-cho-y-kien-
mot-so-noi-dung-quan-trong-c29576.html
  - http://hungyen.dcs.vn/ban-can-su-dang-ubnd-tinh-va-cac-thanh-vien-ubnd-tinh-xem-xet-cho- [...]
```

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/8443/www

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

  - https://hungyen.dcs.vn:8443/manage/account/login
```

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

Synopsis

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

Description

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

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

See Also

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

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/80/www

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

  - http://hungyen.dcs.vn/
  - http://hungyen.dcs.vn/1-nguoi-o-thi-xa-my-hao-bi-bong-nang-do-su-dung-dien-thoai-trong-luc-sac-
pin-c29977.html
  - http://hungyen.dcs.vn/12-nhiem-vu-giai-phap-trong-tam-cua-nganh-giao-duc-thuc-hien-trong-nam-
hoc-moi-c210002.html
  - http://hungyen.dcs.vn/12-nhiem-vu-giai-phap-trong-tam-cua-nganh-giao-duc-thuc-hien-trong-nam-
hoc-moi-c210003.html
  - http://hungyen.dcs.vn/15-bi-can-bi-khoi-to-lien-quan-vu-thao-tung-thi-truong-chung-khoan-
c29059.html
  - http://hungyen.dcs.vn/161-xa-phuong-thi-tran-thuoc-tinh-hung-yen-c2362.html
  - http://hungyen.dcs.vn/235-hec-ta-dien-tich-mat-nuoc-nuoi-tha-thuy-san-c29876.html
  - http://hungyen.dcs.vn/6-thang-dau-nam-toan-tinh-xay-ra-71-vu-tai-nan-giao-thong-c28996.html
  - http://hungyen.dcs.vn/aipa-va-dau-an-cua-viet-nam-tai-cac-dien-dan-lien-nghi-vien-c29792.html
  - http://hungyen.dcs.vn/an-thi-ghi-nhan-tu-dien-tap-chien-dau-phong-thu-cum-xa-c29984.html
  - http://hungyen.dcs.vn/an-thi-san-sang-phong-chong-ung-noi-dong-c29733.html
  - http://hungyen.dcs.vn/an-tuong-doi-bong-da-nhi-dong-u11-tinh-hung-yen-c29906.html
```

```
  - http://hungyen.dcs.vn/ba-dong-luc-de-tang-truong-kinh-te-cao-hon-trong-nua-cuoi-nam-c29724.html
  - http://hungyen.dcs.vn/bai-1-thu-doan-moi-cua-cac-the-luc-thu-dich-xuyen-tac-bo-doi-cu-ho-
c29485.html
  - http://hungyen.dcs.vn/bai-2-bai-hoc-ve-su-tu-bo-nguyen-tac-tu-phe-binh-va-phe-binh-trong-dang-
c29069.html
  - http://hungyen.dcs.vn/bai-2-de-nghi-quyet-cua-dang-tiep-tuc-di-vao-cuoc-song-c25764.html
  - http://hungyen.dcs.vn/bai-2-trong-kho-khan-bo-doi-cu-ho-cang-toa-sang-c29486.html
  - http://hungyen.dcs.vn/ban-bi-thu-trung-uong-dang-thi-hanh-ky-luat-to-chuc-dang-dang-vien-
c29112.html
  - http://hungyen.dcs.vn/ban-can-su-dang-ubnd-tinh-va-cac-thanh-vien-ubnd-tinh-xem-xet-cho-y-kien-
mot-so-noi-dung-quan-trong-c29576.html
  - http://hungyen.dcs.vn/ban-can-su-dang-ubnd-tinh-va-cac-thanh-vien-ubnd-tinh-xem-xet-cho-y-kien-
ve-tien-do-lap-th [...]
```

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/443/www

```
Port 443/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/541

```
Port 541/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/8443/www

```
Port 8443/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 : 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 : 12.548 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 8:52 +07
Scan duration : 3219 sec
Scan for malware : no
```

100669 - Web Application Cookies Are Expired

Synopsis

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

Description

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

See Also

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

Solution

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

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

Risk Factor

None

Plugin Information

Published: 2017/06/07, Modified: 2021/12/20

Plugin Output

tcp/80/www

```
The following cookies are expired :

Name : ccsrftoken_8890982948028592682
Path : /
Value : "0%260"
Domain :
Version : 1
Expires : Thu, 06-Sep-1973 02:06:22 GMT
Comment :
Secure : 1
Httponly : 0
Port :


Name : CENTRAL_MGMT_OVERRIDE_8890982948028592682
Path : /
Value : "0%260"
```

```
Domain :
Version : 1
Expires : Thu, 06-Sep-1973 02:06:22 GMT
Comment :
Secure : 1
Httponly : 0
Port :


Name : ccsrftoken
Path : /
Value : "0%260"
Domain :
Version : 1
Expires : Thu, 06-Sep-1973 02:06:22 GMT
Comment :
Secure : 1
Httponly : 0
Port :


Name : APSCOOKIE_8890982948028592682
Path : /
Value : "0%260"
Domain :
Version : 1
Expires : Thu, 06-Sep-1973 02:06:22 GMT
Comment :
Secure : 1
Httponly : 0
Port :


Name : AUTOSCALE_CONFIG_REC_OVERRIDE_8890982948028592682
Path : /
Value : "0%260"
Domain :
Version : 1
Expires : Thu, 06-Sep-1973 02:06:22 GMT
Comment :
Secure : 1
Httponly : 0
Port :


Name : session_key_8890982948028592682
Path : /
Value : "0%260"
Domain :
Version : 1
Expires : Thu, 06-Sep-1973 02:06:22 GMT
Comment :
Secure : 1
Httponly : 0
Port :


Name : FILE_DOWNLOADING_8890982948028592682
Path : /
Value : "0%260"
Domain :
Version : 1
Expires : Thu, 06-Sep-1973 02:06:22 GMT
Comment :
Secure : 1
Httponly : 0
Port :
```

100669 - Web Application Cookies Are Expired

Synopsis

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

Description

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

See Also

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

Solution

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

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

Risk Factor

None

Plugin Information

Published: 2017/06/07, Modified: 2021/12/20

Plugin Output

tcp/443/www

```
The following cookies are expired :

Name : ccsrftoken_8890982948028592682
Path : /
Value : "0%260"
Domain :
Version : 1
Expires : Thu, 06-Sep-1973 02:06:22 GMT
Comment :
Secure : 1
Httponly : 0
Port :


Name : CENTRAL_MGMT_OVERRIDE_8890982948028592682
Path : /
Value : "0%260"
```

```
Domain :
Version : 1
Expires : Thu, 06-Sep-1973 02:06:22 GMT
Comment :
Secure : 1
Httponly : 0
Port :


Name : ccsrftoken
Path : /
Value : "0%260"
Domain :
Version : 1
Expires : Thu, 06-Sep-1973 02:06:22 GMT
Comment :
Secure : 1
Httponly : 0
Port :


Name : APSCOOKIE_8890982948028592682
Path : /
Value : "0%260"
Domain :
Version : 1
Expires : Thu, 06-Sep-1973 02:06:22 GMT
Comment :
Secure : 1
Httponly : 0
Port :


Name : AUTOSCALE_CONFIG_REC_OVERRIDE_8890982948028592682
Path : /
Value : "0%260"
Domain :
Version : 1
Expires : Thu, 06-Sep-1973 02:06:22 GMT
Comment :
Secure : 1
Httponly : 0
Port :


Name : session_key_8890982948028592682
Path : /
Value : "0%260"
Domain :
Version : 1
Expires : Thu, 06-Sep-1973 02:06:22 GMT
Comment :
Secure : 1
Httponly : 0
Port :


Name : FILE_DOWNLOADING_8890982948028592682
Path : /
Value : "0%260"
Domain :
Version : 1
Expires : Thu, 06-Sep-1973 02:06:22 GMT
Comment :
Secure : 1
Httponly : 0
Port :
```

100669 - Web Application Cookies Are Expired

Synopsis

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

Description

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

See Also

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

Solution

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

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

Risk Factor

None

Plugin Information

Published: 2017/06/07, Modified: 2021/12/20

Plugin Output

tcp/8080/www

```
The following cookies are expired :

Name : ccsrftoken_8890982948028592682
Path : /
Value : "0%260"
Domain :
Version : 1
Expires : Thu, 06-Sep-1973 02:06:22 GMT
Comment :
Secure : 1
Httponly : 0
Port :


Name : CENTRAL_MGMT_OVERRIDE_8890982948028592682
Path : /
Value : "0%260"
```

```
Domain :
Version : 1
Expires : Thu, 06-Sep-1973 02:06:22 GMT
Comment :
Secure : 1
Httponly : 0
Port :


Name : ccsrftoken
Path : /
Value : "0%260"
Domain :
Version : 1
Expires : Thu, 06-Sep-1973 02:06:22 GMT
Comment :
Secure : 1
Httponly : 0
Port :


Name : APSCOOKIE_8890982948028592682
Path : /
Value : "0%260"
Domain :
Version : 1
Expires : Thu, 06-Sep-1973 02:06:22 GMT
Comment :
Secure : 1
Httponly : 0
Port :


Name : AUTOSCALE_CONFIG_REC_OVERRIDE_8890982948028592682
Path : /
Value : "0%260"
Domain :
Version : 1
Expires : Thu, 06-Sep-1973 02:06:22 GMT
Comment :
Secure : 1
Httponly : 0
Port :


Name : session_key_8890982948028592682
Path : /
Value : "0%260"
Domain :
Version : 1
Expires : Thu, 06-Sep-1973 02:06:22 GMT
Comment :
Secure : 1
Httponly : 0
Port :


Name : FILE_DOWNLOADING_8890982948028592682
Path : /
Value : "0%260"
Domain :
Version : 1
Expires : Thu, 06-Sep-1973 02:06:22 GMT
Comment :
Secure : 1
Httponly : 0
Port :
```

100669 - Web Application Cookies Are Expired

Synopsis

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

Description

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

See Also

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

Solution

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

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

Risk Factor

None

Plugin Information

Published: 2017/06/07, Modified: 2021/12/20

Plugin Output

tcp/8443/www

```
The following cookies are expired :

Name : ccsrftoken_8890982948028592682
Path : /
Value : "0%260"
Domain :
Version : 1
Expires : Thu, 06-Sep-1973 02:06:22 GMT
Comment :
Secure : 1
Httponly : 0
Port :


Name : CENTRAL_MGMT_OVERRIDE_8890982948028592682
Path : /
Value : "0%260"
```

```
Domain :
Version : 1
Expires : Thu, 06-Sep-1973 02:06:22 GMT
Comment :
Secure : 1
Httponly : 0
Port :


Name : ccsrftoken
Path : /
Value : "0%260"
Domain :
Version : 1
Expires : Thu, 06-Sep-1973 02:06:22 GMT
Comment :
Secure : 1
Httponly : 0
Port :


Name : APSCOOKIE_8890982948028592682
Path : /
Value : "0%260"
Domain :
Version : 1
Expires : Thu, 06-Sep-1973 02:06:22 GMT
Comment :
Secure : 1
Httponly : 0
Port :


Name : AUTOSCALE_CONFIG_REC_OVERRIDE_8890982948028592682
Path : /
Value : "0%260"
Domain :
Version : 1
Expires : Thu, 06-Sep-1973 02:06:22 GMT
Comment :
Secure : 1
Httponly : 0
Port :


Name : session_key_8890982948028592682
Path : /
Value : "0%260"
Domain :
Version : 1
Expires : Thu, 06-Sep-1973 02:06:22 GMT
Comment :
Secure : 1
Httponly : 0
Port :


Name : FILE_DOWNLOADING_8890982948028592682
Path : /
Value : "0%260"
Domain :
Version : 1
Expires : Thu, 06-Sep-1973 02:06:22 GMT
Comment :
Secure : 1
Httponly : 0
Port :
```

85602 - Web Application Cookies Not Marked Secure

Synopsis

HTTP session cookies might be transmitted in cleartext.

Description

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

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

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

See Also

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

Solution

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

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

Risk Factor

None

References

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

Plugin Information

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

Plugin Output

tcp/80/www

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

Name : ASP.NET_SessionId
Path : /
Value : mfwwkki5qbku3uvf20zx3eqh
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/443/www

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

Name : ASP.NET_SessionId
Path : /
Value : mfwwkki5qbku3uvf20zx3eqh
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 cookie does not set the secure cookie flag :

Name : ASP.NET_SessionId
Path : /
Value : mfwwkki5qbku3uvf20zx3eqh
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/8443/www

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

Name : ASP.NET_SessionId
Path : /
Value : mfwwkki5qbku3uvf20zx3eqh
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/80/www

```
Potentially sensitive parameters for CGI /detail.aspx :

id : Potential horizontal or vertical privilege escalation

Potentially sensitive parameters for CGI /cate_no_right.aspx :

id : Potential horizontal or vertical privilege escalation
```

91815 - Web Application Sitemap

Synopsis

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

Description

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/80/www

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

  - http://hungyen.dcs.vn/
  - http://hungyen.dcs.vn/1-nguoi-o-thi-xa-my-hao-bi-bong-nang-do-su-dung-dien-thoai-trong-luc-sac-
pin-c29977.html
  - http://hungyen.dcs.vn/12-nhiem-vu-giai-phap-trong-tam-cua-nganh-giao-duc-thuc-hien-trong-nam-
hoc-moi-c210002.html
  - http://hungyen.dcs.vn/12-nhiem-vu-giai-phap-trong-tam-cua-nganh-giao-duc-thuc-hien-trong-nam-
hoc-moi-c210003.html
  - http://hungyen.dcs.vn/15-bi-can-bi-khoi-to-lien-quan-vu-thao-tung-thi-truong-chung-khoan-
c29059.html
  - http://hungyen.dcs.vn/161-xa-phuong-thi-tran-thuoc-tinh-hung-yen-c2362.html
  - http://hungyen.dcs.vn/235-hec-ta-dien-tich-mat-nuoc-nuoi-tha-thuy-san-c29876.html
  - http://hungyen.dcs.vn/6-thang-dau-nam-toan-tinh-xay-ra-71-vu-tai-nan-giao-thong-c28996.html
  - http://hungyen.dcs.vn/Images/images.png
  - http://hungyen.dcs.vn/aipa-va-dau-an-cua-viet-nam-tai-cac-dien-dan-lien-nghi-vien-c29792.html
  - http://hungyen.dcs.vn/an-thi-ghi-nhan-tu-dien-tap-chien-dau-phong-thu-cum-xa-c29984.html
  - http://hungyen.dcs.vn/an-thi-san-sang-phong-chong-ung-noi-dong-c29733.html
  - http://hungyen.dcs.vn/an-tuong-doi-bong-da-nhi-dong-u11-tinh-hung-yen-c29906.html
  - http://hungyen.dcs.vn/ba-dong-luc-de-tang-truong-kinh-te-cao-hon-trong-nua-cuoi-nam-c29724.html
  - http://hungyen.dcs.vn/bai-1-thu-doan-moi-cua-cac-the-luc-thu-dich-xuyen-tac-bo-doi-cu-ho-
c29485.html
  - http://hungyen.dcs.vn/bai-2-bai-hoc-ve-su-tu-bo-nguyen-tac-tu-phe-binh-va-phe-binh-trong-dang-
c29069.html
```

```
  - http://hungyen.dcs.vn/bai-2-de-nghi-quyet-cua-dang-tiep-tuc-di-vao-cuoc-song-c25764.html
  - http://hungyen.dcs.vn/bai-2-trong-kho-khan-bo-doi-cu-ho-cang-toa-sang-c29486.html
  - http://hungyen.dcs.vn/ban-bi-thu-trung-uong-dang-thi-hanh-ky-luat-to-chuc-dang-dang-vien-
c29112.html
  - http://hungyen.dcs.vn/ban-can-su-dang-ubnd-tinh-va-cac-thanh-vien-ubnd-tinh-xem-xet-cho-y-kien-
mot-so-noi-dung-quan-trong-c29576.html
  - http://hungyen.dcs.vn/ban-can-su-dang-ubnd-tinh-va-cac-thanh-vien-ubnd-tinh [...]
```

91815 - Web Application Sitemap

Synopsis

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

Description

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/443/www

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

  - https://hungyen.dcs.vn/
  - https://hungyen.dcs.vn/dfc7d243c39529351a844cd6af29d8d0
  - https://hungyen.dcs.vn/dfc7d243c39529351a844cd6af29d8d0/styles.css
  - https://hungyen.dcs.vn/favicon
  - https://hungyen.dcs.vn/favicon/apple-touch-icon.png
  - https://hungyen.dcs.vn/favicon/favicon-16x16.png
  - https://hungyen.dcs.vn/favicon/favicon-32x32.png
  - https://hungyen.dcs.vn/favicon/favicon.ico
  - https://hungyen.dcs.vn/favicon/safari-pinned-tab.svg
  - https://hungyen.dcs.vn/favicon/site.webmanifest

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/8443/www

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

  - https://hungyen.dcs.vn:8443/manage/account/login

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

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 1000 queries in 550s (1.0818 queries per second)

The following CGIs have been discovered :


+ CGI : /
  Methods : POST
  Argument : __EVENTVALIDATION
  Argument : __VIEWSTATE
  Argument : __VIEWSTATEGENERATOR
   Value: 8D0E13E6
  Argument : ctl00$uc_menunew$butimkiemnew
   Value: Button
  Argument : ctl00$uc_menunew$txtkeynew


+ CGI : /home.aspx
  Methods : POST
  Argument : __EVENTVALIDATION
  Argument : __VIEWSTATE
  Argument : __VIEWSTATEGENERATOR
   Value: 8D0E13E6
  Argument : ctl00$uc_menunew$butimkiemnew
   Value: Button
  Argument : ctl00$uc_menunew$txtkeynew
```

```
+ CGI : /cate.aspx
  Methods : POST
  Argument : __EVENTARGUMENT
  Argument : __EVENTTARGET
  Argument : __EVENTVALIDATION
  Argument : __LASTFOCUS
  Argument : __VIEWSTATE
  Argument : __VIEWSTATEGENERATOR
   Value: 942604B6
  Argument : cateid
   Value: 18
  Argument : ctl00$ContentPlaceHolder1$ctl00$butdangky
   Value: G#i
  Argument : ctl00$ContentPlaceHolder1$ctl00$buttimkiem
   Value: Tìm ki#m
  Argument : ctl00$ContentPlaceHolder1$ctl00$ddl_linhvuc
  Argument : ctl00$ContentPlaceHolder1$ctl00$txtcapcha
  Argument : ctl00$ContentPlaceHolder1$ctl00$txtdiachi
  Argument : ctl00$ContentPlaceHolder1$ctl00$txtemail
  Argument : ctl00$ContentPlaceHolder1$ctl00$txthoten
  Argument : ctl00$ContentPlaceHolder1$ctl00$txtkey
  Argument : ctl00$ContentPlaceHolder1$ctl00$txtnoidung
  Argument : ctl00$ContentPlaceHolder1$ctl00$txtsdt
  Argument : ctl00$ContentPlaceHolder1$ctl00$txttitle
  Argument : ctl00$ContentPlaceHolder1$ctl00$txttuoi
  Argument : ctl00$uc_menunew$butimkiemnew
   Value: Button
  Argument : ctl00$uc_menunew$txtkeynew
  Argument : page
   Value: 3
  Argument : uc
   Value: 3


+ CGI : /cate_no_right.aspx
  Methods : POST
  Argument : __EVENTARGUMENT
  Argument : __EVENTTARGET
  Argument : __EVENTVALIDATION
  Argument : __LASTFOCUS
  Argument : __VIEWSTATE
  Argument : __VIEWSTATEGENERATOR
   Value: 1B1E5454
  Argument : cateid
   Value: 260
  Argument : ctl00$ContentPlaceHolder1$ctl00$ddlcap
   Value: Xã
  Ar [...]
```

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/443/www

```
Webmirror performed 10 queries in 1s (10.000 queries per second)

The following CGIs have been discovered :


+ CGI : /logout
  Methods : GET
  Argument : redir
```

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/8443/www

```
Webmirror performed 5 queries in 1s (5.000 queries per second)

The following CGIs have been discovered :


+ CGI : /manage/account/login
  Methods : GET
  Argument : redirect
   Value: %2Fmanage%2F


+ CGI : /manage/account/angular/gf72902384/images/favicons/favicon-152.png
  Methods : GET
  Argument : v
   Value: 2


+ CGI : /manage/account/angular/gf72902384/images/favicons/favicon-144.png
  Methods : GET
  Argument : v
   Value: 2


+ CGI : /manage/account/angular/gf72902384/images/favicons/favicon-120.png
  Methods : GET
  Argument : v
   Value: 2
```

```
+ CGI : /manage/account/angular/gf72902384/images/favicons/favicon-72.png
  Methods : GET
  Argument : v
   Value: 2


+ CGI : /manage/account/angular/gf72902384/images/favicons/favicon-57.png
  Methods : GET
  Argument : v
   Value: 2


+ CGI : /manage/account/angular/gf72902384/images/favicons/favicon-32.png
  Methods : GET
  Argument : v
   Value: 2
```