etc.vn

ETC Report

Report generated by Nessus™ Fri, 24 Mar 2023 14:04:53 +07

Vulnerabilities by Host

Vulnerabilities by Host

etc.vn

0	1	1	0	32
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Fri Mar 24 11:11:53 2023
End time: Fri Mar 24 14:04:52 2023

Host Information

DNS Name: etc.vn
IP: 14.232.240.61
OS: Linux Kernel 2.6

Vulnerabilities

42424 - CGI Generic SQL Injection (blind)

Synopsis

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

Description

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

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

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

See Also

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

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

http://www.nessus.org/u?11ab1866

Solution

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

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

XREF	CWE:20
XREF	CWE:77
XREF	CWE:89
XREF	CWE:91
XREF	CWE:203
XREF	CWE:643
XREF	CWE:713
XREF	CWE:722
XREF	CWE:727
XREF	CWE:751
XREF	CWE:801
XREF	CWE:810
XREF	CWE:928
XREF	CWE:929

Plugin Information

Published: 2009/11/06, Modified: 2022/10/28

Plugin Output

tcp/443/www

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

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

+ The 'page' parameter of the /search CGI :

/search?q=&page=2zz&page=2yy

-------- output --------
            <ul>
                                    <li>
                        <a class="drop-item" href="https://etc.vn/vi/sea
rch?page=2&q="
```

```
                           title="Ti#ng Vi#t">
                            <img src="/resources/company/images/fl [...]
-------- vs --------
            <ul>
                                    <li>
                        <a class="drop-item" href="https://etc.vn/vi/sea
rch?page=2yy&q="
                           title="Ti#ng Vi#t">
                            <img src="/resources/company/images/fl [...]
------------------------

/search?q=&page=2zz&page=2yy {2}

-------- output --------
            <ul>
                                    <li>
                        <a class="drop-item" href="https://etc.vn/vi/sea
rch?page=2&q="
                           title="Ti#ng Vi#t">
                            <img src="/resources/company/images/fl [...]
-------- vs --------
            <ul>
                                    <li>
                        <a class="drop-item" href="https://etc.vn/vi/sea
rch?page=2yy&q="
                           title="Ti#ng Vi#t">
                            <img src="/resources/company/images/fl [...]
------------------------

+ The 'page' parameter of the /en/search CGI :

/en/search?q=&page=2zz&page=2yy

-------- output --------
            <ul>
                                    <li>
                        <a class="drop-item" href="https://etc.vn/vi/sea
rch?page=2&q="
                           title="Ti#ng Vi#t">
                            <img src="/resources/company/images/fl [...]
-------- vs --------
            <ul>
                                    <li>
                        <a class="drop-item" href="https://etc.vn/vi/sea
rch?page=2yy&q="
                           title="Ti#ng Vi#t [...]
```

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/443/www

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

  - https://etc.vn/
  - https://etc.vn/amazon-web-service-dao-tao-gioi-thieu-ve-dam-may-rieng-tai-cho-amazon-outpost-
cho-hon-40-ky-su-cntt-cong-ty-etc
  - https://etc.vn/cau-chuyen-thuong-hieu
  - https://etc.vn/chuyen-tham-trung-tam-itera-dau-nam-2023-day-la-khoi-dau-cua-mot-ky-nguyen-moi
  - https://etc.vn/en
  - https://etc.vn/en/
  - https://etc.vn/en/about-us
  - https://etc.vn/en/amazon-web-service-dao-tao-gioi-thieu-ve-dam-may-rieng-tai-cho-amazon-outpost-
cho-hon-40-ky-su-cntt-cong-ty-etc
  - https://etc.vn/en/brand-story
  - https://etc.vn/en/chuyen-tham-trung-tam-itera-dau-nam-2023-day-la-khoi-dau-cua-mot-ky-nguyen-moi
  - https://etc.vn/en/contact
  - https://etc.vn/en/epay-trao-tang-cac-goi-thiet-bi-va-dich-vu-cho-ubnd-tinh-ha-nam
  - https://etc.vn/en/etc-and-epay-proudly-be-a-strategic-partner-in-the-implementation-of-the-e-id-
and-authentication-service-project
  - https://etc.vn/en/etc-employee-is-honored-to-receive-the-offensive-security-certified-
professional
  - https://etc.vn/en/etc-epay-contribute-to-promote-digital-transfer-of-financial-services
  - https://etc.vn/en/etc-switching-using-customs-declaration-software-provided-by-customs
  - https://etc.vn/en/etc-thay-dien-mao-don-ky-nguyen-moi
  - https://etc.vn/en/etc-to-chuc-khoa-dao-tao-ve-bao-mat-an-ninh-mang-cho-cbnv
  - https://etc.vn/en/etc-tro-thanh-1-trong-9-doi-tac-titanium-tai-viet-nam-cua-ong-trum-dell-
technologies
  - https://etc.vn/en/etc-va-epay-tham-gia-trien-lam-trung-bay-cac-giai-phap-cong-nghe-nganh-cong-an
  - https://etc.vn/en/itera-1
  - https://etc.vn/en/itera-it-era-etcs-new-technology-age
  - https://etc.vn/en/jobs
  - https://etc.vn/en/jobs/
  - https://etc.vn/en/jobs/back-end-developer-nodejs
  - https://etc.vn/en/jobs/chuyen-vien-doi-soat
  - https://etc.vn/en/jobs/net-developer-1
  - https://etc.vn/en/jobs/networksecurity-engineer-intern-fresher-junior-senior
  - https://etc.vn/en/jobs/networksecuritysystem-presa [...]
```

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/443/www

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

+ The following resources may be vulnerable to injectable parameter :

+ The 'page' parameter of the /tin-etc CGI :

/tin-etc?page=%00dmdnhi

-------- output --------
<ul>
<li>
<a class="drop-item" href="https://etc.vn/vi/tin-etc?page=%00dmdnhi"
title="Ti#ng Vi#t">
<img src="/resources/company/images/flag-vi.jpg"  title="Ti#ng V [...]
------------------------

+ The 'page' parameter of the /tin-tuc CGI :
```

```
/tin-tuc?page=%00dmdnhi

-------- output --------
<ul>
<li>
<a class="drop-item" href="https://etc.vn/vi/tin-tuc?page=%00dmdnhi"
title="Ti#ng Vi#t">
<img src="/resources/company/images/flag-vi.jpg"  title="Ti#ng V [...]
------------------------

+ The 'page' parameter of the /search CGI :

/search?page=%00dmdnhi

-------- output --------
<ul>
<li>
<a class="drop-item" href="https://etc.vn/vi/search?page=%00dmdnhi"
title="Ti#ng Vi#t">
<img src="/resources/company/images/flag-vi.jpg"  title="Ti#ng V [...]
------------------------

+ The 'q' parameter of the /search CGI :

/search?q=%00dmdnhi

-------- output --------
<link rel="shortcut icon" href="https://etc.vn/storage/setup/etc-f [...]

<title>K#t qu# tìm ki#m: &quot;dmdnhi&quot;</title>
<meta name="description" content="K#t qu# tìm ki#m: &quot;d [...]
<meta name="viewport" content="width=device-width, initial-scale=1">
------------------------

+ The 'page' parameter of the /search CGI :

/search?page=%00dmdnhi&q=

-------- output --------
<ul>
<li>
<a class="drop-item" href="https://etc.vn/vi/search?page=%00dmdnhi&q="
title="Ti#ng Vi#t">
<img src="/resources/company/images/flag-vi.jpg"  title="Ti#ng V [...]
------------------------

+ The 'q' parameter of the /search CGI :

/search?page=2&q=%00dmdnhi

-------- output --------
<link rel="shortcut icon" href="https://etc.vn/storage/setup/etc-f [...]

<title>K#t qu# tìm ki#m: &quot;dmdnhi&quot;</title>
<meta name="description" content="K#t qu# tìm ki#m: &quot;d [...]
<meta name="viewport" content="width=device-wid [...]
```

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]

cross-site scripting (comprehensive test): S=425        SP=425       AP=1955      SC=34
 AC=13736
persistent XSS                           : S=100        SP=100       AP=460       SC=8
 AC=3232
arbitrary command execution              : S=550        SP=550       AP=2530      SC=44
 AC=17776
web code injection                       : S=25         SP=25        AP=115       SC=2
 AC=808
script injection                         : S=25         SP=25        AP=115       SC=2
 AC=808
HTML injection                           : S=125        SP=125       AP=575       SC=10
 AC=4040
arbitrary command execution (time based) : S=150        SP=150       AP=690       SC=12
 AC=4848
XML injection                            : S=25         SP=25        AP=115       SC=2
 AC=808
unseen parameters                        : S=875        SP=875       AP=4025      SC=70
 AC=28280
```

```
directory traversal (write access)       : S=50         SP=50        AP=230       SC=4
 AC=1616
SQL injection (2nd order)                : S=25         SP=25        AP=115       SC=2
 AC=808
on site request forgery                  : S=25         SP=25        AP=115       SC=2
 AC=808
blind SQL injection (4 requests)         : S=100        SP=100       AP=460       SC=8
 AC=3232
HTTP response splitting                  : S=225        SP=225       AP=1035      SC=18
 AC=7272
directory traversal (extended test)      : S=1275       SP=1275      AP=5865      SC=102
 AC=41208
header injection                         : S=50         SP=50        AP=230       SC=4
 AC=1616
injectable parameter                     : S=50         SP=50        AP=230       SC=4
 AC=1616
local file inclusion                   [...]
```

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 :
- HTML injection
- script injection
- uncontrolled redirection
- on site request forgery
- cross-site scripting (comprehensive test)
- arbitrary command execution
- SSI injection
- local file inclusion
- SQL injection (2nd order)
- directory traversal
- directory traversal (extended test)
- web code injection
- SQL injection
- cross-site scripting (extended patterns)
- header injection

The following tests were interrupted and did not report all possible flaws :
```

```
- blind 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/443/www

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


https://img.chinhsachcuocsong.vn/MediaUpload/Org/2022/12/20/202019-img_20221220_201229.jpg - /ung-
dung-du-lieu-dan-cu-trong-kiem-tra-an-ninh-truoc-khi-len-may-bay
https://img.chinhsachcuocsong.vn/MediaUpload/Org/2022/12/20/202207-img_20221220_201652.jpg - /ung-
dung-du-lieu-dan-cu-trong-kiem-tra-an-ninh-truoc-khi-len-may-bay
https://pinterest.com/pin/create/button?media=https%3A%2F%2Fetc.vn%2Fresources%2Fcore%2Fcore
%2Fbase%2Fimages%2Fplaceholder.png&url=https%3A%2F%2Fetc.vn%2Fen%2Fjobs%2Fback-end-developer-
nodejs&description= - /en/jobs/back-end-developer-nodejs
https://pinterest.com/pin/create/button?media=https%3A%2F%2Fetc.vn%2Fresources%2Fcore%2Fcore%2Fbase
%2Fimages%2Fplaceholder.png&url=https%3A%2F%2Fetc.vn%2Fen%2Fjobs%2Fchuyen-vien-doi-soat&description=
 - /en/jobs/chuyen-vien-doi-soat
https://pinterest.com/pin/create/button?media=https%3A%2F%2Fetc.vn%2Fresources%2Fcore%2Fcore%2Fbase
%2Fimages%2Fplaceholder.png&url=https%3A%2F%2Fetc.vn%2Fen%2Fjobs%2Fnet-developer-1&description= - /
en/jobs/net-developer-1
https://pinterest.com/pin/create/button?media=https%3A%2F%2Fetc.vn%2Fresources%2Fcore%2Fcore%2Fbase
%2Fimages%2Fplaceholder.png&url=https%3A%2F%2Fetc.vn%2Fen%2Fjobs%2Fnetworksecurity-engineer-intern-
fresher-junior-senior&description= - /en/jobs/networksecurity-engineer-intern-fresher-junior-senior
https://pinterest.com/pin/create/button?media=https%3A%2F%2Fetc.vn%2Fresources%2Fcore%2Fcore
%2Fbase%2Fimages%2Fplaceholder.png&url=https%3A%2F%2Fetc.vn%2Fen%2Fjobs%2Fnetworksecuritysystem-
presale&description= - /en/jobs/networksecuritysystem-presale
https://pinterest.com/pin/create/button?media=https%3A%2F%2Fetc.vn%2Fresources%2Fcore%2Fcore%2Fbase
%2Fimages%2Fplaceholder.png&url=https%3A%2F%2Fetc.vn%2Fen%2Fjobs%2Fnhan-vien-bao-hanh-sua-chua-san-
pham&description= - /en/jobs/nhan-vien-bao-hanh-sua-chua-san-pham
https://pinterest.com/pin/create/button?media=https%3A%2F%2Fetc.vn%2Fresources%2Fcore%2Fcore%2Fbase
%2Fima [...]
```

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 cookies do not have the 'secure' property enabled, despite being served over HTTPS :

  Domain   :
  Path     : /
  Name     : XSRF-TOKEN
  Value    :
 eyJpdiI6IjFVNmtuRmdNZHdxQnRScWpTSVhOdFE9PSIsInZhbHVlIjoiakFpR2o3V1hFdmZlTE8rSCtybUFyMkRnalBhVWFQUUtycGlBdFl1aU5uS
  Secure   : false
  HttpOnly : false
```

```
  Domain   :
  Path     : /
  Name     : dcore_session
  Value    :
eyJpdiI6IkJTSnllUVhXRzVZeWRqVHdUamhKdEE9PSIsInZhbHVlIjoiSkpDL1ZVaEQzVldFbko5QklBV2txWHVXTUlEU2pna2M4dXJxT3pSSHhoe
  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 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 :

    /

  - 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/443/www

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

  - HTTP methods GET HEAD are allowed on :

    /en
    /en/jobs
    /jobs
    /search


Based on tests of each method :

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

    /
    /en
    /en/jobs
    /jobs
    /resources
    /resources/company
    /resources/company/css
    /resources/company/fonts
    /resources/company/fonts/fontawesome-pro-5.15.3-web
    /resources/company/fonts/fontawesome-pro-5.15.3-web/css
    /resources/core
    /resources/core/plugins
    /resources/core/plugins/language
    /resources/core/plugins/language/css
    /resources/core/plugins/simple-slider
    /resources/core/plugins/simple-slider/css
    /search
    /storage
    /themes

  - Invalid/unknown HTTP methods are allowed on :

    /
    /en
    /en/jobs
    /jobs
    /resources
    /resources/company
    /resources/company/css
    /resources/company/fonts
    /resources/company/fonts/fontawesome-pro-5.15.3-web
    /resources/company/fonts/fontawesome-pro-5.15.3-web/css
    /resources/core
    /resources/core/plugins
    /resources/core/plugins/language
    /resources/core/plugins/language/css
    /resources/core/plugins/simple-slider
    /resources/core/plugins/simple-slider/css
    /search
    /storage
    /themes
```

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
```

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/443/www

```
The remote web server type is :

nginx
```

85805 - HTTP/2 Cleartext Detection

Synopsis

An HTTP/2 server is listening on the remote host.

Description

The remote host is running an HTTP server that supports HTTP/2 running over cleartext TCP (h2c).

See Also

https://http2.github.io/

https://tools.ietf.org/html/rfc7540

https://github.com/http2/http2-spec

Solution

Limit incoming traffic to this port if desired.

Risk Factor

None

Plugin Information

Published: 2015/09/04, Modified: 2022/04/11

Plugin Output

tcp/8404/www

```
The server supports direct HTTP/2 connections
without encryption.
```

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
  Date: Fri, 24 Mar 2023 04:49:17 GMT
  Content-Type: text/html
  Content-Length: 162
  Connection: keep-alive
  Location: https://etc.vn/
  Strict-Transport-Security: max-age=31536000

Response Body :

<html>
<head><title>301 Moved Permanently</title></head>
<body>
<center><h1>301 Moved Permanently</h1></center>
<hr><center>nginx</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/443/www

```
Response Code : HTTP/1.1 200 OK

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

  Server: nginx
  Content-Type: text/html; charset=UTF-8
  Transfer-Encoding: chunked
  Connection: keep-alive
  Vary: Accept-Encoding
  Cache-Control: no-cache, private
  Date: Fri, 24 Mar 2023 04:49:18 GMT
  Set-Cookie: XSRF-
TOKEN=eyJpdiI6IlJUNGFkTzk0M3pQU0s5cmM0WnVsNmc9PSIsInZhbHVlIjoieHV3cldERW1wUkhzNFFDVFg2OUJnV1E2d2t3aXF0WEcxL3ZBV0Nh
 expires=Fri, 24-Mar-2023 06:49:18 GMT; Max-Age=7200; path=/; samesite=lax
  Set-Cookie:
 dcore_session=eyJpdiI6ImJFd040MUpGRXpWTldqS1BCVEhqUkE9PSIsInZhbHVlIjoidHZVVlFtbGlXbWxKZUJWOVY3VW1VU0dFaE5jbW1YQi9
 expires=Fri, 24-Mar-2023 06:49:18 GMT; Max-Age=7200; path=/; httponly; samesite=lax
  Strict-Transport-Security: max-age=31536000

Response Body :

<!DOCTYPE html>
<html lang="vi">
```

```
<head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <!-- HTML5 Shim and Respond.js IE8 support of HTML5 elements and media queries -->
    <!-- WARNING: Respond.js doesn't work if you view the page via file:// -->
    <!--[if lt IE 9]>
            <script src="https://oss.maxcdn.com/libs/html5shiv/3.7.0/html5shiv.js"></script>
            <script src="https://oss.maxcdn.com/libs/respond.js/1.4.2/respond.min.js"></script>
        <![endif]-->
    <link rel="shortcut icon" href="https://etc.vn/storage/setup/etc-favicon.png">

<title>ETC</title>
<meta name="description"  [...]
```

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://etc.vn/
  HTTP response   : HTTP/1.1 301 Moved Permanently
  Redirect to     : https://etc.vn/
  Redirect type   : 30x redirect


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

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/443/www

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

  - https://etc.vn/
  - https://etc.vn/amazon-web-service-dao-tao-gioi-thieu-ve-dam-may-rieng-tai-cho-amazon-outpost-
cho-hon-40-ky-su-cntt-cong-ty-etc
  - https://etc.vn/cau-chuyen-thuong-hieu
  - https://etc.vn/chuyen-tham-trung-tam-itera-dau-nam-2023-day-la-khoi-dau-cua-mot-ky-nguyen-moi
  - https://etc.vn/en
  - https://etc.vn/en/
  - https://etc.vn/en/about-us
  - https://etc.vn/en/amazon-web-service-dao-tao-gioi-thieu-ve-dam-may-rieng-tai-cho-amazon-outpost-
cho-hon-40-ky-su-cntt-cong-ty-etc
  - https://etc.vn/en/brand-story
```

```
  - https://etc.vn/en/chuyen-tham-trung-tam-itera-dau-nam-2023-day-la-khoi-dau-cua-mot-ky-nguyen-moi
  - https://etc.vn/en/contact
  - https://etc.vn/en/epay-trao-tang-cac-goi-thiet-bi-va-dich-vu-cho-ubnd-tinh-ha-nam
  - https://etc.vn/en/etc-and-epay-proudly-be-a-strategic-partner-in-the-implementation-of-the-e-id-
and-authentication-service-project
  - https://etc.vn/en/etc-employee-is-honored-to-receive-the-offensive-security-certified-
professional
  - https://etc.vn/en/etc-epay-contribute-to-promote-digital-transfer-of-financial-services
  - https://etc.vn/en/etc-switching-using-customs-declaration-software-provided-by-customs
  - https://etc.vn/en/etc-thay-dien-mao-don-ky-nguyen-moi
  - https://etc.vn/en/etc-to-chuc-khoa-dao-tao-ve-bao-mat-an-ninh-mang-cho-cbnv
  - https://etc.vn/en/etc-tro-thanh-1-trong-9-doi-tac-titanium-tai-viet-nam-cua-ong-trum-dell-
technologies
  - https://etc.vn/en/etc-va-epay-tham-gia-trien-lam-trung-bay-cac-giai-phap-cong-nghe-nganh-cong-an
  - https://etc.vn/en/itera-1
  - https://etc.vn/en/itera-it-era-etcs-new-technology-age
  - https://etc.vn/en/jobs
  - https://etc.vn/en/jobs/
  - https://etc.vn/en/jobs/back-end-developer-nodejs
  - https://etc.vn/en/jobs/chuyen-vien-doi-soat
  - https://etc.vn/en/jobs/net-developer-1
  - https://etc.vn/en/jobs/networksecurity-engineer-intern-fresher-junior-senior
  - https://etc.vn/en/jobs/networksecurity [...]
```

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/443/www

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

  - https://etc.vn/
  - https://etc.vn/amazon-web-service-dao-tao-gioi-thieu-ve-dam-may-rieng-tai-cho-amazon-outpost-
cho-hon-40-ky-su-cntt-cong-ty-etc
  - https://etc.vn/cau-chuyen-thuong-hieu
  - https://etc.vn/chuyen-tham-trung-tam-itera-dau-nam-2023-day-la-khoi-dau-cua-mot-ky-nguyen-moi
  - https://etc.vn/en
  - https://etc.vn/en/
  - https://etc.vn/en/about-us
  - https://etc.vn/en/amazon-web-service-dao-tao-gioi-thieu-ve-dam-may-rieng-tai-cho-amazon-outpost-
cho-hon-40-ky-su-cntt-cong-ty-etc
  - https://etc.vn/en/brand-story
  - https://etc.vn/en/chuyen-tham-trung-tam-itera-dau-nam-2023-day-la-khoi-dau-cua-mot-ky-nguyen-moi
  - https://etc.vn/en/contact
  - https://etc.vn/en/epay-trao-tang-cac-goi-thiet-bi-va-dich-vu-cho-ubnd-tinh-ha-nam
  - https://etc.vn/en/etc-and-epay-proudly-be-a-strategic-partner-in-the-implementation-of-the-e-id-
and-authentication-service-project
```

```
  - https://etc.vn/en/etc-employee-is-honored-to-receive-the-offensive-security-certified-
professional
  - https://etc.vn/en/etc-epay-contribute-to-promote-digital-transfer-of-financial-services
  - https://etc.vn/en/etc-switching-using-customs-declaration-software-provided-by-customs
  - https://etc.vn/en/etc-thay-dien-mao-don-ky-nguyen-moi
  - https://etc.vn/en/etc-to-chuc-khoa-dao-tao-ve-bao-mat-an-ninh-mang-cho-cbnv
  - https://etc.vn/en/etc-tro-thanh-1-trong-9-doi-tac-titanium-tai-viet-nam-cua-ong-trum-dell-
technologies
  - https://etc.vn/en/etc-va-epay-tham-gia-trien-lam-trung-bay-cac-giai-phap-cong-nghe-nganh-cong-an
  - https://etc.vn/en/itera-1
  - https://etc.vn/en/itera-it-era-etcs-new-technology-age
  - https://etc.vn/en/jobs
  - https://etc.vn/en/jobs/
  - https://etc.vn/en/jobs/back-end-developer-nodejs
  - https://etc.vn/en/jobs/chuyen-vien-doi-soat
  - https://etc.vn/en/jobs/net-developer-1
  - https://etc.vn/en/jobs/networksecurity-engineer-intern-fresher-junior-senior
  - https://etc.vn/en/jobs/networksecuritysystem-presale
  - https [...]
```

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: 2023/03/08

Plugin Output

tcp/22/ssh

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/03/08

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: 2023/03/08

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: 2023/03/08

Plugin Output

tcp/8404/www

```
Port 8404/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: 2022/06/09

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.5.0
Nessus build : 20097
Plugin feed version : 202303232359
Scanner edition used : Nessus
Scanner OS : LINUX
Scanner distribution : debian10-x86-64
Scan type : Normal
Scan name : etc.vn
```

```
Scan policy used : webScan
Scanner IP : 10.10.17.176
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Ping RTT : 42.223 ms
Thorough tests : yes
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : enabled
Web application tests : enabled
Web app tests -  Test mode : all_pairs
Web app tests -  Try all HTTP methods : yes
Web app tests -  Maximum run time : 10 minutes.
Web app tests -  Stop at first flaw : param
Max hosts : 2
Max checks : 2
Recv timeout : 15
Backports : None
Allow post-scan editing : Yes
Scan Start Date : 2023/3/24 11:11 +07
Scan duration : 10364 sec
```

85601 - Web Application Cookies Not Marked HttpOnly

Synopsis

HTTP session cookies might be vulnerable to cross-site scripting attacks.

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, one or more of those cookies are not marked 'HttpOnly', meaning that a malicious client-side script, such as JavaScript, could read them. The HttpOnly flag is a security mechanism to protect against cross-site scripting attacks, which was proposed by Microsoft and initially implemented in Internet Explorer. All modern browsers now support it.

Note that this plugin detects all general cookies missing the HttpOnly cookie flag, whereas plugin 48432 (Web Application Session Cookies Not Marked HttpOnly) will only detect session cookies from an authenticated session missing the HttpOnly cookie flag.

See Also

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

Solution

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

If possible, add the 'HttpOnly' attribute to all session cookies and any cookies containing sensitive data.

Risk Factor

None

References

XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:442
XREF	CWE:629
XREF	CWE:711
XREF	CWE:712
XREF	CWE:722
XREF	CWE:725
XREF	CWE:750
XREF	CWE:751
XREF	CWE:800
XREF	CWE:801

XREF	CWE:809
XREF	CWE:811
XREF	CWE:864
XREF	CWE:900
XREF	CWE:928
XREF	CWE:931
XREF	CWE:990

Plugin Information

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

Plugin Output

tcp/80/www

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

Name : XSRF-TOKEN
Path : /
Value :
 eyJpdiI6IjFVNmtuRmdNZHdxQnRScWpTSVhOdFE9PSIsInZhbHVlIjoiakFpR2o3V1hFdmZlTE8rSCtybUFyMkRnalBhVWFQUUtycGlBdFl1aU5uS
Domain :
Version : 1
Expires : Fri, 24-Mar-2023 06:25:37 GMT
Comment :
Secure : 0
Httponly : 0
Port :
```

85601 - Web Application Cookies Not Marked HttpOnly

Synopsis

HTTP session cookies might be vulnerable to cross-site scripting attacks.

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, one or more of those cookies are not marked 'HttpOnly', meaning that a malicious client-side script, such as JavaScript, could read them. The HttpOnly flag is a security mechanism to protect against cross-site scripting attacks, which was proposed by Microsoft and initially implemented in Internet Explorer. All modern browsers now support it.

Note that this plugin detects all general cookies missing the HttpOnly cookie flag, whereas plugin 48432 (Web Application Session Cookies Not Marked HttpOnly) will only detect session cookies from an authenticated session missing the HttpOnly cookie flag.

See Also

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

Solution

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

If possible, add the 'HttpOnly' attribute to all session cookies and any cookies containing sensitive data.

Risk Factor

None

References

XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:442
XREF	CWE:629
XREF	CWE:711
XREF	CWE:712
XREF	CWE:722
XREF	CWE:725
XREF	CWE:750
XREF	CWE:751
XREF	CWE:800
XREF	CWE:801

XREF	CWE:809
XREF	CWE:811
XREF	CWE:864
XREF	CWE:900
XREF	CWE:928
XREF	CWE:931
XREF	CWE:990

Plugin Information

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

Plugin Output

tcp/443/www

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

Name : XSRF-TOKEN
Path : /
Value :
 eyJpdiI6IjFVNmtuRmdNZHdxQnRScWpTSVhOdFE9PSIsInZhbHVlIjoiakFpR2o3V1hFdmZlTE8rSCtybUFyMkRnalBhVWFQUUtycGlBdFl1aU5uS
Domain :
Version : 1
Expires : Fri, 24-Mar-2023 06:25:37 GMT
Comment :
Secure : 0
Httponly : 0
Port :
```

85602 - Web Application Cookies Not Marked Secure

Synopsis

HTTP session cookies might be transmitted in cleartext.

Description

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

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

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

See Also

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

Solution

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

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

Risk Factor

None

References

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

Plugin Information

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

Plugin Output

tcp/80/www

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

Name : dcore_session
Path : /
Value :
 eyJpdiI6IkJTSnllUVhXRzVZeWRqVHdUamhKdEE9PSIsInZhbHVlIjoiSkpDL1ZVaEQzVldFbko5QklBV2txWHVXTUlEU2pna2M4dXJxT3pSSHhoe
Domain :
Version : 1
Expires : Fri, 24-Mar-2023 06:25:37 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : XSRF-TOKEN
Path : /
Value :
 eyJpdiI6IjFVNmtuRmdNZHdxQnRScWpTSVhOdFE9PSIsInZhbHVlIjoiakFpR2o3V1hFdmZlTE8rSCtybUFyMkRnalBhVWFQUUtycGlBdFl1aU5uS
Domain :
Version : 1
Expires : Fri, 24-Mar-2023 06:25:37 GMT
Comment :
Secure : 0
Httponly : 0
Port :
```

85602 - Web Application Cookies Not Marked Secure

Synopsis

HTTP session cookies might be transmitted in cleartext.

Description

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

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

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

See Also

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

Solution

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

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

Risk Factor

None

References

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

Plugin Information

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

Plugin Output

tcp/443/www

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

Name : dcore_session
Path : /
Value :
 eyJpdiI6IkJTSnllUVhXRzVZeWRqVHdUamhKdEE9PSIsInZhbHVlIjoiSkpDL1ZVaEQzVldFbko5QklBV2txWHVXTUlEU2pna2M4dXJxT3pSSHhoe
Domain :
Version : 1
Expires : Fri, 24-Mar-2023 06:25:37 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : XSRF-TOKEN
Path : /
Value :
 eyJpdiI6IjFVNmtuRmdNZHdxQnRScWpTSVhOdFE9PSIsInZhbHVlIjoiakFpR2o3V1hFdmZlTE8rSCtybUFyMkRnalBhVWFQUUtycGlBdFl1aU5uS
Domain :
Version : 1
Expires : Fri, 24-Mar-2023 06:25:37 GMT
Comment :
Secure : 0
Httponly : 0
Port :
```

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://etc.vn/
  - https://etc.vn/amazon-web-service-dao-tao-gioi-thieu-ve-dam-may-rieng-tai-cho-amazon-outpost-
cho-hon-40-ky-su-cntt-cong-ty-etc
  - https://etc.vn/cau-chuyen-thuong-hieu
  - https://etc.vn/chuyen-tham-trung-tam-itera-dau-nam-2023-day-la-khoi-dau-cua-mot-ky-nguyen-moi
  - https://etc.vn/en
  - https://etc.vn/en/
  - https://etc.vn/en/about-us
  - https://etc.vn/en/amazon-web-service-dao-tao-gioi-thieu-ve-dam-may-rieng-tai-cho-amazon-outpost-
cho-hon-40-ky-su-cntt-cong-ty-etc
  - https://etc.vn/en/brand-story
  - https://etc.vn/en/chuyen-tham-trung-tam-itera-dau-nam-2023-day-la-khoi-dau-cua-mot-ky-nguyen-moi
  - https://etc.vn/en/contact
  - https://etc.vn/en/epay-trao-tang-cac-goi-thiet-bi-va-dich-vu-cho-ubnd-tinh-ha-nam
  - https://etc.vn/en/etc-and-epay-proudly-be-a-strategic-partner-in-the-implementation-of-the-e-id-
and-authentication-service-project
  - https://etc.vn/en/etc-employee-is-honored-to-receive-the-offensive-security-certified-
professional
  - https://etc.vn/en/etc-epay-contribute-to-promote-digital-transfer-of-financial-services
  - https://etc.vn/en/etc-switching-using-customs-declaration-software-provided-by-customs
  - https://etc.vn/en/etc-thay-dien-mao-don-ky-nguyen-moi
  - https://etc.vn/en/etc-to-chuc-khoa-dao-tao-ve-bao-mat-an-ninh-mang-cho-cbnv
```

```
  - https://etc.vn/en/etc-tro-thanh-1-trong-9-doi-tac-titanium-tai-viet-nam-cua-ong-trum-dell-
technologies
  - https://etc.vn/en/etc-va-epay-tham-gia-trien-lam-trung-bay-cac-giai-phap-cong-nghe-nganh-cong-an
  - https://etc.vn/en/itera-1
  - https://etc.vn/en/itera-it-era-etcs-new-technology-age
  - https://etc.vn/en/jobs
  - https://etc.vn/en/jobs/
  - https://etc.vn/en/jobs/back-end-developer-nodejs
  - https://etc.vn/en/jobs/chuyen-vien-doi-soat
  - https://etc.vn/en/jobs/net-developer-1
  - https://etc.vn/en/jobs/networksecurity-engineer-intern-fresher-junior-senior
  - https://etc.vn/en/jobs/networksecuritysystem-presale
  - https://etc. [...]
```

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/443/www

```
The following directories were discovered:
/search, /storage, /en, /themes

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

49705 - Web Server Harvested Email Addresses

Synopsis

Email addresses were harvested from the web server.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/443/www

```
The following email addresses have been gathered :


- 'sales@etc.vn', referenced from :
   /en/service/firewall-solution-network-attack-prevention
   /jobs/tuyen-dung-tech-lead
   /service/professional-solutions-for-ministry-of-health
   /en/about-us
   /service/may-phan-tich-va-phat-hien-ma-tuy-cam-tay
   /en/service/trien-khai-tich-hop-bo-giai-phap-an-toan-an-ninh-siem-soc
   /en/jobs/solution-architect
   /jobs/chuyen-vien-doi-soat
   /en/service/he-thong-soi-chieu-va-phan-tich-hinh-anh
   /en/etc-to-chuc-khoa-dao-tao-ve-bao-mat-an-ninh-mang-cho-cbnv
   /ve-chung-toi
   /itera
   /jobs/nhan-vien-ky-thuat-thiet-bi-khoa-hoc-nghiep-vu
   /resources/company/index.html
   /en/service/may-phan-tich-va-phat-hien-ma-tuy-cam-tay
   /en/service/deploy-and-integrate-network-infrastructure
   /jobs/solution-architect
   /service/trien-khai-tich-hop-ha-tang-giai-phap-ai-bigdata
   /chuyen-tham-trung-tam-itera-dau-nam-2023-day-la-khoi-dau-cua-mot-ky-nguyen-moi
   /service/giai-phap-nghiep-vu-bo-cong-an
   /en/service/he-thong-may-chu-luu-tru-sao-luu-du-lieu
   /en/jobs/networksecurity-engineer-intern-fresher-junior-senior
   /service/dich-vu-quan-tri-va-van-hanh-he-thong-1
   /service/unmanned-aircraft-system-uas
   /en/jobs/tuyen-dung-dev-lead-backend
   /en/service/giai-phap-quan-ly-van-hanh-khai-thac-san-bay-cang-hang-khong
```

```
    /en/jobs/nhan-vien-phan-tich-nghiep-vu-ba-du-an-epay
    /en/service/data-center
    /service/virtualization-and-cloud-computing-solutions
    /service/trien-khai-giai-phap-ao-hoa-va-dien-toan-dam-may
    /service/fod-system-and-prevent-runway-incursions
    /en/etc-thay-dien-mao-don-ky-nguyen-moi
    /en/service/khai-bao-hai-quan
    /cau-chuyen-thuong-hieu
    /etc-chuyen-doi-su-dung-phan-mem-ke-khai-hai-quan-do-co-quan-hai-quan-cung-cap
    /en/etc-employee-is-honored-to-receive-the-offensive-security-certified-professional
    /jobs/nhan-vien-ke-toan
    /service/state-bank-professional-solutions
    /service/customs-declaration
    /service/he-thong-may-chu-luu-tru-sao-luu-du-lieu
    /etc-va-epay-gop-pha [...]
```

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/80/www

```
CGI scanning will be disabled for this host because the host responds
to requests for non-existent URLs with HTTP code 301
rather than 404. The requested URL was :

    http://etc.vn/0v0Pns7Nipb8.html
```

10302 - Web Server robots.txt Information Disclosure

Synopsis

The remote web server contains a 'robots.txt' file.

Description

The remote host contains a file named 'robots.txt' that is intended to prevent web 'robots' from visiting certain directories in a website for maintenance or indexing purposes. A malicious user may also be able to use the contents of this file to learn of sensitive documents or directories on the affected site and either retrieve them directly or target them for other attacks.

See Also

http://www.robotstxt.org/orig.html

Solution

Review the contents of the site's robots.txt file, use Robots META tags instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive material.

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2018/11/15

Plugin Output

tcp/443/www

```
Contents of robots.txt :

User-agent: *
Disallow:
```

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: 2023/03/08

Plugin Output

tcp/443/www

```
Webmirror performed 343 queries in 253s (1.0355 queries per second)

The following CGIs have been discovered :


+ CGI : /search
  Methods : GET
  Argument : page
   Value: 5
  Argument : q


+ CGI : /en/search
  Methods : GET
  Argument : page
   Value: 5
  Argument : q


+ CGI : /tin-tuc
  Methods : GET
  Argument : page
   Value: 3


+ CGI : /jobs
  Methods : GET
```

```
  Argument : category
   Value: 20
  Argument : keyword
  Argument : location
   Value: 1
  Argument : page
   Value: 2
  Argument : type
   Value: 1


+ CGI : /en/jobs
  Methods : GET
  Argument : category
   Value: 20
  Argument : keyword
  Argument : location
   Value: 1
  Argument : page
   Value: 2
  Argument : type
   Value: 1


+ CGI : /jobs/apply
  Methods : POST
  Argument : _token
   Value: JnFOF4eJ5xgu8tCAHRRdkuSBdqwNsvvDJ1rGsqSe
  Argument : cover_letter
  Argument : email
  Argument : first_name
  Argument : job_id
  Argument : job_type
   Value: internal
  Argument : last_name
  Argument : message
  Argument : resume


+ CGI : /tin-etc
  Methods : GET
  Argument : page
   Value: 3
```

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: 2021/04/07

Plugin Output

tcp/80/www

```
URL     : http://etc.vn/
Version : unknown
source  : Server: nginx
```

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: 2021/04/07

Plugin Output

tcp/443/www

```
URL     : https://etc.vn/
Version : unknown
source  : Server: nginx
```