fire

Report generated by Nessus™ Mon, 16 Oct 2023 20:55:02 India Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

65.61.137.117

0	0	5	5	48
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Mon Oct 16 18:52:30 2023
End time: Mon Oct 16 20:55:01 2023

Host Information

IP: 65.61.137.117
OS: Dell EMC VMX, Microsoft Windows Embedded Standard 7

Vulnerabilities

47831 - CGI Generic XSS (comprehensive test)

Synopsis

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

Description

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

See Also

https://en.wikipedia.org/wiki/Cross_site_scripting#Non-persistent
http://www.nessus.org/u?ea9a0369
http://projects.webappsec.org/w/page/13246920/Cross%20Site%20Scripting

Solution

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

Risk Factor

Medium

CVSS v2.0 Base Score

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

References

XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:80
XREF	CWE:81
XREF	CWE:83
XREF	CWE:84
XREF	CWE:85
XREF	CWE:86
XREF	CWE:87
XREF	CWE:116
XREF	CWE:442
XREF	CWE:692
XREF	CWE:712
XREF	CWE:722
XREF	CWE:725
XREF	CWE:751
XREF	CWE:801
XREF	CWE:811
XREF	CWE:928
XREF	CWE:931

Plugin Information

Published: 2010/07/26, Modified: 2022/04/11

Plugin Output

tcp/80/www

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

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

+ The 'query' parameter of the /search.jsp CGI :

/search.jsp?query=%FF%FE%3C%73%63%72%69%70%74%3E%61%6C%65%72%74%28%32%30
%33%29%3C%2F%73%63%72%69%70%74%3E

-------- output --------
<p>No results were found for the query:<br /><br />

яю<script>alert(203)</script>
```

```
</div>
-------------------------
```

47831 - CGI Generic XSS (comprehensive test)

Synopsis

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

Description

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

See Also

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

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

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

Solution

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

Risk Factor

Medium

CVSS v2.0 Base Score

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

References

XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:80
XREF	CWE:81
XREF	CWE:83
XREF	CWE:84
XREF	CWE:85
XREF	CWE:86
XREF	CWE:87
XREF	CWE:116
XREF	CWE:442
XREF	CWE:692

XREF	CWE:712
XREF	CWE:722
XREF	CWE:725
XREF	CWE:751
XREF	CWE:801
XREF	CWE:811
XREF	CWE:928
XREF	CWE:931

Plugin Information

Published: 2010/07/26, Modified: 2022/04/11

Plugin Output

tcp/8080/www

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

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

+ The 'query' parameter of the /search.jsp CGI :

/search.jsp?query=%FF%FE%3C%73%63%72%69%70%74%3E%61%6C%65%72%74%28%32%30
%33%29%3C%2F%73%63%72%69%70%74%3E

-------- output --------
<p>No results were found for the query:<br /><br />

яю<script>alert(203)</script>

</div>
------------------------
```

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://65.61.137.117/
  - http://65.61.137.117/feedback.jsp
  - http://65.61.137.117/index.jsp
  - http://65.61.137.117/login.jsp
  - http://65.61.137.117/search.jsp
  - http://65.61.137.117/status_check.jsp
  - http://65.61.137.117/subscribe.jsp
  - http://65.61.137.117/survey_questions.jsp
```

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://65.61.137.117/
  - https://65.61.137.117/feedback.jsp
  - https://65.61.137.117/index.jsp
  - https://65.61.137.117/login.jsp
  - https://65.61.137.117/search.jsp
  - https://65.61.137.117/status_check.jsp
  - https://65.61.137.117/subscribe.jsp
  - https://65.61.137.117/survey_questions.jsp
```

85582 - Web Application Potentially Vulnerable to Clickjacking

Synopsis

The remote web server may fail to mitigate a class of web application vulnerabilities.

Description

The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy 'frame-ancestors' response header in all content responses. This could potentially expose the site to a clickjacking or UI redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions.

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

Content-Security-Policy (CSP) has been proposed by the W3C Web Application Security Working Group, with increasing support among all major browser vendors, as a way to mitigate clickjacking and other attacks. The 'frame-ancestors' policy directive restricts which sources can embed the protected resource.

Note that while the X-Frame-Options and Content-Security-Policy response headers are not the only mitigations for clickjacking, they are currently the most reliable methods that can be detected through automation. Therefore, this plugin may produce false positives if other mitigation strategies (e.g., frame-busting JavaScript) are deployed or if the page does not perform any security-sensitive transactions.

See Also

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

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

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

Solution

Return the X-Frame-Options or Content-Security-Policy (with the 'frame-ancestors' directive) HTTP header with the page's response.

This prevents the page's content from being rendered by another site when using the frame or iframe HTML tags.

Risk Factor

Medium

CVSS v2.0 Base Score

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

References

XREF	CWE:693

Plugin Information

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

Plugin Output

tcp/8080/www

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

  - http://65.61.137.117:8080/
  - http://65.61.137.117:8080/feedback.jsp
  - http://65.61.137.117:8080/index.jsp
  - http://65.61.137.117:8080/login.jsp
  - http://65.61.137.117:8080/search.jsp
  - http://65.61.137.117:8080/status_check.jsp
  - http://65.61.137.117:8080/subscribe.jsp
  - http://65.61.137.117:8080/survey_questions.jsp
```

42057 - Web Server Allows Password Auto-Completion

Synopsis

The 'autocomplete' attribute is not disabled on password fields.

Description

The remote web server contains at least one HTML form field that has an input of type 'password' where 'autocomplete' is not set to 'off'.

While this does not represent a risk to this web server per se, it does mean that users who use the affected forms may have their credentials saved in their browsers, which could in turn lead to a loss of confidentiality if any of them use a shared host or if their machine is compromised at some point.

Solution

Add the attribute 'autocomplete=off' to these fields to prevent browsers from caching credentials.

Risk Factor

Low

Plugin Information

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

Plugin Output

tcp/80/www

```
Page : /login.jsp
Destination Page: /doLogin
```

42057 - Web Server Allows Password Auto-Completion

Synopsis

The 'autocomplete' attribute is not disabled on password fields.

Description

The remote web server contains at least one HTML form field that has an input of type 'password' where 'autocomplete' is not set to 'off'.

While this does not represent a risk to this web server per se, it does mean that users who use the affected forms may have their credentials saved in their browsers, which could in turn lead to a loss of confidentiality if any of them use a shared host or if their machine is compromised at some point.

Solution

Add the attribute 'autocomplete=off' to these fields to prevent browsers from caching credentials.

Risk Factor

Low

Plugin Information

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

Plugin Output

tcp/443/www

```
Page : /login.jsp
Destination Page: /doLogin
```

42057 - Web Server Allows Password Auto-Completion

Synopsis

The 'autocomplete' attribute is not disabled on password fields.

Description

The remote web server contains at least one HTML form field that has an input of type 'password' where 'autocomplete' is not set to 'off'.

While this does not represent a risk to this web server per se, it does mean that users who use the affected forms may have their credentials saved in their browsers, which could in turn lead to a loss of confidentiality if any of them use a shared host or if their machine is compromised at some point.

Solution

Add the attribute 'autocomplete=off' to these fields to prevent browsers from caching credentials.

Risk Factor

Low

Plugin Information

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

Plugin Output

tcp/8080/www

```
Page : /login.jsp
Destination Page: /doLogin
```

26194 - Web Server Transmits Cleartext Credentials

Synopsis

The remote web server might transmit credentials in cleartext.

Description

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

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

Solution

Make sure that every sensitive form transmits content over HTTPS.

Risk Factor

Low

CVSS v2.0 Base Score

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

References

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

Plugin Information

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

Plugin Output

tcp/80/www

```
Page : /login.jsp
Destination Page: /doLogin
```

26194 - Web Server Transmits Cleartext Credentials

Synopsis

The remote web server might transmit credentials in cleartext.

Description

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

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

Solution

Make sure that every sensitive form transmits content over HTTPS.

Risk Factor

Low

CVSS v2.0 Base Score

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

References

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

Plugin Information

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

Plugin Output

tcp/8080/www

```
Page : /login.jsp
Destination Page: /doLogin
```

39446 - Apache Tomcat Detection

Synopsis

The remote web server is an Apache Tomcat server.

Description

Nessus was able to detect a remote Apache Tomcat web server.

See Also

https://tomcat.apache.org/

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0535

Plugin Information

Published: 2009/06/18, Modified: 2023/05/24

Plugin Output

tcp/80/www

```
URL     : http://65.61.137.117/
Version : unknown
```

39446 - Apache Tomcat Detection

Synopsis

The remote web server is an Apache Tomcat server.

Description

Nessus was able to detect a remote Apache Tomcat web server.

See Also

https://tomcat.apache.org/

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0535

Plugin Information

Published: 2009/06/18, Modified: 2023/05/24

Plugin Output

tcp/443/www

```
URL     : https://65.61.137.117/
Version : unknown
```

39446 - Apache Tomcat Detection

Synopsis

The remote web server is an Apache Tomcat server.

Description

Nessus was able to detect a remote Apache Tomcat web server.

See Also

https://tomcat.apache.org/

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0535

Plugin Information

Published: 2009/06/18, Modified: 2023/05/24

Plugin Output

tcp/8080/www

```
URL     : http://65.61.137.117:8080/
Version : unknown
```

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 'content' parameter of the /index.jsp CGI :

/index.jsp?content=eaceym

-------- output --------


<p>Failed due to The requested resource (/static/eaceym) is not availabl
e</p>

</td>
------------------------

+ The 'query' parameter of the /search.jsp CGI :
```

```
/search.jsp?query=eaceym

-------- output --------
<p>No results were found for the query:<br /><br />

eaceym

</div>
------------------------

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

http://65.61.137.117/index.jsp?content=eaceym
http://65.61.137.117/search.jsp?query=eaceym
```

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 'content' parameter of the /index.jsp CGI :

/index.jsp?content=eaceym

-------- output --------


<p>Failed due to The requested resource (/static/eaceym) is not availabl
e</p>

</td>
------------------------

+ The 'query' parameter of the /search.jsp CGI :
```

```
/search.jsp?query=eaceym

-------- output --------
<p>No results were found for the query:<br /><br />

eaceym

</div>
------------------------

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

https://65.61.137.117/index.jsp?content=eaceym
https://65.61.137.117/search.jsp?query=eaceym
```

47830 - CGI Generic Injectable Parameter

Synopsis

Some CGIs are candidate for extended injection tests.

Description

Nessus was able to to inject innocuous strings into CGI parameters and read them back in the HTTP response.

The affected parameters are candidates for extended injection tests like cross-site scripting attacks.

This is not a weakness per se, the main purpose of this test is to speed up other scripts. The results may be useful for a human pen-tester.

Solution

n/a

Risk Factor

None

References

XREF CWE:86

Plugin Information

Published: 2010/07/26, Modified: 2021/01/19

Plugin Output

tcp/8080/www

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

+ The following resources may be vulnerable to injectable parameter :

+ The 'content' parameter of the /index.jsp CGI :

/index.jsp?content=eaceym

-------- output --------


<p>Failed due to The requested resource (/static/eaceym) is not availabl
e</p>

</td>
------------------------

+ The 'query' parameter of the /search.jsp CGI :
```

```
/search.jsp?query=eaceym

-------- output --------
<p>No results were found for the query:<br /><br />

eaceym

</div>
------------------------

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

http://65.61.137.117:8080/index.jsp?content=eaceym
http://65.61.137.117:8080/search.jsp?query=eaceym
```

40406 - CGI Generic Tests HTTP Errors

Synopsis

Nessus encountered errors while running its generic CGI attacks.

Description

Nessus ran into trouble while running its generic CGI tests against the remote web server (for example, connection refused, timeout, etc). When this happens, Nessus aborts the current test and switches to the next CGI script on the same port or to another web server. Thus, test results may be incomplete.

Solution

Rescan with a longer network timeout or less parallelism for example, by changing the following options in the scan policy :

- Network -> Network Receive Timeout (check_read_timeout)

- Options -> Number of hosts in parallel (max_hosts)

- Options -> Number of checks in parallel (max_checks)

Risk Factor

None

Plugin Information

Published: 2009/07/28, Modified: 2021/01/19

Plugin Output

tcp/80/www

```
Nessus encountered :

  - 9 errors involving SSI injection (on HTTP headers) checks :
    . connecting to server: errno=6 (connection refused)
  - 8 errors involving SQL injection (on HTTP headers) checks :
    . connecting to server: errno=6 (connection refused)

This web server appears to be unresponsive now.
```

40406 - CGI Generic Tests HTTP Errors

Synopsis

Nessus encountered errors while running its generic CGI attacks.

Description

Nessus ran into trouble while running its generic CGI tests against the remote web server (for example, connection refused, timeout, etc). When this happens, Nessus aborts the current test and switches to the next CGI script on the same port or to another web server. Thus, test results may be incomplete.

Solution

Rescan with a longer network timeout or less parallelism for example, by changing the following options in the scan policy :

- Network -> Network Receive Timeout (check_read_timeout)

- Options -> Number of hosts in parallel (max_hosts)

- Options -> Number of checks in parallel (max_checks)

Risk Factor

None

Plugin Information

Published: 2009/07/28, Modified: 2021/01/19

Plugin Output

tcp/443/www

```
Nessus encountered :

  - 1 error involving SQL injection (on parameters names) checks :
   . connecting to server: errno=6 (connection refused)

This web server appears to be unresponsive now.
```

40406 - CGI Generic Tests HTTP Errors

Synopsis

Nessus encountered errors while running its generic CGI attacks.

Description

Nessus ran into trouble while running its generic CGI tests against the remote web server (for example, connection refused, timeout, etc). When this happens, Nessus aborts the current test and switches to the next CGI script on the same port or to another web server. Thus, test results may be incomplete.

Solution

Rescan with a longer network timeout or less parallelism for example, by changing the following options in the scan policy :

- Network -> Network Receive Timeout (check_read_timeout)

- Options -> Number of hosts in parallel (max_hosts)

- Options -> Number of checks in parallel (max_checks)

Risk Factor

None

Plugin Information

Published: 2009/07/28, Modified: 2021/01/19

Plugin Output

tcp/8080/www

```
Nessus encountered :

  - 1 error involving directory traversal (write access) checks :
    . connecting to server: errno=1 (operation timed out)
```

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=2          SP=2         AP=2         SC=2         AC=2

SQL injection                            : S=408        SP=408       AP=1104      SC=120
 AC=2304
unseen parameters                        : S=595        SP=595       AP=1610      SC=175
 AC=3360
local file inclusion                     : S=17         SP=17        AP=46        SC=5         AC=96

web code injection                       : S=17         SP=17        AP=46        SC=5         AC=96

XML injection                            : S=17         SP=17        AP=46        SC=5         AC=96

format string                            : S=34         SP=34        AP=92        SC=10
 AC=192
script injection                         : S=2          SP=2         AP=2         SC=2         AC=2

cross-site scripting (comprehensive test): S=68         SP=68        AP=184       SC=20
 AC=384
```

```
injectable parameter                      : S=34         SP=34        AP=92        SC=10
 AC=192
cross-site scripting (extended patterns) : S=12         SP=12        AP=12        SC=12        AC=12

directory traversal (write access)       : S=34         SP=34        AP=92        SC=10
 AC=192
SSI injection                            : S=51         SP=51        AP=138       SC=15
 AC=288
header injection                         : S=4          SP=4         AP=4         SC=4         AC=4

HTML injection                           : S=10         SP=10        AP=10        SC=10        AC=10

directory traversal                      : S=425        SP=425       AP=1150      SC=125
 AC=2400
arbitrary command execution (time based) : S=102        SP=102       AP=276       SC=30
 AC=576
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]

cross-site scripting (comprehensive test): S=68         SP=68        AP=184       SC=20
 AC=384
persistent XSS                           : S=68         SP=68        AP=184       SC=20
 AC=384
arbitrary command execution              : S=272        SP=272       AP=736       SC=80
 AC=1536
web code injection                       : S=17         SP=17        AP=46        SC=5         AC=96

script injection                         : S=2          SP=2         AP=2         SC=2         AC=2

HTML injection                           : S=10         SP=10        AP=10        SC=10        AC=10

arbitrary command execution (time based) : S=102        SP=102       AP=276       SC=30
 AC=576
XML injection                            : S=17         SP=17        AP=46        SC=5         AC=96

unseen parameters                        : S=595        SP=595       AP=1610      SC=175
 AC=3360
```

```
directory traversal (write access)       : S=34         SP=34        AP=92        SC=10
 AC=192
SQL injection (2nd order)                : S=17         SP=17        AP=46        SC=5         AC=96

on site request forgery                  : S=2          SP=2         AP=2         SC=2         AC=2

blind SQL injection (4 requests)         : S=68         SP=68        AP=184       SC=20
 AC=384
HTTP response splitting                  : S=18         SP=18        AP=18        SC=18        AC=18

directory traversal (extended test)      : S=867        SP=867       AP=2346      SC=255
 AC=4896
header injection                         : S=4          SP=4         AP=4         SC=4         AC=4

injectable parameter                     : S=34         SP=34        AP=92        SC=10
 AC=192
local file inclusion                   [...]
```

33817 - CGI Generic Tests Load Estimation (all tests)

Synopsis

Load estimation for web application tests.

Description

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

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8080/www

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

SSI injection                           : S=51         SP=51        AP=138       SC=15
 AC=288
arbitrary command execution (time based) : S=102        SP=102       AP=276       SC=30
 AC=576
cross-site scripting (comprehensive test): S=68         SP=68        AP=184       SC=20
 AC=384
HTTP response splitting                 : S=18         SP=18        AP=18        SC=18        AC=18

web code injection                      : S=17         SP=17        AP=46        SC=5         AC=96

format string                           : S=34         SP=34        AP=92        SC=10
 AC=192
header injection                        : S=4          SP=4         AP=4         SC=4         AC=4

on site request forgery                 : S=2          SP=2         AP=2         SC=2         AC=2

SQL injection (2nd order)               : S=17         SP=17        AP=46        SC=5         AC=96
```

```
directory traversal                      : S=425        SP=425       AP=1150      SC=125
 AC=2400
persistent XSS                           : S=68         SP=68        AP=184       SC=20
 AC=384
blind SQL injection                      : S=204        SP=204       AP=552       SC=60
 AC=1152
script injection                         : S=2          SP=2         AP=2         SC=2         AC=2

blind SQL injection (4 requests)         : S=68         SP=68        AP=184       SC=20
 AC=384
XML injection                            : S=17         SP=17        AP=46        SC=5         AC=96

directory traversal (write access)       : S=34         SP=34        AP=92        SC=10
 AC=192
arbitrary command execution              : S=272        SP=272       AP=736       SC=80
 AC=1536
unseen parameters                       [...]
```

39470 - CGI Generic Tests Timeout

Synopsis

Some generic CGI attacks ran out of time.

Description

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

Solution

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

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

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

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

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

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/80/www

```
The following tests timed out without finding any flaw :
- directory traversal
```

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 :
- directory traversal
- SQL injection (on parameters names)
- XSS (on parameters names)
- SSI injection
- SQL injection
- cross-site scripting (comprehensive test)
```

39470 - CGI Generic Tests Timeout

Synopsis

Some generic CGI attacks ran out of time.

Description

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

Solution

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

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

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

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

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

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8080/www

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

49704 - External URLs

Synopsis

Links to external sites were gathered.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/80/www

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

http://www-142.ibm.com/software/products/us/en/subcategory/SWI10 -
https://github.com/AppSecDev/AltoroJ/   -
```

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

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

http://www-142.ibm.com/software/products/us/en/subcategory/SWI10 -
https://github.com/AppSecDev/AltoroJ/   -
```

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/8080/www

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

http://www-142.ibm.com/software/products/us/en/subcategory/SWI10 - /
https://github.com/AppSecDev/AltoroJ/   - /
```

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/443/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     : JSESSIONID
  Value    : 12F6293F511F493D972C0CE725161D9C
  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 the response to an OPTIONS request :

  - HTTP methods  DELETE  HEAD  OPTIONS  POST  PUT GET
    are allowed on :

    /status_check.jsp
    /swagger


Based on tests of each method :

  - HTTP methods GET HEAD OPTIONS POST are allowed on :

    /
    /status_check.jsp
    /swagger
```

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  DELETE  HEAD  OPTIONS  POST  PUT GET
    are allowed on :

    /status_check.jsp
    /swagger


Based on tests of each method :

  - HTTP methods GET HEAD OPTIONS POST are allowed on :

    /
    /status_check.jsp
    /swagger
```

43111 - HTTP Methods Allowed (per directory)

Synopsis

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

Description

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

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

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

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

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

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

See Also

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

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8080/www

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

  - HTTP methods  DELETE  HEAD  OPTIONS  POST  PUT GET
    are allowed on :

    /status_check.jsp
    /swagger


Based on tests of each method :

  - HTTP methods GET HEAD OPTIONS POST are allowed on :

    /
    /status_check.jsp
    /swagger
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

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

Plugin Output

tcp/80/www

```
The remote web server type is :

Apache-Coyote/1.1
```

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 :

Apache-Coyote/1.1
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

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

Plugin Output

tcp/8080/www

```
The remote web server type is :

Apache-Coyote/1.1
```

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 : GET, HEAD, POST, PUT, DELETE, OPTIONS
Headers :

  Server: Apache-Coyote/1.1
  Content-Type: text/html;charset=ISO-8859-1
  Transfer-Encoding: chunked
  Date: Mon, 16 Oct 2023 14:21:26 GMT
  Connection: close

Response Body :



<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/
xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >
<head>
<title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
```

```
</head>
<body style="margin-top:5px;">
<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
  <table width="100%" border="0" cellpadding="0" cellspacing="0">
  <tr>
      <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283
 height=80/></a></td>
  <td align="right" valign="top">
    <a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</
font></a> | <a id="HyperLink3" href="/index.jsp?content=inside_contact.htm">Contact Us</a> | <a
 id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
          <input type="text" name="query" id="query" accesskey="S" />
          <input type="submit" value="Go" />
  </td>
  </tr>
  <tr>
  <td align="right" style="background-image:url('/images/
gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt="" width=354
 height=60/></td>
  </tr>
  </table>
</form>
</div>
<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif"
 width=12 height=14 style="vertical-align: bottom;" alt="Secure Login"/>   <a id="AccountLink"
 href= [...]
```

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 : GET, HEAD, POST, PUT, DELETE, OPTIONS
Headers :

  Server: Apache-Coyote/1.1
  Content-Type: text/html;charset=ISO-8859-1
  Transfer-Encoding: chunked
  Date: Mon, 16 Oct 2023 14:21:43 GMT
  Connection: close

Response Body :



<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/
xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >
<head>
<title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
```

```
</head>
<body style="margin-top:5px;">
<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
  <table width="100%" border="0" cellpadding="0" cellspacing="0">
  <tr>
      <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283
 height=80/></a></td>
  <td align="right" valign="top">
    <a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</
font></a> | <a id="HyperLink3" href="/index.jsp?content=inside_contact.htm">Contact Us</a> | <a
 id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
          <input type="text" name="query" id="query" accesskey="S" />
          <input type="submit" value="Go" />
  </td>
  </tr>
  <tr>
  <td align="right" style="background-image:url('/images/
gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt="" width=354
 height=60/></td>
  </tr>
  </table>
</form>
</div>
<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif"
 width=12 height=14 style="vertical-align: bottom;" alt="Secure Login"/>   <a id="AccountLink"
 href [...]
```

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/1.1 200 OK

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

  Server: Apache-Coyote/1.1
  Content-Type: text/html;charset=ISO-8859-1
  Transfer-Encoding: chunked
  Date: Mon, 16 Oct 2023 14:21:23 GMT
  Connection: close

Response Body :



<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/
xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >
<head>
<title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
```

```
</head>
<body style="margin-top:5px;">
<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
  <table width="100%" border="0" cellpadding="0" cellspacing="0">
  <tr>
      <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283
 height=80/></a></td>
  <td align="right" valign="top">
    <a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</
font></a> | <a id="HyperLink3" href="/index.jsp?content=inside_contact.htm">Contact Us</a> | <a
 id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
          <input type="text" name="query" id="query" accesskey="S" />
          <input type="submit" value="Go" />
  </td>
  </tr>
  <tr>
  <td align="right" style="background-image:url('/images/
gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt="" width=354
 height=60/></td>
  </tr>
  </table>
</form>
</div>
<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif"
 width=12 height=14 style="vertical-align: bottom;" alt="Secure Login"/>   <a id="AccountLink"
 href= [...]
```

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://65.61.137.117/
  - http://65.61.137.117/feedback.jsp
  - http://65.61.137.117/index.jsp
  - http://65.61.137.117/login.jsp
  - http://65.61.137.117/search.jsp
  - http://65.61.137.117/status_check.jsp
  - http://65.61.137.117/subscribe.jsp
  - http://65.61.137.117/survey_questions.jsp
  - http://65.61.137.117/swagger/index.html
```

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

Synopsis

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

Description

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

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

See Also

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

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

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

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/443/www

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

  - https://65.61.137.117/
  - https://65.61.137.117/feedback.jsp
  - https://65.61.137.117/index.jsp
  - https://65.61.137.117/login.jsp
  - https://65.61.137.117/search.jsp
  - https://65.61.137.117/status_check.jsp
  - https://65.61.137.117/subscribe.jsp
  - https://65.61.137.117/survey_questions.jsp
  - https://65.61.137.117/swagger/index.html
```

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

Synopsis

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

Description

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

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

See Also

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

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

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

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8080/www

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

  - http://65.61.137.117:8080/
  - http://65.61.137.117:8080/feedback.jsp
  - http://65.61.137.117:8080/index.jsp
  - http://65.61.137.117:8080/login.jsp
  - http://65.61.137.117:8080/search.jsp
  - http://65.61.137.117:8080/status_check.jsp
  - http://65.61.137.117:8080/subscribe.jsp
  - http://65.61.137.117:8080/survey_questions.jsp
  - http://65.61.137.117:8080/swagger/index.html
```

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

Synopsis

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

Description

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

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

See Also

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

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/80/www

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

  - http://65.61.137.117/
  - http://65.61.137.117/feedback.jsp
  - http://65.61.137.117/index.jsp
  - http://65.61.137.117/login.jsp
  - http://65.61.137.117/search.jsp
  - http://65.61.137.117/status_check.jsp
  - http://65.61.137.117/subscribe.jsp
  - http://65.61.137.117/survey_questions.jsp
  - http://65.61.137.117/swagger/index.html
```

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

Synopsis

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

Description

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

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

See Also

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

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/443/www

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

  - https://65.61.137.117/
  - https://65.61.137.117/feedback.jsp
  - https://65.61.137.117/index.jsp
  - https://65.61.137.117/login.jsp
  - https://65.61.137.117/search.jsp
  - https://65.61.137.117/status_check.jsp
  - https://65.61.137.117/subscribe.jsp
  - https://65.61.137.117/survey_questions.jsp
  - https://65.61.137.117/swagger/index.html
```

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

Synopsis

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

Description

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

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

See Also

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

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8080/www

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

  - http://65.61.137.117:8080/
  - http://65.61.137.117:8080/feedback.jsp
  - http://65.61.137.117:8080/index.jsp
  - http://65.61.137.117:8080/login.jsp
  - http://65.61.137.117:8080/search.jsp
  - http://65.61.137.117:8080/status_check.jsp
  - http://65.61.137.117:8080/subscribe.jsp
  - http://65.61.137.117:8080/survey_questions.jsp
  - http://65.61.137.117:8080/swagger/index.html
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/09/25

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: 2023/09/25

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: 2023/09/25

Plugin Output

tcp/8080/www

```
Port 8080/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 : 10.6.0
Nessus build : 20103
Plugin feed version : 202310160612
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : fire
```

```
Scan policy used : Web Application Tests
Scanner IP : 192.168.0.100
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 262.210 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 : 2023/10/16 18:52 India Standard Time
Scan duration : 7336 sec
Scan for malware : no
```

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 : JSESSIONID
Path : /
Value : 12F6293F511F493D972C0CE725161D9C
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 : JSESSIONID
Path : /
Value : 12F6293F511F493D972C0CE725161D9C
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 : JSESSIONID
Path : /
Value : 12F6293F511F493D972C0CE725161D9C
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 1
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/80/www

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

  - http://65.61.137.117/
  - http://65.61.137.117/feedback.jsp
  - http://65.61.137.117/index.jsp
  - http://65.61.137.117/login.jsp
  - http://65.61.137.117/search.jsp
  - http://65.61.137.117/status_check.jsp
  - http://65.61.137.117/style.css
  - http://65.61.137.117/subscribe.jsp
  - http://65.61.137.117/survey_questions.jsp
  - http://65.61.137.117/swagger/favicon-16x16.png
  - http://65.61.137.117/swagger/favicon-32x32.png
  - http://65.61.137.117/swagger/index.html
  - http://65.61.137.117/swagger/properties.json
  - http://65.61.137.117/swagger/swagger-ui.css

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

91815 - Web Application Sitemap

Synopsis

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

Description

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/443/www

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

  - https://65.61.137.117/
  - https://65.61.137.117/feedback.jsp
  - https://65.61.137.117/index.jsp
  - https://65.61.137.117/login.jsp
  - https://65.61.137.117/search.jsp
  - https://65.61.137.117/status_check.jsp
  - https://65.61.137.117/style.css
  - https://65.61.137.117/subscribe.jsp
  - https://65.61.137.117/survey_questions.jsp
  - https://65.61.137.117/swagger/favicon-16x16.png
  - https://65.61.137.117/swagger/favicon-32x32.png
  - https://65.61.137.117/swagger/index.html
  - https://65.61.137.117/swagger/properties.json
  - https://65.61.137.117/swagger/swagger-ui.css

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

91815 - Web Application Sitemap

Synopsis

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

Description

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8080/www

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

  - http://65.61.137.117:8080/
  - http://65.61.137.117:8080/feedback.jsp
  - http://65.61.137.117:8080/index.jsp
  - http://65.61.137.117:8080/login.jsp
  - http://65.61.137.117:8080/search.jsp
  - http://65.61.137.117:8080/status_check.jsp
  - http://65.61.137.117:8080/style.css
  - http://65.61.137.117:8080/subscribe.jsp
  - http://65.61.137.117:8080/survey_questions.jsp
  - http://65.61.137.117:8080/swagger/favicon-16x16.png
  - http://65.61.137.117:8080/swagger/favicon-32x32.png
  - http://65.61.137.117:8080/swagger/index.html
  - http://65.61.137.117:8080/swagger/properties.json
  - http://65.61.137.117:8080/swagger/swagger-ui.css

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: 2023/09/25

Plugin Output

tcp/80/www

```
Webmirror performed 27 queries in 36s (0.0750 queries per second)

The following CGIs have been discovered :


+ CGI : /index.jsp
  Methods : GET
  Argument : content
   Value: security.htm


+ CGI : /search.jsp
  Methods : GET
  Argument : query


+ CGI : /default.jsp
  Methods : GET
  Argument : content
   Value: security.htm


+ CGI : /doLogin
  Methods : POST
  Argument : btnSubmit
   Value: Login
  Argument : passw
```

```
  Argument : uid


+ CGI : /sendFeedback
  Methods : POST
  Argument : cfile
   Value: comments.txt
  Argument : comments
  Argument : email_addr
  Argument : name
  Argument : reset
   Value:  Clear Form
  Argument : subject
  Argument : submit
   Value:  Submit


+ CGI : /doSubscribe
  Methods : POST
  Argument : btnSubmit
   Value: Subscribe
  Argument : txtEmail


+ CGI : /survey_questions.jsp
  Methods : GET
  Argument : step
   Value: a


+ CGI : /status_check.jsp/util/serverStatusCheckService.jsp
  Methods : GET
  Argument : HostName
```

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: 2023/09/25

Plugin Output

tcp/443/www

```
Webmirror performed 27 queries in 84s (0.0321 queries per second)

The following CGIs have been discovered :


+ CGI : /index.jsp
  Methods : GET
  Argument : content
   Value: security.htm


+ CGI : /search.jsp
  Methods : GET
  Argument : query


+ CGI : /default.jsp
  Methods : GET
  Argument : content
   Value: security.htm


+ CGI : /doLogin
  Methods : POST
  Argument : btnSubmit
   Value: Login
  Argument : passw
```

```
  Argument : uid


+ CGI : /sendFeedback
  Methods : POST
  Argument : cfile
   Value: comments.txt
  Argument : comments
  Argument : email_addr
  Argument : name
  Argument : reset
   Value:  Clear Form
  Argument : subject
  Argument : submit
   Value:  Submit


+ CGI : /doSubscribe
  Methods : POST
  Argument : btnSubmit
   Value: Subscribe
  Argument : txtEmail


+ CGI : /survey_questions.jsp
  Methods : GET
  Argument : step
   Value: a


+ CGI : /status_check.jsp/util/serverStatusCheckService.jsp
  Methods : GET
  Argument : HostName
```

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: 2023/09/25

Plugin Output

tcp/8080/www

```
Webmirror performed 27 queries in 31s (0.0870 queries per second)

The following CGIs have been discovered :


+ CGI : /index.jsp
  Methods : GET
  Argument : content
   Value: security.htm


+ CGI : /search.jsp
  Methods : GET
  Argument : query


+ CGI : /default.jsp
  Methods : GET
  Argument : content
   Value: security.htm


+ CGI : /doLogin
  Methods : POST
  Argument : btnSubmit
   Value: Login
  Argument : passw
```

```
  Argument : uid


+ CGI : /sendFeedback
  Methods : POST
  Argument : cfile
   Value: comments.txt
  Argument : comments
  Argument : email_addr
  Argument : name
  Argument : reset
   Value:  Clear Form
  Argument : subject
  Argument : submit
   Value:  Submit


+ CGI : /doSubscribe
  Methods : POST
  Argument : btnSubmit
   Value: Subscribe
  Argument : txtEmail


+ CGI : /survey_questions.jsp
  Methods : GET
  Argument : step
   Value: a


+ CGI : /status_check.jsp/util/serverStatusCheckService.jsp
  Methods : GET
  Argument : HostName
```