beSTORM Report

2015 February 28

Project Settings

Name	Value
beSTORM Version:	5.0.3 (6317)
Project Name:	beSTORM project1
Thread Count:	1
Remote Monitor IP Address / Hostname:	127.0.0.1

Module Settings

Module name:	HTTP (Simple)
Fuzzing conditioned elements:	Yes
Generator type:	Text
Increment order:	Normal
Overflow elements once:	No
Scale type:	Base2+/-1
Saturation Rate Threshold:	100
Automatic Saturation Rate Threshold:	no
Batch Mode:	yes
Report Connectivity Issues as Exceptions:	no
Minion Enabled:	no
Minion Host and Port:	unset (6980)

Environment Settings

Name	Value	Type	Required
Body Content (default is set to empty)		Not Set	No
Remote Hostname	127.0.0.1	Not Set	Yes
Remote Port	80	Not Set	Yes
Remote Protocol Type	tcp	Not Set	Yes

Monitor Settings

Monitor Type	Enabled
Monitor Enforcement	yes
ARP Echo	no
ICMP Echo	no
TCP ECho	no
UDP ECho	no
Remote Debugger	yes
Monitored Hostname	127.0.0.1
Monitored Port	unset

Control Ports

Name	Port Number
Incoming Commands	6970
Incoming Exceptions	6969
Outgoing Commands	6971

Default Attack Types

Name	Replicated Buffer	Min	Max	Number Ranging	Binary	Decimal	Hex	Negative	Appender (Type)	Base64
Repeated A	A	0	65536	No	No	Yes	Yes	No	No (Prefix)	No
Repeated %n	%n	0	512	No	No	Yes	Yes	No	No (Prefix)	No
Repeated %25n	%25n	0	256	No	No	Yes	Yes	No	No (Prefix)	No
Repeated Base64 (A)	A	0	16384	No	No	Yes	Yes	No	No (Prefix)	Yes
BiggerSmaller	<>	0	32768	No	No	Yes	Yes	No	No (Prefix)	No
Repeated %00	%00	0	21846	No	No	Yes	Yes	No	No (Prefix)	No
Number Generating DEC		0	-1	Yes	No	Yes	No	No	No (Prefix)	No
Negative Number Generating DEC		0	-2147483648	Yes	No	Yes	No	Yes	No (Prefix)	No
Number Generating HEX		0	-1	Yes	No	No	Yes	No	No (Prefix)	No
Repeated Space		0	65536	No	No	Yes	Yes	No	No (Prefix)	No

Hostname (textual) Attack Types

Name	Replicated Buffer	Min	Max	Number Ranging	Binary	Decimal	Hex	Negative	Appender (Type)	Base64
Broadcast Address	255.255.255.255	0	1	No	No	Yes	Yes	No	No (Prefix)	No
Localhost Address	127.0.0.1	0	1	No	No	Yes	Yes	No	No (Prefix)	No

Multicast Address	239.255.255.253	0	1	No	No	Yes	Yes	No	No (Prefix)	No
Nocast Address	0.0.0.0	0	1	No	No	Yes	Yes	No	No (Prefix)	No
Repeated A (Up to 16 bytes)	A	0	17	No	No	Yes	Yes	No	No (Prefix)	No
NULL (Up to 16 bytes)	00	0	17	No	No	Yes	Yes	No	No (Prefix)	No
Repeated %n (Up to 16 bytes)	%n	0	9	No	No	Yes	Yes	No	No (Prefix)	No
Zero Dot (Up to 4 times)	.0	0	4	No	No	Yes	Yes	No	No (Prefix)	No
255 Dot (Up to 4 times)	.255	0	4	No	No	Yes	Yes	No	No (Prefix)	No
256 Dot (Up to 4 times)	.256	0	4	No	No	Yes	Yes	No	No (Prefix)	No
-1 Dot (Up to 4 times)	.-1	0	3	No	No	Yes	Yes	No	No (Prefix)	No
Repeated A with DotCom	A	0	256	No	No	Yes	Yes	No	No (Prefix)	No
Repeated Number A with Dot	8A.	0	256	No	No	Yes	Yes	No	No (Prefix)	No

Integer (textual) Attack Types

Name	Replicated Buffer	Min	Max	Number Ranging	Binary	Decimal	Hex	Negative	Appender (Type)	Base64
Repeated A (up to 32 Bit)	A	0	12	No	No	Yes	Yes	No	No (Prefix)	No
NULL (Up to 32bit)	00	0	12	No	No	Yes	Yes	No	No (Prefix)	No
Repeated %n (up to 32 Bit)	%n	0	6	No	No	Yes	Yes	No	No (Prefix)	No
Number Generating DEC (32 Bit)		0	-1	Yes	No	Yes	No	No	No (Prefix)	No
Negative Number Generating DEC (32 Bit)		0	-2147483648	Yes	No	Yes	No	Yes	No (Prefix)	No

Running time

beSTORM has been running for (total): **0 months, 0 days 0 hours 0 minutes 55 seconds**

Started	Ended	Duration
23:23:54 02/28/15	23:24:07 02/28/15	0 months, 0 days 0 hours 0 minutes 13 seconds
23:24:10 02/28/15	23:24:27 02/28/15	0 months, 0 days 0 hours 0 minutes 17 seconds
23:24:30 02/28/15	23:24:36 02/28/15	0 months, 0 days 0 hours 0 minutes 6 seconds
23:24:36 02/28/15	23:24:48 02/28/15	0 months, 0 days 0 hours 0 minutes 12 seconds
23:24:51 02/28/15	23:24:54 02/28/15	0 months, 0 days 0 hours 0 minutes 3 seconds
23:25:00 02/28/15	23:25:04 02/28/15	0 months, 0 days 0 hours 0 minutes 4 seconds

Exception Report

beSTORM has found a total of **5** exception(s):

Exception caught on 23:24:07 02/28/15

The following information was reported:

Exception reported on 127.0.0.1 (23:24:07 02/28/15)

During the testing of: Accept-Charset value
Test type: Repeated Base64 (A)

Information:
Monitor stopped responding. Potential vulnerability in tested environment.
Attack Vector List:
M0:P0:B0.BT0:B0.BT0:B0.BT0:SE0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B4.BT4:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0

The following attack vectors have been involved in generating the exception:

M0:P0:B0.BT0:B0.BT0:B0.BT0:SE0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B4.BT4:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0

The following data was used to generate the exception: (show perl script hide perl script)

```
GET / HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.1.6) Gecko/20070723 Iceweasel/2.0.0.6 (Debian-2.0.0.6-1)
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
Referer: http://127.0.0.1/
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: QUFBQQ==
Keep-Alive: 0
Connection: close
Cookie: mycookie
If-Modified-Since: Sun, 07 Oct 2007 01:06:55 GMT
```

Exception caught on 23:24:28 02/28/15

The following information was reported:

Exception reported on 127.0.0.1 (23:24:28 02/28/15)

During the testing of: Referer value
Test type: Number Generating HEX

Information:
Monitor stopped responding. Potential vulnerability in tested environment.
Attack Vector List:
M0:P0:B0.BT0:B0.BT0:B0.BT0:SE0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B9.BT2097152:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0

The following attack vectors have been involved in generating the exception:

M0:P0:B0.BT0:B0.BT0:B0.BT0:SE0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B9.BT2097152:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0

The following data was used to generate the exception: (show perl script hide perl script)

GET / HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.1.6) Gecko/20070723 Iceweasel/2.0.0.6 (Debian-2.0.0.6-1)
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
Referer: 200000
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 0
Connection: close
Cookie: mycookie
If-Modified-Since: Sun, 07 Oct 2007 01:06:55 GMT

Exception caught on 23:24:36 02/28/15

The following information was reported:

Exception reported on 127.0.0.1 by monitor located at 127.0.0.1 (23:24:36 02/28/15)

During the testing of: User-Agent value
Test type: Repeated A

Information:
Page fault on read access to 0x41414141

Stack trace:
ERROR: StackWalk64-Endless-Callstack!, GetLastError: 0 (Address: 41414141)

Attack Vector List:
M0:P0:B0.BT0:B0.BT0:B0.BT0:SE0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B1.BT2049:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0

The following attack vectors have been involved in generating the exception:

M0:P0:B0.BT0:B0.BT0:B0.BT0:SE0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B1.BT2049:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0

The following data was used to generate the exception: (show perl script hide perl script)

GET / HTTP/1.1
Host: 127.0.0.1
User-Agent: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
Referer: http://127.0.0.1/
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 0
Connection: close
Cookie: mycookie
If-Modified-Since: Sun, 07 Oct 2007 01:06:55 GMT

Exception caught on 23:24:48 02/28/15

The following information was reported:

Exception reported on 127.0.0.1 by monitor located at 127.0.0.1 (23:24:48 02/28/15)

During the testing of: HTTP Type
Test type: Repeated Base64 (A)

Information:
Page fault on read access to 0x42465551

Stack trace:
ERROR: StackWalk64-Endless-Callstack!, GetLastError: 0 (Address: 42465551)

Attack Vector List:
M0:P0:B0.BT0:B0.BT0:B0.BT0:SE0:B0.BT0:B0.BT0:B4.BT2049:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0

The following attack vectors have been involved in generating the exception:

M0:P0:B0.BT0:B0.BT0:B0.BT0:SE0:B0.BT0:B0.BT0:B4.BT2049:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0

The following data was used to generate the exception: (show perl script hide perl script)

GET / QUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFB
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.1.6) Gecko/20070723 Iceweasel/2.0.0.6 (Debian-2.0.0.6-1)
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
Referer: http://127.0.0.1/
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 0
Connection: close
Cookie: mycookie
If-Modified-Since: Sun, 07 Oct 2007 01:06:55 GMT

Exception caught on 23:24:54 02/28/15

The following information was reported:

Exception reported on 127.0.0.1 by monitor located at 127.0.0.1 (23:24:54 02/28/15)

During the testing of: HTTP Type
Test type: Repeated %00

Information:
Page fault on read access to 0x30302530

Stack trace:
ERROR: SymGetSymFromAddr64, GetLastError: 126 (Address: 30302530)
ERROR: SymGetLineFromAddr64, GetLastError: 126 (Address: 30302530)
ERROR: SymGetModuleInfo64, GetLastError: 1114 (Address: 30302530)
30302530 ((module-name not available)): (filename not available): (function-name not available)

ERROR: SymGetSymFromAddr64, GetLastError: 126 (Address: 30253030)
ERROR: SymGetLineFromAddr64, GetLastError: 126 (Address: 30253030)
ERROR: SymGetModuleInfo64, GetLastError: 1114 (Address: 30253030)
30253030 ((module-name not available)): (filename not available): (function-name not available)

Attack Vector List:
M0:P0:B0.BT0:B0.BT0:B0.BT0:SE0:B0.BT0:B0.BT0:B6.BT1025:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0

The following attack vectors have been involved in generating the exception:

M0:P0:B0.BT0:B0.BT0:B0.BT0:SE0:B0.BT0:B0.BT0:B6.BT1025:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0:B0.BT0

The following data was used to generate the exception: (show perl script hide perl script)

GET /
%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.1.6) Gecko/20070723 Iceweasel/2.0.0.6 (Debian-2.0.0.6-1)
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
Referer: http://127.0.0.1/
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 0
Connection: close
Cookie: mycookie
If-Modified-Since: Sun, 07 Oct 2007 01:06:55 GMT

Test list

Test Name	Attack Types	Status
SimpleHTTP Protocol	Default	Not done
SimpleHTTP Sequence	Default	Not done
Sender	Default	Not done
Data	Default	Not done
Simple GET HTTP Packet	Default	Not done
Method	Default	Not done
URI	Default	In progress
HTTP Type	Default	Done
HTTP Major	Integer (textual)	Done
HTTP Minor	Integer (textual)	Done
Host value	Hostname (textual)	Done
User-Agent value	Default	Done
Accept value	Default	Done
Referer value	Default	Done
Accept-Language value	Default	Done
Accept-Encoding value	Default	Done
Accept-Charset value	Default	Done
Keep-Alive value	Integer (textual)	Done
Connection value	Default	Done
Cookie value	Default	Done
If-Modified-Since value	Format (textual)	Done
Simple POST HTTP Packet	Default	Not done
Method	Default	Not done
URI	Default	Not done
HTTP Type	Default	Not done
HTTP Major	Integer (textual)	Not done
HTTP Minor	Integer (textual)	Not done
Host value	Hostname (textual)	Not done
User-Agent value	Default	Not done
Accept value	Default	Not done
Referer value	Default	Not done
Accept-Language value	Default	Not done
Accept-Encoding value	Default	Not done
Accept-Charset value	Default	Not done
Keep-Alive value	Default	Not done
Connection value	Default	Not done
Cookie value	Default	Not done
If-Modified-Since value	Default	Not done
Content-Type value	Default	Not done
Content-Length value	Default	Not done
Body	Default	Not done