

Forum:[Hack Forums](#)

Thread: [Shell Upload via phpMyAdmin 4.5.4?](#)

Xphile - April 26, 2017, 11:39 am

Hey all,

I'm currently working through the [Orcus CTF](#) from HackFest last year.

I've already gained access to the PHPMA panel and have access to the MySQL (5.7.16) database, however I now need a shell so I can gain root on the actual VM.

Does anyone have a method of doing this?

Here's some more info about the target:

Code DB Info:

Server: Localhost via UNIX socket
Server type: MySQL
Server version: 5.7.16-0ubuntu0.16.04.1 - (Ubuntu)
Protocol version: 10
User: dbuser@localhost
Server charset: UTF-8 Unicode (utf8)

Code Webserver Info:

Apache/2.4.18 (Ubuntu)
Database client version: libmysql - mysqlnd 5.0.12-dev - 20150407 - \$Id: 241ae00989d1995ffcbbf63d579943635faf9972 \$
PHP extension: mysqli Documentation
PHP version: 7.0.8-0ubuntu0.16.04.3

Code Configuration file:

```
//Set the database access information as constants
```

```
DEFINE ('DB_USER', 'dbuser');  
DEFINE ('DB_PASSWORD', 'dbpassword');  
DEFINE ('DB_HOST', 'localhost');  
DEFINE ('DB_NAME', 'quizdb');
```

```
@ $dbc = new mysqli(DB_HOST, DB_USER, DB_PASSWORD, DB_NAME);
```

```
if (mysqli_connect_error()){  
    echo "Could not connect to MySQL. Please try again";  
    exit();  
}
```

As soon as I complete this VM I'll post a walkthrough for other members playing this CTF series.

Thanks for any helpful suggestions. ?

zifor - April 26, 2017, 4:37 pm

Here what i do if got access to phpmyadmin.

1. Search any writable area in server. Sometime database can write to entire folder of web server, in this case you can write your shell in same folder with index.html. But if database can't write, you can search where is "upload" folder, it's writable folder. or any tmp folder in web server.

Let's say sql can write to html folder.

ex : /var/www/html/site

2. Use SQL command to write shell or any php code you want.

If it longtext, you can create new table and copy all of your code to the column.

- 2a. create table 'shellz' that have one or two column.
- 2b. copy your code to it.

it will look like this if you create two column

table : shellz		
PHP Code		
<?php		

-	id	- code -

-	1	- put your code here -
-		-
-		-

3. Use select to write into file.

Select 'code' from 'shellz' where id=1 into DumpFile "/var/www/html/site/shellz.php";

Correct me if i wrong, i always use click to create syntaxt in phpmyadmin, so i don't remember what syntaxt look correctly, but this is the logic. So you maybe get error if only copy and paste.

4. Access your php code via browser or curl.

Easy.. just little tricky :)

??

Xphile - April 28, 2017, 5:59 am
(Apr 26, 2017 04:37 PM)zifor Wrote: [\[CITE\]](#) -snip-
Thanks for the response. However it seems that this scenario has countermeasures against that. Apparently due to the '--secure-file-priv' option being enabled, I can't write to any files.
Instead, I found another route in and I'm currently trying to obtain root privileges.
Either way, it's greatly appreciated that you tried to help.
Thanks a lot man. ?

Byte-Array - *April 28, 2017, 7:46 am*

Check log files if they are and do log poisoning....