

Forum:[Hack Forums](#)

Thread: [MySQL username + password -- How to connect?](#)

IIBAN - October 22, 2012, 9:24 am

Hi guys,

I already tried to connect to my host via navicat/heidisql: no luck.

Is there any other way to connect to the mysql database, even though the mysql port isn't open?

I have root username + password by the way, just need a way to connect to the database somehow.

Would like to hear your opinions :)

IIBAN - October 22, 2012, 9:30 am

(Oct 22, 2012 09:26 AM)eXpan Wrote: [\[CITE\]](#) SQL Databases tend to only be in the network or only allowing localhost to connect.

You will need to root or shell the webhost on it or any other source that has access.

I have and SQL inject point, can I inflict any damage there? Change the MYSQL user or something like that?

Th3PonyWizard - October 22, 2012, 9:41 am

Port is close? It's being filtered / local only. I don't think you can connect remotely. That is, you'll be able to do so locally with a shell.

(Oct 22, 2012 09:26 AM)eXpan Wrote: [\[CITE\]](#) SQL Databases tend to only be in the network or only allowing localhost to connect.lolwut. If the MySQL service port (Usually 3306) is open, OP will be able to connect remotly with any MySQL application. I guess sysadmins are starting to be aware to the issue, but most of dem are open as I can see.

IIBAN - October 22, 2012, 9:44 am

(Oct 22, 2012 09:41 AM)Th3PonyWizard Wrote: [\[CITE\]](#) Port is close? It's being filtered / local only. I don't think you can connect remotely. That is, you'll be able to do so locally with a shell.

lolwut. If the MySQL service port (Usually 3306) is open, OP will be able to connect remotly with any MySQL application. I guess sysadmins are starting to be aware to the issue, but most of dem are open as I can see.

The port is closed, yes. Already tried logging in remotely and couldn't do so.

So now I will have to continue my hunt in looking for an admin panel... Yay!

Zixem - October 22, 2012, 9:46 am

Look for MySQL client or just do it like I do: (ubuntu)

Code mysql -h host -u root -pEnter password and you're in.

IIBAN - October 22, 2012, 9:57 am

(Oct 22, 2012 09:46 AM)Th3FreakPony Wrote: [\[CITE\]](#) Look for MySQL client or just do it like I do: (ubuntu)

Code mysql -h host -u root -pEnter password and you're in.

ERROR 2003 (HY000): Can't connect to MySQL server on 'x.x.x.x' (111)

Mormaii - October 22, 2012, 11:45 am

If what you want to is shell the website only then check if the SQL user has FILE privileges and do SELECT INTO OUTFILE,etc.. and there you have your shell. If you are interested in the contents of the database then you'll have to upload your shell and then connect via your shell (or localhost to them) to the database.

IIBAN - October 22, 2012, 1:22 pm

(Oct 22, 2012 11:45 AM)mormaii2 Wrote: [\[CITE\]](#) If what you want to is shell the website only then check if the SQL user has FILE privileges and do SELECT INTO OUTFILE,etc.. and there you have your shell. If you are interested in the contents of the database then you'll have to upload your shell and then connect via your shell (or localhost to them) to the database.

The user in my sql injectionpoint does not have writing privileges, so into outfile is out of the option unless I can login to another mysql user. Any suggestions?

Mormaii - October 22, 2012, 1:26 pm

(Oct 22, 2012 01:22 PM)Seventy7 Wrote: [\[CITE\]](#) The user in my sql injectionpoint does not have writing privileges, so into outfile is out of the option unless I can login to another mysql user. Any suggestions?

I do not know anything about what you're trying to do/what is the situation/what you want to accomplish.

IIBAN - October 22, 2012, 1:38 pm

(Oct 22, 2012 01:26 PM)mormaii2 Wrote: [\[CITE\]](#) I do not know anything about what you're trying to do/what is the situation/what you want to accomplish.

Here's the situation:

- I have an injectionpoint from which I dumped the MYSQL users + passwords, the result of this is that I have the password of the root user.

- Now I would like to log into the MYSQL database, so I can add my shell.

My goals: Get a shell on the server. ?

sniffers - October 22, 2012, 1:49 pm

bro, you need sql dumper for connect to mysql

Mormaii - October 22, 2012, 1:51 pm

(Oct 22, 2012 01:38 PM)Seventy7 Wrote: [\[CITE\]](#) Here's the situation:

- I have an injectionpoint from which I dumped the MYSQL users + passwords, the result of this is that I have the password of the root user.

- Now I would like to log into the MYSQL database, so I can add my shell.

My goals: Get a shell on the server. ?

You can look for other domains on the same server so if you can upload a shell to those sites you could log in as root into the database from that domain and upload shell on target site.

IIBAN - October 22, 2012, 2:10 pm

(Oct 22, 2012 01:51 PM)mormaii2 Wrote: [\[CITE\]](#) You can look for other domains on the same server so if you can upload a shell to those sites you could log in as root into the database from that domain and upload shell on target site.

I have access to the wordpress blog of the site, as an administrator, but I can't install plugins/themes = no shell if I am correct.

Mormaii - October 22, 2012, 4:44 pm

(Oct 22, 2012 02:10 PM)Seventy7 Wrote: [\[CITE\]](#) I have access to the wordpress blog of the site, as an administrator, but I can't install plugins/themes = no shell if I am correct.

I don't have any experience with wordpress but i've seen there are ways in which it could be done. Have you tried timthumb?

MrBlah - October 23, 2012, 5:59 am

(Oct 22, 2012 01:38 PM)Seventy7 Wrote: [\[CITE\]](#) Here's the situation:

- I have an injectionpoint from which I dumped the MYSQL users + passwords, the result of this is that I have the password of the root user.

- Now I would like to log into the MYSQL database, so I can add my shell.

My goals: Get a shell on the server. ?

Hint: If you have an injection point and you manually dumped the database you might as well use UDF injection or load_file using the same injection point to upload your shell on the site ..

In case you have no idea what i just said.. please google for more info about it.

IIBAN - October 23, 2012, 7:16 am

(Oct 23, 2012 05:59 AM)MrBlah Wrote: [\[CITE\]](#) Hint: If you have an injection point and you manually dumped the database you might as well use UDF injection or load_file using the same injection point to upload your shell on the site ..

In case you have no idea what i just said.. please google for more info about it.

@@version = 5.1.47-enterprise-gpl-pro-log, so UDF injection is out of the option I reckon. I already tried load_file which didn't work.

I thought of connecting to the database as another (root) user via the SQL injectionpoint, is this even possible?