

Forum:[Hack Forums](#)

Thread: [Get MySQL root pw](#)

TeoZ - October 24, 2015, 11:46 am

Hello to everyone,

I would ask you a lil thing:

Is there any way to get the MySQL password of a server if I have the total access to any file in the (linux) server?

Is there any file i can download to find this mysterious password?

It's not a problem if it is hashed, I just need to find it!

Thank you guys ?

AdamDeJames - October 24, 2015, 2:26 pm

maybe check config files.

IE for mybb, DB info is in /inc/config.php

TeoZ - October 24, 2015, 3:07 pm

I have no such directory, i only have mysql/my.cnf, but there is nothing useful wrote in...hmmm

If, for example, PhpMyAdmin asks me a password for login, how can't be there a file with the password written in? :(

Viktory - October 24, 2015, 5:15 pm

grep thru filesystem for "password" or something

TeoZ - October 25, 2015, 12:56 am

I have tried to take the file debian.cnf but there is nothing written in, tried with the file my.cnf and there isn't any password, tried with mysql.cnf and is empty...

Maybe something in var/lib/mysql?

I may have found the file with the root pw, but i still need help :S

I need to access to the mysql directory (var/lib/mysql) but it is protected from default by Linux, how can I through PHP access to it, and download the file?

Is there any way I can "emulate" Linux termial to use chmod?

Maybe with shell_exec? I don't wanna make damage X)

c00perzz - October 25, 2015, 1:30 pm

www-data user will not give you access to that. You will need privilege escalation...

How bout using your brain - October 26, 2015, 4:32 am

Ehm mysql root password is just stored in the mysql.user database. As a hash. So good luck with that.

Only thing you can do is to reset it, but you will probably have to have root (or mysql user) privs. which means you can just copy the whole mysql database anyway and resetting the root password would be then useless in that case.

TeoZ - October 26, 2015, 5:59 am

(Oct 26, 2015 04:32 AM)How bout using your brain Wrote: [CITE](#) no, you can't decrypt a hash
I wouldn't be so sure about this ?

That's the answer you find on low sites.

(Oct 26, 2015 04:32 AM)How bout using your brain Wrote: [\[CITE\]](#) Ehm mysql root password is just stored in the mysql.user database. As a hash. So good luck with that.

I have found where I can get it, I just need to access to the directory, because PHP can't access to it, so I cannot download the file.

(Oct 25, 2015 01:30 PM)c00perzz Wrote: [\[CITE\]](#) www-data user will not give you access to that. You will need privilege escalation...

Can you make me a little example of this?

[img]http://forums.tigsource.com/Smileys/derek/beg.gif[/img]

How bout using your brain - October 26, 2015, 6:03 am

(Oct 26, 2015 05:59 AM)TeoZ Wrote: [\[CITE\]](#) I wouldn't be so sure about this ?

I am 100% certain about this ?

(Oct 26, 2015 05:59 AM)TeoZ Wrote: [\[CITE\]](#) I have found where I can get it, I just need to access to the directory, because PHP can't access to it, so I cannot download the file.If you had access to that directory, you could just download the whole databases, no need to get root password...

Sharkky - October 26, 2015, 6:23 am

No, hash are one-way, it is impossible for anyone to decrypt a hash.

But you can use rainbow tables ; You hash a dictionary, so that you know what are the plaintext for the hash that are in your dictionary.

And then you grep through it for the hash, and you'll find the corresponding pass.

But if the password wasn't originally in your dictionary, you won't get any match.

Anyway, mysql is a relatively reliable service.

You can google "mysql privilege escalation", but you won't find much, and this will be rather complicated.

Glubz - October 26, 2015, 7:27 am

Sometimes it's hidden and you have to search through the entire table until you find something juicy.

TeoZ - October 26, 2015, 8:09 am

(Oct 26, 2015 06:23 AM)Sharkky Wrote: [\[CITE\]](#) Anyway, mysql is a relatively reliable service.

You can google "mysql privilege escalation", but you won't find much, and this will be rather complicated.

Yeah, i tried it, and that's the reason I asked him to give me a little example ?

(Oct 26, 2015 06:03 AM)How bout using your brain Wrote: [\[CITE\]](#) If you had access to that directory, you could just download the whole databases, no need to get root password...

I have the access to the database through a "only read" user, so I want to take the root password, to connect to the db with it, and perform an UPDATE query ?

Through a PHP file that I can edit, i can access to the entire server, but (I checked it on a Linux pc of mine) the folder of mysql is protected, and to unlock it I needed to use "chmod 0777" on linux terminal...

I saw PHP cannot access to that folder when i tried to print all files in that (scandir), showing me nothing...

How bout using your brain - October 26, 2015, 8:24 am

(Oct 26, 2015 08:09 AM)TeoZ Wrote: [\[CITE\]](#) Through a PHP file that I can edit, i can access to the entire server, but (I checked it on a Linux pc of mine) the folder of mysql is protected, and to unlock it I needed to use "chmod 0777" on linux terminal...

You can not. You have to be root or the owner of the file/directory. In your case that is the "mysql" user, while php is running under "www-data" user. You can not change the permissions of files you do not own.

Hooded Robin - October 26, 2015, 12:29 pm

by default MySQL stores the databases in files in (select @@datadir) directory, typically /var/lib/mysql/. The mysql user table contains the login credentials for mysql and is the one you are looking for. Assuming @@datadir maps to /var/lib/mysql/ then you would want to look for the file /var/lib/mysql/mysql/user.MYD. By default on Debian/Ubuntu you need privileged permissions to access these files, on Windows it's less restricted typically. ?

If you have privileged mysql access or sqli, then just query the user table directly to dump the values:

Code select host,user,password,super_priv,file_priv from mysql.user

limainfinita - October 26, 2015, 4:24 pm

you just have to check the config files

that is easy if you use c99 shell as it as an option to search for all the config files in the system.

SIM-1073426 - October 27, 2015, 4:43 am

<https://hackmag.com/security/hacking-mysql-databases-methods-and-tools/>

See if this helps, haven't actually read it myself though. Lol

TeoZ - October 27, 2015, 6:03 am

(Oct 26, 2015 04:24 PM)limainfinita Wrote: [\[CITE\]](#) you just have to check the config files that is easy if you use c99 shell as it as an option to search for all the config files in the system. I already tried to upload a shell but it doesn't work, I may not have necessary permissions... Moreover I prefer not to leave on the server any trace, and I would keep it as last try...

(Oct 27, 2015 04:43 AM)Aces. Wrote: [\[CITE\]](#)
<https://hackmag.com/security/hacking-mysql-databases-methods-and-tools/>

See if this helps, haven't actually read it myself though. Lol

Damn that's so long ?

Asap i will give it a read, ty :)

(Oct 26, 2015 08:24 AM)How bout using your brain Wrote: [\[CITE\]](#) You can not. You have to be root or the owner of the file/directory. In your case that is the "mysql" user, while php is running under "www-data" user. You can not change the permissions of files you do not own.

That's a bad piece of news :(

(Oct 26, 2015 12:29 PM)Hooded Robin Wrote: [\[CITE\]](#) by default MySQL stores the databases in files in (select @@datadir) directory, typically /var/lib/mysql/. The mysql user table contains the login credentials for mysql and is the one you are looking for. Assuming @@datadir maps to /var/lib/mysql/ then you would want to look for the file /var/lib/mysql/mysql/user.MYD. By default on Debian/Ubuntu you need privileged permissions to access these files, on Windows it's less restricted typically. ?

If you have privileged mysql access or sqli, then just query the user table directly to dump the values:

```
Code select host,user,password,super_priv,file_priv from mysql.user
```

Yeah, that's the file I'm trying to download, but when I try to access to that directory through PHP it found no files in it.

I have a "just read" user, so I see only some database, for example I don't see "mysql" database when i connect to the server through workbench...

limainfinita - October 27, 2015, 1:50 pm

why do you want to mysql root tho?

TeoZ - October 28, 2015, 11:13 am

Why do you want to know it tho?

PS: already told

limainfinita - October 29, 2015, 9:08 am

(Oct 28, 2015 11:13 AM)TeoZ Wrote: [\[CITE\]](#) Why do you want to know it tho?

PS: already told

sorry cant find that part you explain why

TeoZ - October 29, 2015, 9:16 am

Need to perform an update query

Key Punch - October 29, 2015, 8:30 pm

If it was me I would first attempt using the full arsenal of metasploit and/or bypass any remote brute forcing restrictions with the meterpreter portfwd and routing functionality. and/or attempt all potential mysql exploits(may already be metasploit modules for the majority of them). it may be worth wild pivot attacking to another machine to gain a better foothold within the network the target is currently connected too.

To sum it up I would proceed in this order..

1. if you currently have access to a non root mysql password see what GRANT privileges you may have.. <-- Few cases you may not have sufficient permissions to retrieve the MYSQL root hash but you may be able to grant yourself that privilege.

2. Attempt to dump the MYSQL hashes via exploitation through metasploit modules and/or manual exploitation.

3. Attempt a pivot attack to gain a better foothold <-- Find the CIDR (subnet range) via meterpreter or linux "ifconfig -all" // windows "ipconfig /all" and proceed with an arpscan/tcp ping range scan and maybe spice it up with a little service/os detection.. Remember to modify the active routing tables via meterpreter/manual relay..

4. If the pivot attack was successful it may be worth wild attempting to enumerate the hashes a neighboring system that also uses MYSQL and attempt to use the enumerated MYSQL root password to authenticate as root on the initial target machine. System admins use a universal root/sa passwords across the local network more times then they don't..

5. Capture some ftp/smb/etc... flavored packets and see what juicy passwords you can get then attempt to authenticate as root with the newly gathered passwords..

6. as a last resort you could attempt to social engineer the sysadmin posing as someone from security or the customer of that computer and request a local password reset..

Hopefully these steps will solve the issue you are experiencing. :)

TeoZ - *October 30, 2015, 7:47 am*

Ehm, I can't understand these things, I'm not a pro hacker XD
May you help me through skype or what else?

To answer to the first point:

I already checked it, and the user I use can only use the "select" command.

TeoZ - *November 1, 2015, 1:33 am*

Maybe they use the same pw for all users, but don't know the name :S
I tried just with root and it doesn't work.