

Forum:[Hack Forums](#)

Thread: [Hacked a popular website](#)

Generals - August 17, 2015, 12:08 am

Hi i just hacked a popular website and i look up their source code to get the MSSQL login Credential via MySQL Injection (they has 2 SQL servers).

so how i can connect remotely to their MSSQL server ?

any kind of replies is appreciated, Thanks in advance. ?

Spoiler ([Click to View](#))

yes, i'm a skid

Wireless Network - August 17, 2015, 12:15 am

Do you have shell on site? Some shells has built in feature so you can login throught it.

Generals - August 17, 2015, 12:28 am

(Aug 17, 2015 12:15 AM)Wireless Network Wrote: [\[CITE\]](#) Do you have shell on site? Some shells has built in feature so you can login throught it.

I don't have a shell on the site, i unable to upload shell because the username is not "root", but i cracked their root mysql password (too bad that they're not using phpmyadmin as their MySQL Manager). ?

Frosteh - August 17, 2015, 1:31 am

Port scan the website and see what ports are open, the default remote admin port for MySQL is 3306, if that port is open you might be able to connect providing they don't have any IP restrictions on their firewall or MySQL config.

Also check for SSH ports which are open for remote shell access, you can do MySQL through SSH easy enough, so look for ports around the 22-23 range.

If you didn't shell the site how are you viewing source code?

dongrat - August 17, 2015, 3:36 am

what website is it? :P tell me plz

Generals - August 18, 2015, 9:17 am

(Aug 17, 2015 01:31 AM)Frosteh Wrote: [\[CITE\]](#) Port scan the website and see what ports are open, the default remote admin port for MySQL is 3306, if that port is open you might be able to connect providing they don't have any IP restrictions on their firewall or MySQL config.

Also check for SSH ports which are open for remote shell access, you can do MySQL through SSH easy enough, so look for ports around the 22-23 range.

If you didn't shell the site how are you viewing source code?

i look up their "/etc/passwd" file , mysql's SSH is set to "nologin" and the MySQL root password & MSSQL admin password is not the same as their root SSH/Server password . the MySQL user has read file privilege, so i can read/view their source code, but i can't view "/etc/shadow" file due to

permission issue.

rootsh3ll - August 18, 2015, 2:23 pm

You can use HeidiSQL to login remotely to MSSQL server.

here is the video link: <https://www.youtube.com/watch?v=gjREfF5C4RQ>

ShNuG - August 18, 2015, 7:36 pm

there's a shell called sophie which connects to the MSSQL DB and gets you information. You just need to know some basic MSSQL commands for data retrieval.

Here's the link : <http://www.exploresecurity.com/wp-content/uploads/custom/sophie.aspx>

Here's the link if you want to know more about it :

<http://www.exploresecurity.com/sophie-a-web-sql-shell/>

If you need any help, HMU ?

FFY00 - August 19, 2015, 2:34 pm

U can use MySQL Workbench to acess the SQL remotly...

boribari - August 26, 2015, 11:52 am

to you can login mysql server first you need know the mysql server ip .

Th3PonyWizard - August 27, 2015, 12:19 am

(Aug 19, 2015 02:34 PM)FFY00 Wrote: [\[CITE\]](#) U can use MySQL Workbench to acess the SQL remotly... (Aug 26, 2015 11:52 AM)boribari Wrote: [\[CITE\]](#) to you can login mysql server first you need know the mysql server ip .MySQL by default is configured not to accept remote connections.

SIM-2223238 - August 27, 2015, 12:21 am

(Aug 27, 2015 12:19 AM)Th3PonyWizard Wrote: [\[CITE\]](#) MySQL by default is configured not to accept remote connections.

Most of the servers allow remote connection tho.

Th3PonyWizard - August 27, 2015, 12:24 am

(Aug 27, 2015 12:21 AM)Aggron Wrote: [\[CITE\]](#) Most of the servers allow remote connection tho. Depends how it is being setup. Most big hosting companies allow remote connections from their own nodes to their own MySQLs. Meaning that the MySQL servers have an array of whitelisted IPs that they consider safe. Popular websites (VPSs, unique setups) wouldn't fuck up this bad usually

netpulse - August 27, 2015, 11:02 am

You can try to use navicat

ItsDrosenBerg - December 24, 2015, 11:14 pm

hey bro i wanna buy your ig liker but i cant pm yet, can you pm me your skype or kik