

Forum:[Hack Forums](#)

Thread: [What to do after wp-config.php?](#)

Nurox2019 - October 20, 2019, 10:45 pm

Hi Guys,

I found a wp-config file on a site with the username and password defined for the MySQL database.

I am trying to find out where to actually log in now.

The DB host defined is just localhost. Is there anyway I can log in with these credentials?

Numinous - October 20, 2019, 10:47 pm

You need to find out their Phpmyadmin page, usually the path is example.com/phpmyadmin or example.com:3306

Or you can also try example.com/db.php or example.com/adminer.php etc

Nurox2019 - October 20, 2019, 11:06 pm

(Oct 20, 2019 10:47 PM)Numinous Wrote: [\[CITE\]](#) You need to find out their Phpmyadmin page, usually the path is example.com/phpmyadmin or example.com:3306

Or you can also try example.com/db.php or example.com/adminer.php etc

Hey thanks for the reply. Tried your suggestions wasn't able to pull anything up. Used nmap, there's no information about port 3306. Any other ways of trying to find this? I gave spidering a shot with ZAP haven't seen anything interesting so far.

Open ports if relevant:

21/tcp filtered ftp
22/tcp open ssh
23/tcp filtered telnet
80/tcp open http
110/tcp filtered pop3
143/tcp filtered imap
443/tcp open https
3389/tcp filtered ms-wbt-server

hackologist - October 21, 2019, 10:08 am

run a reverse ip scan and if you are lucky enough to get shell to any web of same server you can use adminer and login into DB :)

scalp3r - October 22, 2019, 1:51 pm

If you've got access to wp-config.php, you most likely have access to other interesting files and folders you should be poking around in.

Different hosting co's will require different configs for mysql db access. The providers that use 'localhost' provide clients with cPanel, Plesk, and directAdmin.

In this case, MySQL and the wordpress database it manages is installed on the server. On the

server it probably lives somewhere like /var/lib/mysql/_DATA_BASE_NAME

Odds are that the hosting co already had phpmyadmin installed, that the site owner "is managing" from their cPanel, when logged into the hosting co's VPS.

Try the creds in the default /wp-login.php page, the owner could have used the same for both... seeing as they didn't configure the directory access correctly.

To access that db, I believe you need the site owners creds for the web host they use. That is the safest/more-silent way to get access.

Nurox2019 - November 4, 2019, 12:56 am

(Oct 22, 2019 01:51 PM)scalp3r_ Wrote: [\[CITE\]](#) If you've got access to wp-config.php, you most likely have access to other interesting files and folders you should be poking around in.

Different hosting co's will require different configs for mysql db access. The providers that use 'localhost' provide clients with cPanel, Plesk, and directAdmin.

In this case, MySQL and the wordpress database it manages is installed on the server. On the server it probably lives somewhere like /var/lib/mysql/_DATA_BASE_NAME

Odds are that the hosting co already had phpmyadmin installed, that the site owner "is managing" from their cPanel, when logged into the hosting co's VPS.

Try the creds in the default /wp-login.php page, the owner could have used the same for both... seeing as they didn't configure the directory access correctly.

To access that db, I believe you need the site owners creds for the web host they use. That is the safest/more-silent way to get access.

Thanks guys. Sorry for the late reply I was busy with some things and I mistakenly thought that I no longer had access to wp-config.

Turns out I still have access and you were right they do have phpmyadmin installed. I tried poking around and couldn't find anything else interesting, trying the credentials in the wp-login.php file was one of the first things I tried before posting here, to no luck.

I did a whois search on the domain and figured out they were registered with ovh.com.

I did some further digging and found out that they had a public phpmyadmin portal that can be found here: [phpMyAdmin](#) (relax it automatically embedded the link, I'm not trying to hack anyone, it's just for reference)

The server parameter appears to just be <username>.mysql.db.ha.ovh.net

I believe it is referring to the username of the database (which as we know I have). Trying to enter that in along with the password did not work, the actual mysql database was not found so I then tried the privatesql suggestion in the box when you hover over the server parameter, also did not work and it asked for a port. The ports have changed since the last time I posted the open ports are here:

```
22/tcp open  ssh
80/tcp open  http
443/tcp open https
3000/tcp closed ppp
8000/tcp closed http-alt
```

8443/tcp open https-alt

None really scream at me (tried to log into ssh it is misconfigured and hence unable to log in as it returns public key cert on filezilla).

I am under the assumption that this is an old mysql database that maybe has not been updated because this server address did not work (which is the conventional server address). I then tried the two links below for mysql 4 and mysql5.1

Tried entering in the same format as the previous phpmyadmin page and no results but after watching an older video on how to setup a mysql database which would have been how the admin would have setup at the time I realized the server address follows a different convention for example: mysql51-127.perso rather than <username>.mysql.db.ovh.net

I know I've just given a lot of information so it may be unlikely that anyone can be bothered shedding some light on retrieving the server address lol.

I'd greatly appreciate the insight if anyone is willing.

I must say it was very interesting following this trail, I feel so close but without the server address I'm pretty much stumped.

Just as a side note, wpscan showed an interesting bug:

Title: Arigato Autoresponder and Newsletter <= 2.5.1.8 - Authenticated Blind SQL Injection & Multiple XSS

| Fixed in: 2.5.2

| References:

- | - [Arigato Autoresponder and Newsletter](#)
- | - [CVE - CVE-2018-1002001](#)
- | - [CVE - CVE-2018-1002000](#)
- | - [CVE - CVE-2018-1002007](#)
- | - [CVE - CVE-2018-1002008](#)
- | - [CVE - CVE-2018-1002009](#)
- | - [WordPress Plugin Arigato Autoresponder and Newsletter 2.5 - Blind SQL Injection /](#)

[Reflected Cross-Site Scripting - PHP webapps Exploit](#)

- | - [Larry Cashdollar Vulnerability](#)
- | - [Changeset 1963802 for bft-autoresponder WordPress Plugin Repository](#)

Unfortunately it requires me to be authenticated which is sort of a loss at the moment :(

Thanks everyone for all of your help so far.

EDIT: I also thought that I should probably add, I am trying to get into web app penetration testing. I don't really care for hacking for profit or anything I'm just really enjoying it. The site in question is actually one of my favourite websites, I am planning to report this to them if I can pull this off (they are a hacking website themselves lol).