Write Up CTF-JOINTS-2023

Team : Haripotar
Asal : SMKN 04 Malang
Anggota :

- **Fikri Muhammad Abdillah (FlaB) - Captain**
- **Firda Gheitsa Sahira (abcfirdaa)**

A. Cryptography

1. Easy CBC

   Kami mendapatkan file challenge.py dan out.bmp, dari script python, terlihat bahwa gambar tersebut di encrypt menggunakan AES-CBC.
   Lalu kami langsung saja membuat script decryptnya, yang sebenarnya hanya mengganti function Encrypt AES, menjadi decrypt.

```
from cryptography.hazmat.primitives.ciphers import Cipher, algorithms, modes
from cryptography.hazmat.backends import default_backend
import PIL.Image as Image

class CBCDecryption:
    def __init__(self, key, iv):
        self.cipher = Cipher(algorithms.AES(key), modes.CBC(iv),
backend=default_backend())
        self.decryptor = self.cipher.decryptor()

    def decrypt(self, image):
        return self.decryptor.update(image)

    def finalize_decrypt(self):
        return self.decryptor.finalize()

def DecryptImage(decryption, image, output):
    image = Image.open(image)
    image.save('temp.bmp')
    with open('temp.bmp', 'rb') as reader:
        with open(output, 'wb') as writer:
            image_data = reader.read()
            header, body = image_data[:54], image_data[54:]
            body += b'\x35' * (16 -(len(body) % 16))
            body = decryption.decrypt(body) + decryption.finalize_decrypt()
            writer.write(header + body)
            writer.close()
            reader.close()
```

```python
def main():
    key = b'JOINTSCTF2023'
    key = key.ljust(32, b'\x35')

    iv = key[:16]
    iv = bytearray(iv)
    for i in range(16):
        iv[i] = iv[i] ^ 0x35
    iv = bytes(iv)

    AesCbc = CBCDecryption(key, iv)
    DecryptImage(decryption=AesCbc, image='out.bmp', output='flag.jpg')

if __name__ == '__main__':
    main()
```

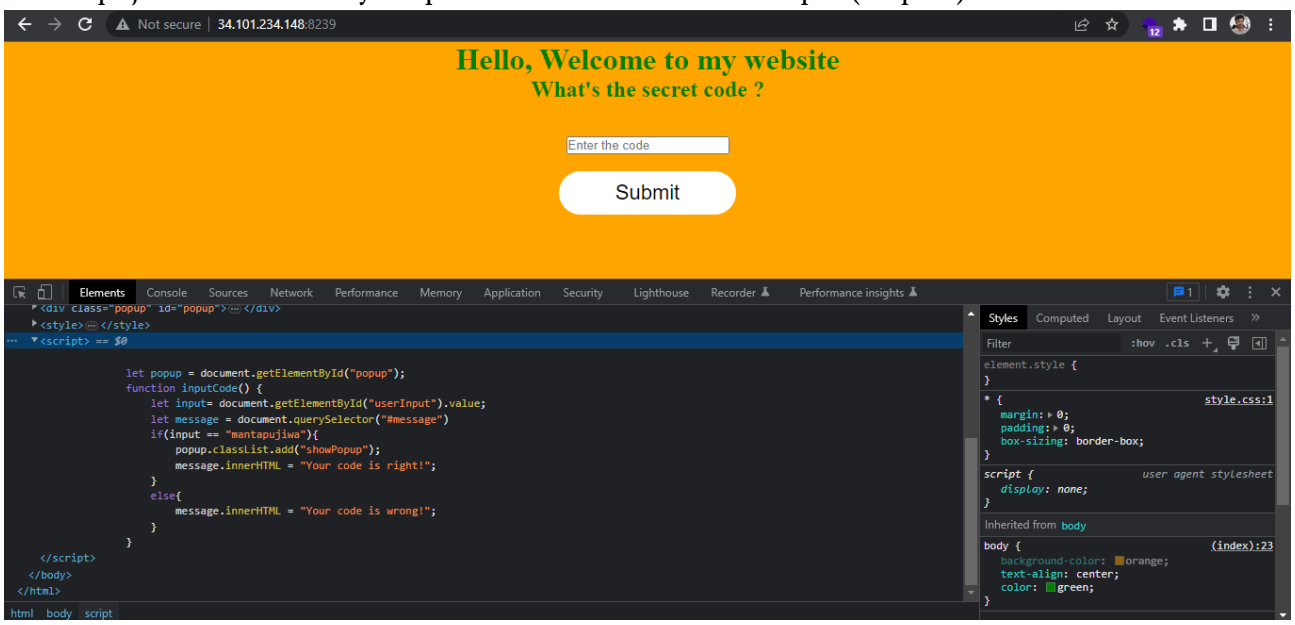
dan kami pun mendapatkan flag nya

FLAG: **JCTF2024{n4rim0_in9_pAndum}**

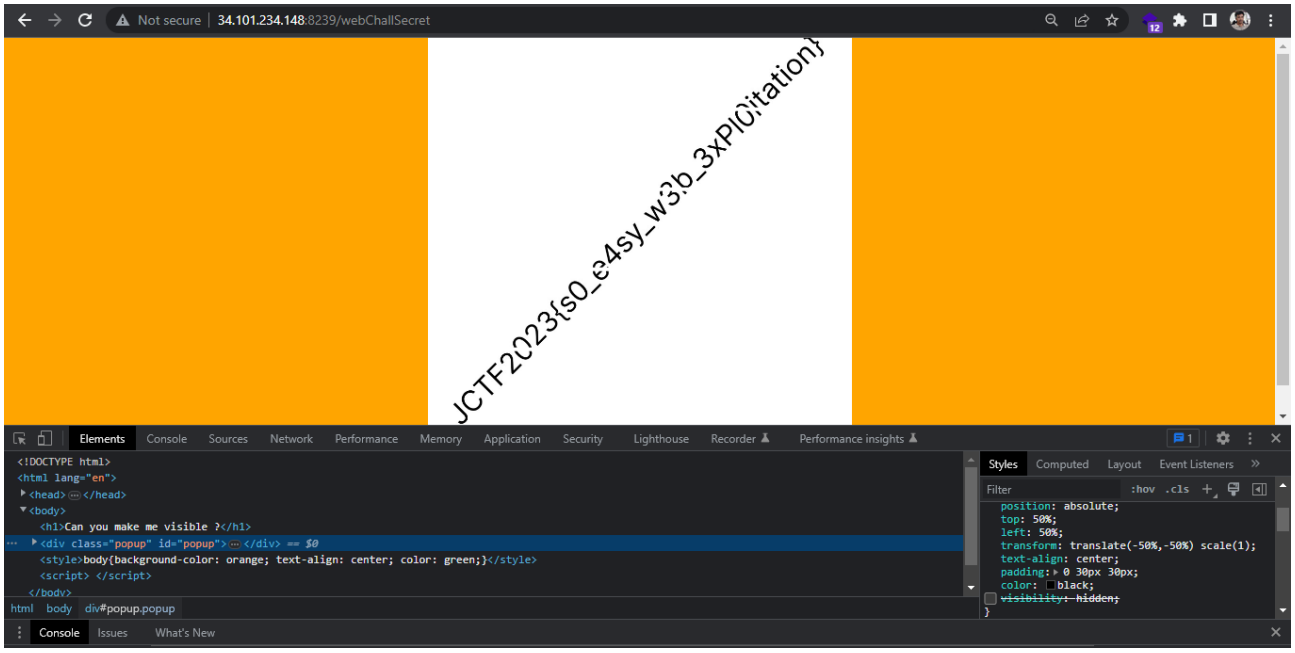
B. Web Exploitation

1. Vision

Kami mendapatkan link web, dan disana disuruh memasukkan password yaitu `mantapujiwa`. Password nya dapat di lihat saat mode developer (Inspect).



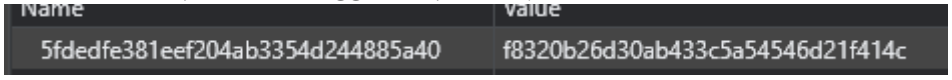
Selanjutnya terdapat gambar flag, namun flag tersebut tidak terlihat. Untuk menampakannya dapat menggunakan mode developer (Inspect), lalu menekan element, dan uncheck `visibility: hidden;` pada tab style.



FLAG: **JCTF2023{s0_e4sy_w3b_3xPl0itation}**

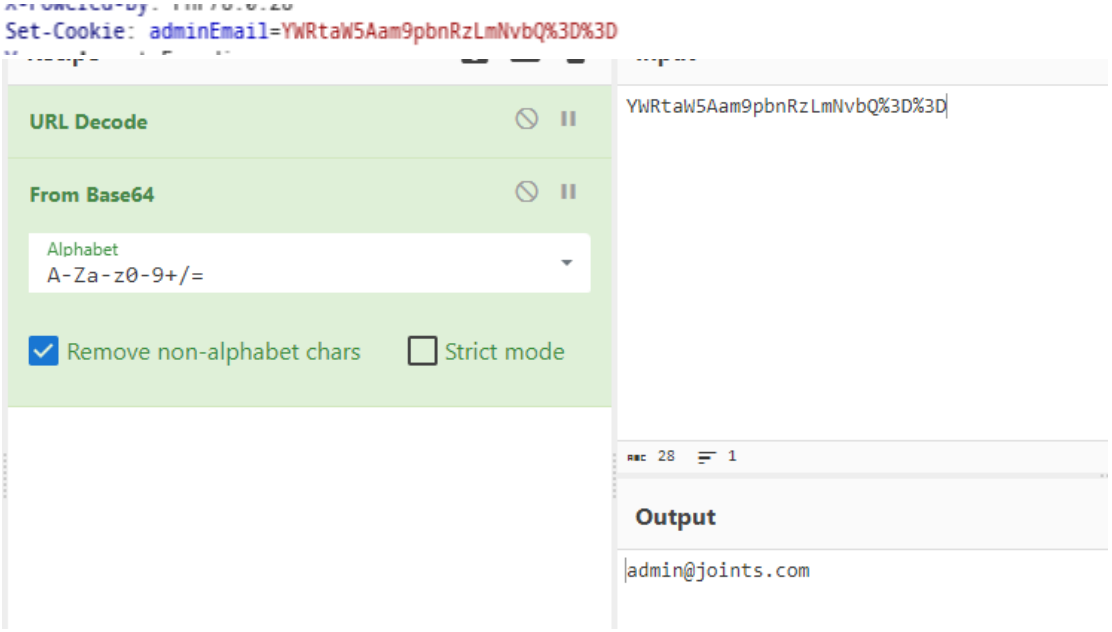
2. LoG1n

Kami mendapatkan link web. Didalam web tersebut terdapat login, lalu kami pun masuk sebagai guest. Saat check cookies, terdapat cookies yang tidak normal, saat saya mencoba decrypt, ternyata string cookies tersebut berupa encrypt md5 yang bertuliskan `isAdmin: False`, lalu saya pun menggantinya menjadi True.



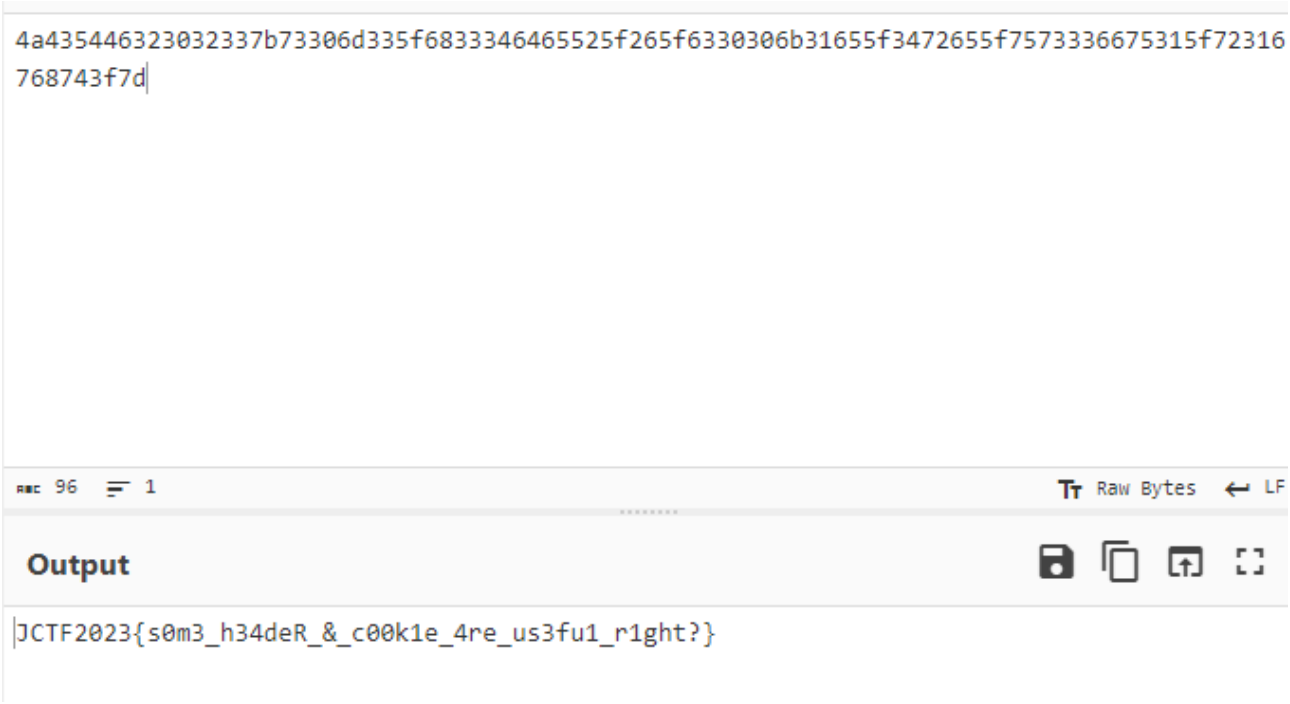
Kami pun mendapatkan link `secret_thing_is_here/flag`. Saat masuk ke dalam link tersebut, kami pun mendapatkan teka teki, sebagai berikut:

- You are not the admin, the admin speaking Urdu
  (Accept-Language: ur)
- The admin only use SuperSecretAdminBrowser
  (User-Agent: SuperSecretAdminBrowser)
- Email (From: admin@joints.com)



- U was Tracker, use untracked one
  (DNT: 1)

Dan langsung redirect ke flag asli, dan mendapatkan flag yang di encryprt base-64



FLAG: **JCTF{s0m3_h34deR_&_c00k1e_4re_us3fu1_r1ght?}**

C. Reverse Engineering

1. For You

   Disini kami mendapatkan file `4u.txt`, didalamnya terdapat assembly code python, saya pun menuliskan nya kedalam python karna tidak dapat menggunakan toolnya.

```
import re
s = ('2', '_', 'e', 'n', 'u', 's', '3', '3', 'n', 'n', 'T', 'C', '_', '_', '2',
'0', 'r', 't', 'g', '1', '0', '_', 'J', 'h', 's', 'w', '{', '4', 'e', 'u', '3',
'y', '}', '_', '3', 'F', 'o', 'd', '_', 'e', 'j', 'i', 't')
s = s[::-1]
r = open("res.pyasm").read().split("\n\n")
for x in r[3:]:
    x = re.search(f"LOAD_CONST +\d+ \(\d+\)", x).group()[:-1].split("(")[1]
    print(s[int(x)], end="")
```

```
PS D:\Programming\Cyber Security\CTF-Joints 2023\Reverse Engginering\1\try> python .\solve.py
JCTF2023{w3_just_engin33red_th1s_0ne_4_you}
PS D:\Programming\Cyber Security\CTF-Joints 2023\Reverse Engginering\1\try>
```

FLAG: **JCTF2023{w3_just_engin33red_th1s_0ne_4_you}**

D. OSINT

1. whereIsThis

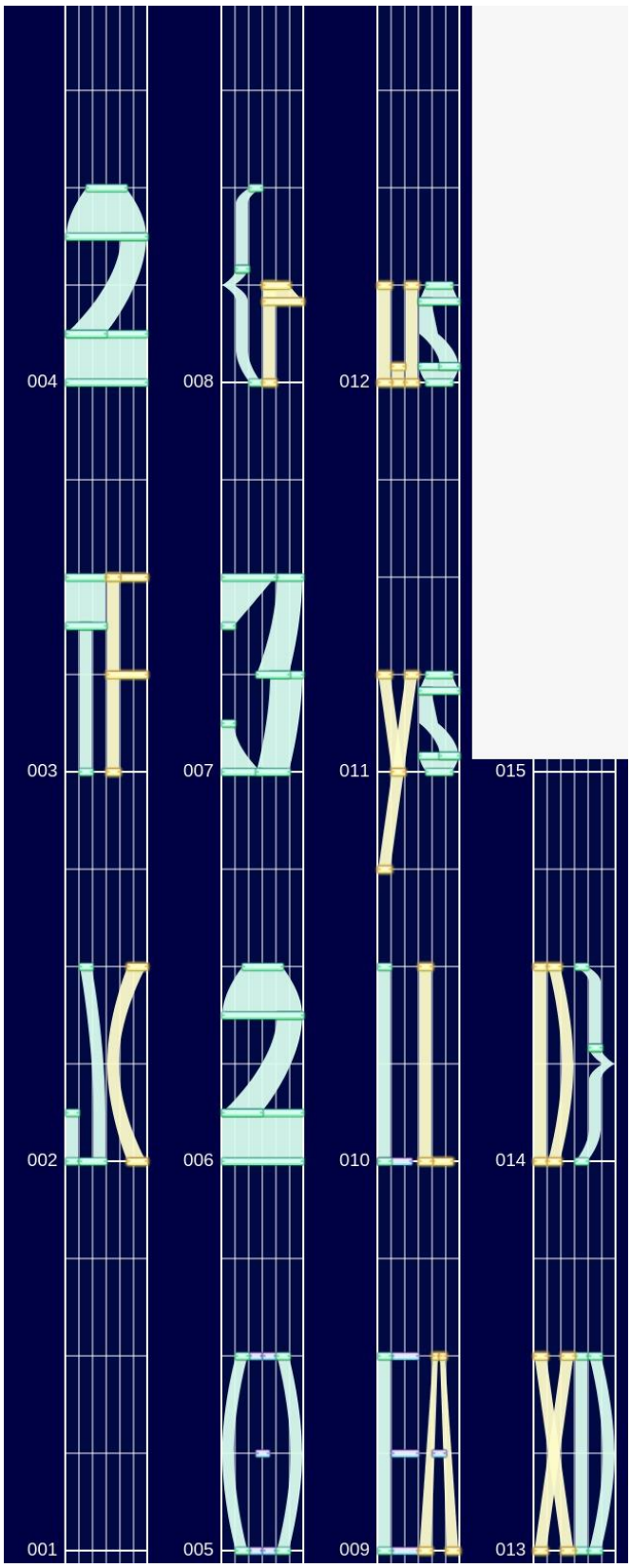
   Disini kami mendapatkan foto. Saat menggunakan exiftool, kami tidak mendapatkan apapun. Jadi kami mencari nama tempat yang terlihat (`pentol mbokdhe`). Kami pun menemukan lokasi nya yang berada pada kota Yogyakarya, dan kami pun mendapatkan flag nya

   FLAG: **JCTF2023{69FC+8V_TERBAN}**

E. Misc

1. Mega SUS

   Disini kami mendapatkan file `flag.sus`, disana terdapat hint berupa `Project Sekai` dan `Rhythm`. Awalnya kami kira, itu adalah file OSU karena ekstensi file tersebut sama dengan nama soalnya yang membuat kami berfikir ekstensi tersebut tidak perlu dihiraukan. Setelah mencari lebih jauh, akhirnya kami menemukan cara menggunakan file tersebut dengan melihat ekstensi file tersebut `.sus`, kami menggunakan tool `sus to image converter` dan mendapatkan flag nya



Dan kami pun mendapatkan flag
FLAG: **JCTF2023{rEALLysusXDD}**