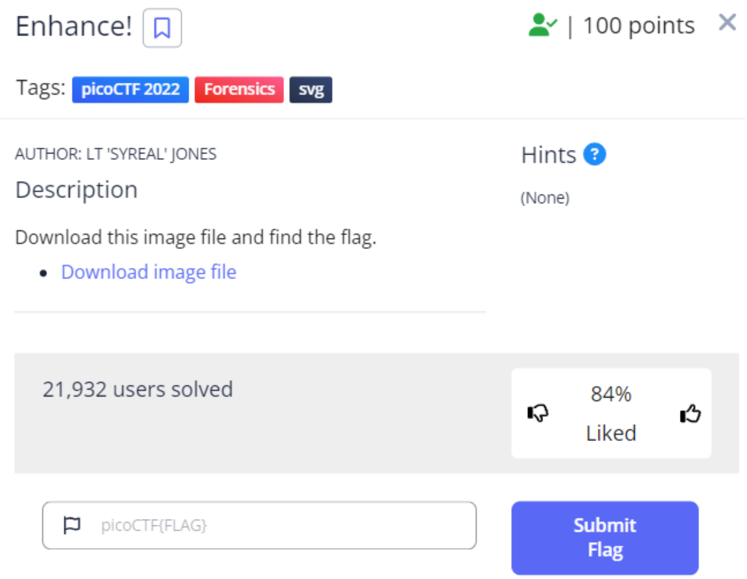
PicoCTF writeups 2022 - Mantone Malikhetla

Enhance



Enhance! | 100 points

Tags: picoCTF 2022 Forensics svg

AUTHOR: LT 'SYREAL' JONES

Description

Download this image file and find the flag.

- Download image file

Hints

(None)

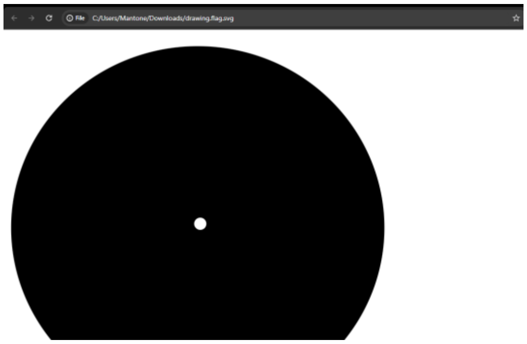
21,932 users solved

84% Liked

picoCTF{FLAG}

Submit Flag

This is what the image looks like

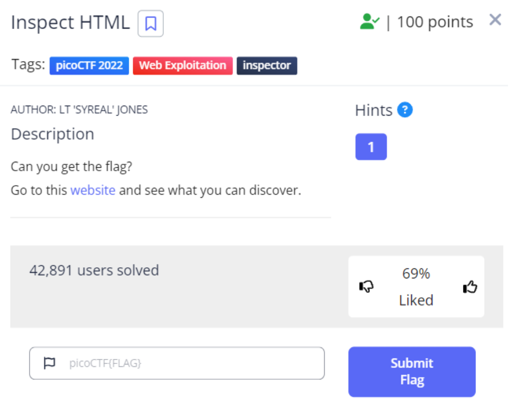


Opened svg file in Notepad++

XML text with the clue in the text

Flag : picoCTF{3nh4nc3d_24374675}

Inspect HTML



Inspect HTML

| 100 points

Tags: picoCTF 2022 Web Exploitation inspector

AUTHOR: LT 'SYREAL' JONES

Description

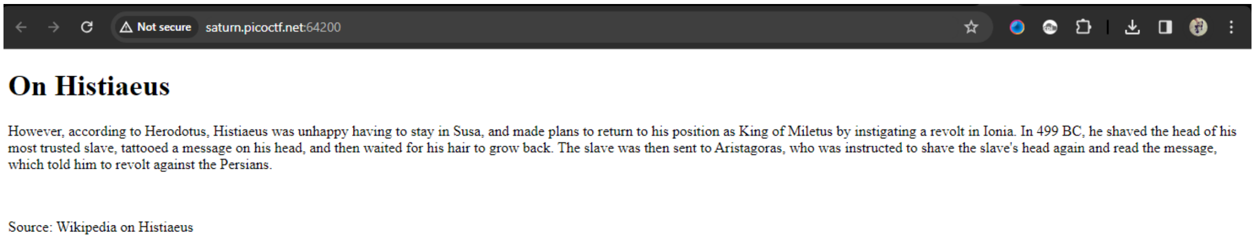
Can you get the flag?

Go to this website and see what you can discover.

Hints

42,891 users solved

69% Liked



Not secure saturn.picoctf.net:64200

On Histiaeus

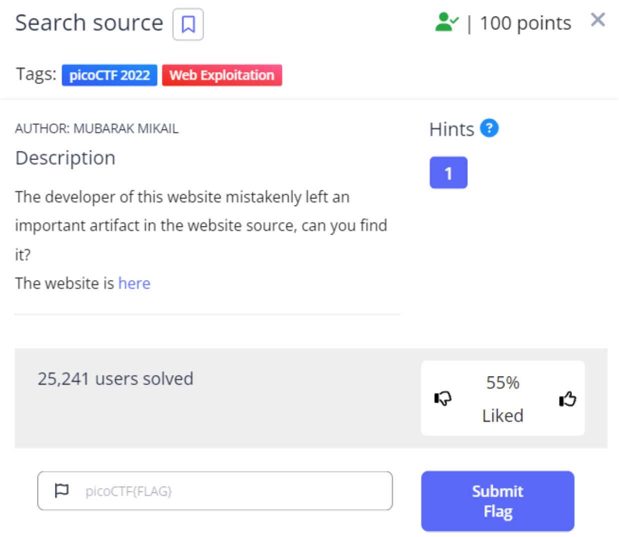
However, according to Herodotus, Histiaeus was unhappy having to stay in Susa, and made plans to return to his position as King of Miletus by instigating a revolt in Ionia. In 499 BC, he shaved the head of his most trusted slave, tattooed a message on his head, and then waited for his hair to grow back. The slave was then sent to Aristagoras, who was instructed to shave the slave's head again and read the message, which told him to revolt against the Persians.

Source: Wikipedia on Histiaeus

picoCTF{1n5p3t0r_0f_h7ml_8113f7e2}

Inspect source code of website > flag written as a comment in the webpage

Search source



Search source

| 100 points

Tags: picoCTF 2022 Web Exploitation

AUTHOR: MUBARAK MIKAIL

Description

The developer of this website mistakenly left an important artifact in the website source, can you find it?

The website is here

Hints ?

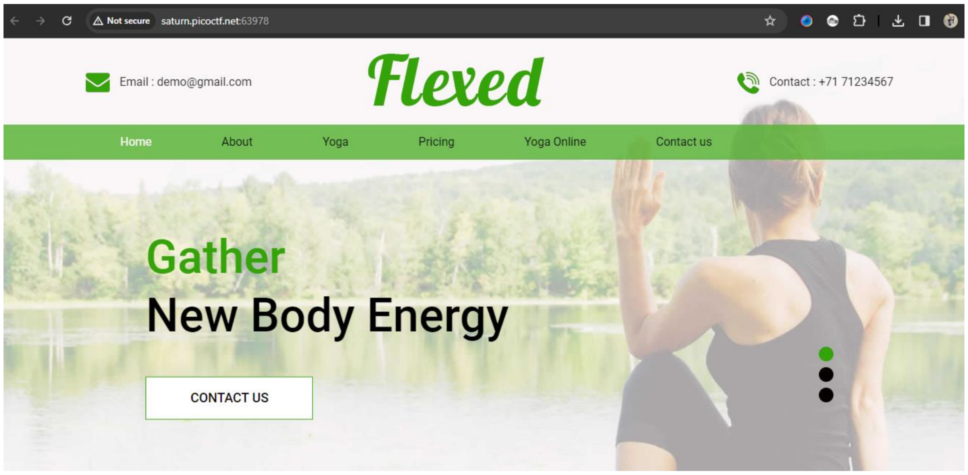
1

25,241 users solved

55% Liked

picoCTF{FLAG}

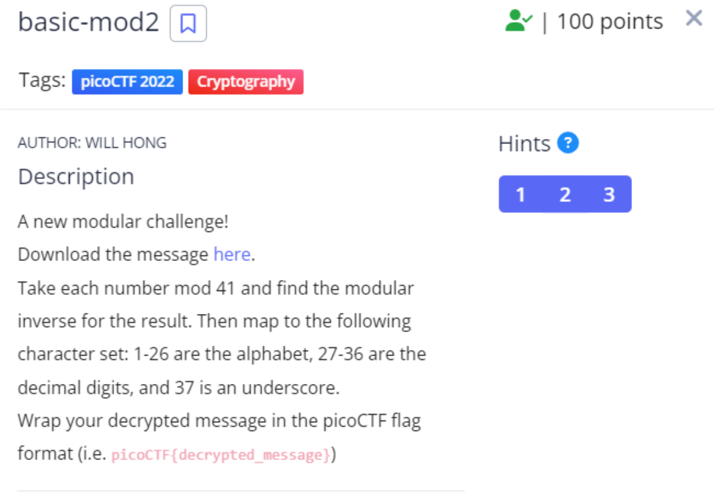
Submit Flag



picoCTF{1nsp3ti0n_0f_w3bpag3s_ec95fa49}

Inspect source code of website > ‘style.css’ document contains flag in a comment

basic-mod2



basic-mod2

| 100 points

Tags: picoCTF 2022 Cryptography

AUTHOR: WILL HONG

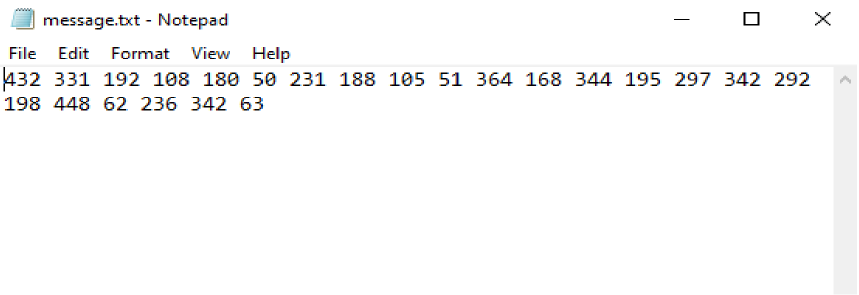
Description

A new modular challenge!

Download the message here.

Take each number mod 41 and find the modular inverse for the result. Then map to the following character set: 1-26 are the alphabet, 27-36 are the decimal digits, and 37 is an underscore.

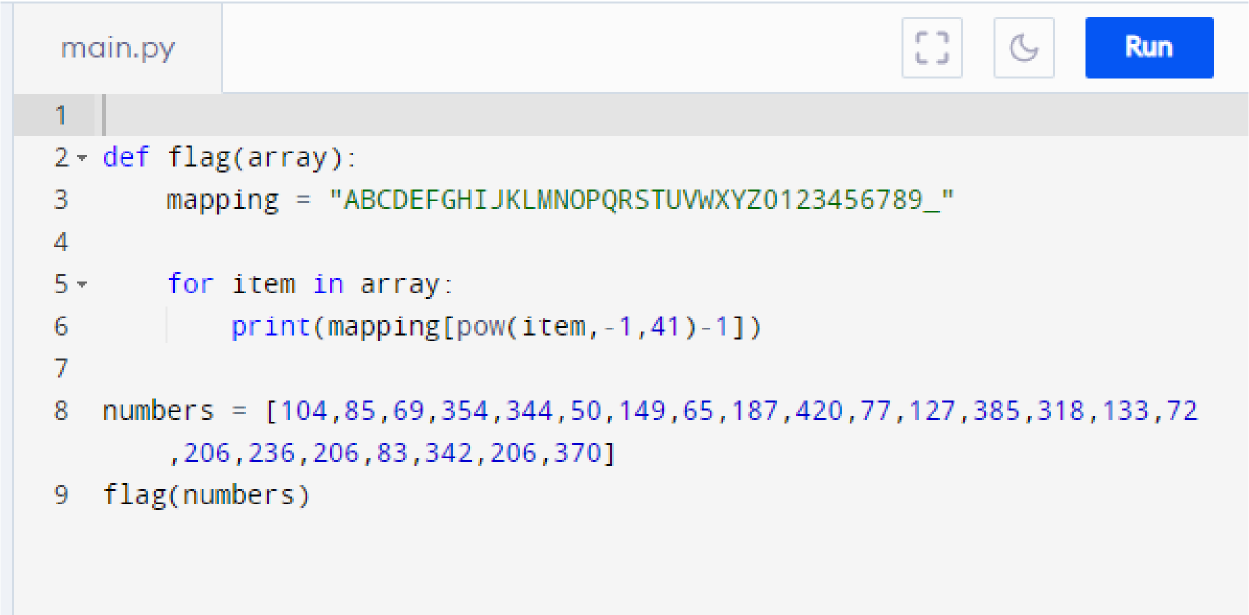
Wrap your decrypted message in the picoCTF flag format (i.e. `picoCTF{decrypted_message}`)



```
432 331 192 108 180 50 231 188 105 51 364 168 344 195 297 342 292
198 448 62 236 342 63
```

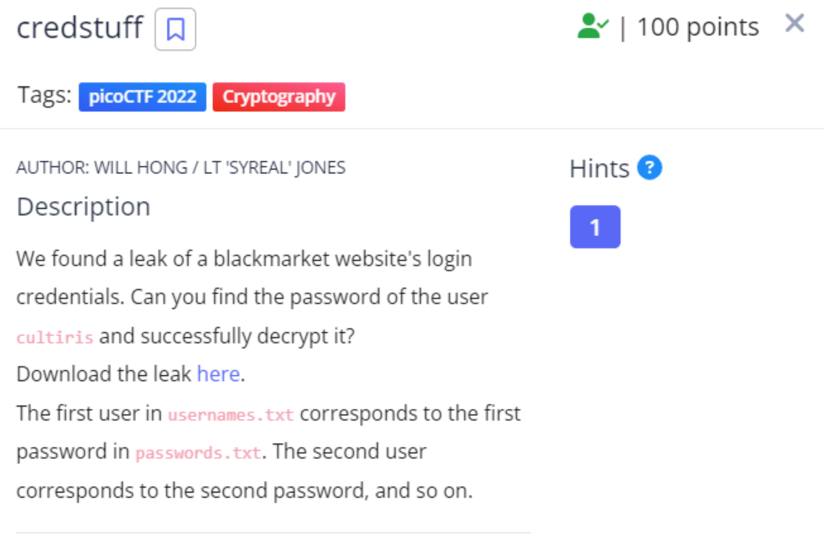
picoCTF{1NV3R53LY_H4RD_DADAACAA}

solution code



```python

def flag(array):
    mapping = "ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789_"

    for item in array:
        print(mapping[pow(item,-1,41)-1])

numbers = [104,85,69,354,344,50,149,65,187,420,77,127,385,318,133,72
    ,206,236,206,83,342,206,370]
flag(numbers)
```

cred-stuff



credstuff

| 100 points

Tags: picoCTF 2022 Cryptography

AUTHOR: WILL HONG / LT 'SYREAL' JONES

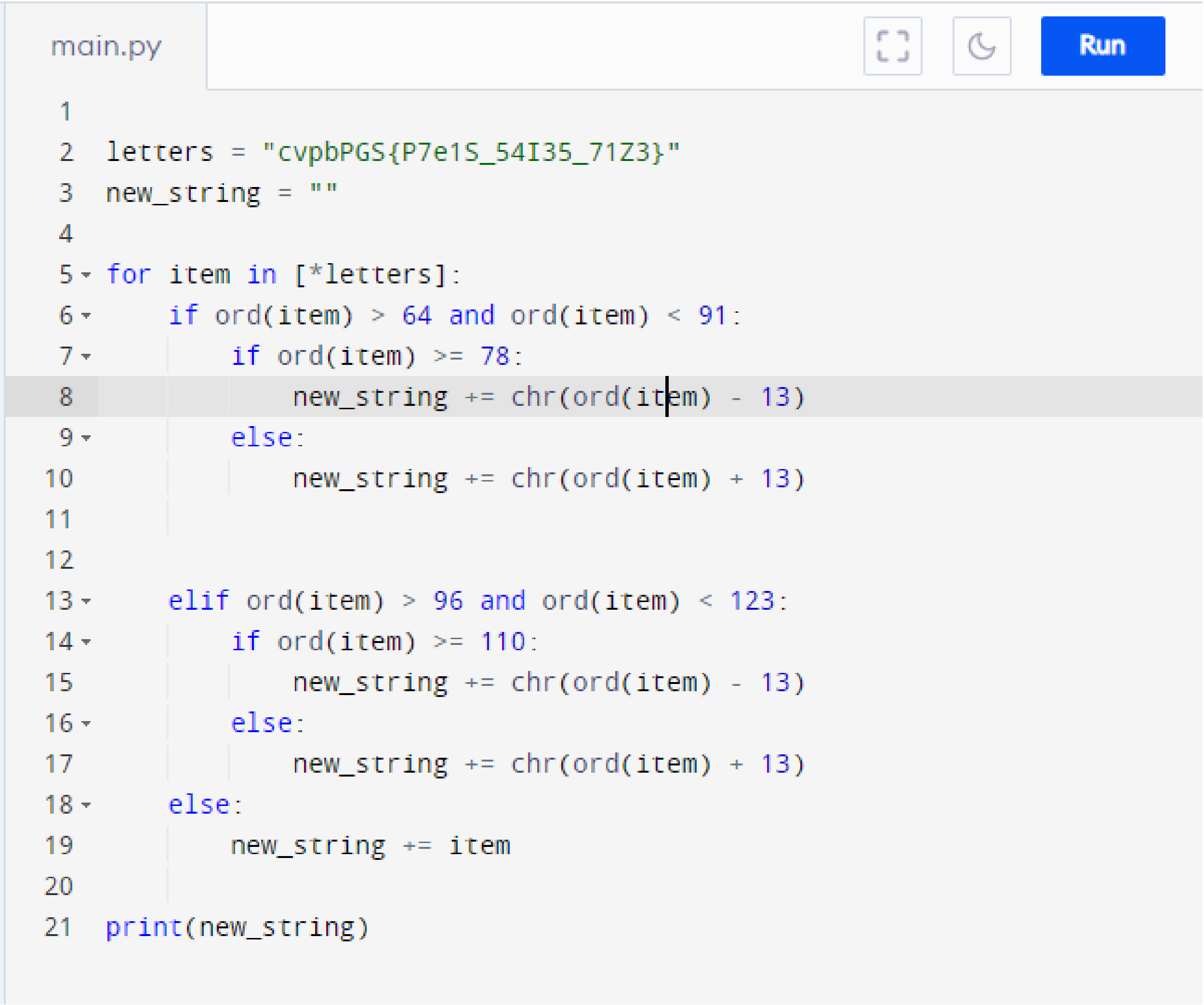
Description

We found a leak of a blackmarket website's login credentials. Can you find the password of the user `cultiris` and successfully decrypt it?

Download the leak here.

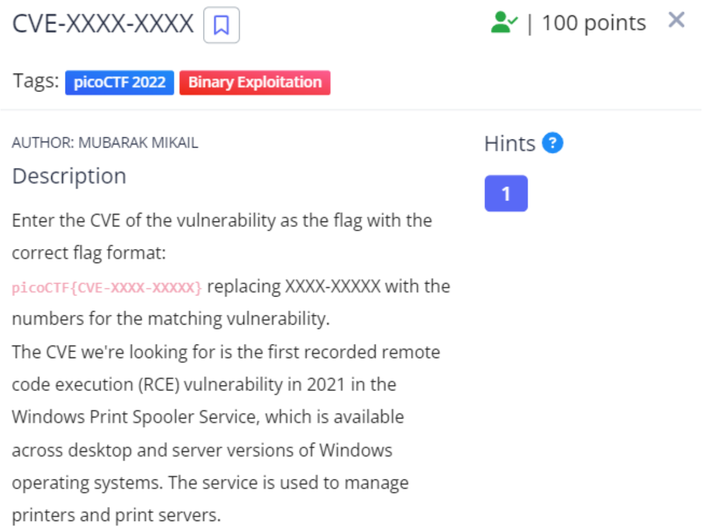
The first user in `usernames.txt` corresponds to the first password in `passwords.txt`. The second user corresponds to the second password, and so on.

picoCTF{C7r1F_54V35_71M3}



```python

letters = "cvpbPGS{P7e1S_54I35_71Z3}"
new_string = ""

for item in [*letters]:
    if ord(item) > 64 and ord(item) < 91:
        if ord(item) >= 78:
            new_string += chr(ord(item) - 13)
        else:
            new_string += chr(ord(item) + 13)


    elif ord(item) > 96 and ord(item) < 123:
        if ord(item) >= 110:
            new_string += chr(ord(item) - 13)
        else:
            new_string += chr(ord(item) + 13)
    else:
        new_string += item

print(new_string)
```

CVE-XXXX-XXXXX



CVE-XXXX-XXXX | 100 points

Tags: picoCTF 2022 Binary Exploitation

AUTHOR: MUBARAK MIKAIL

Description

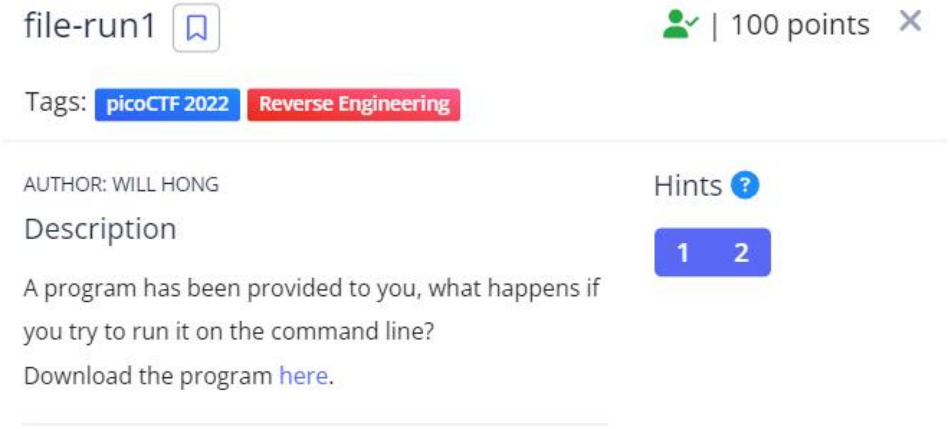
Enter the CVE of the vulnerability as the flag with the correct flag format:

`picoCTF{CVE-XXXX-XXXXX}` replacing XXXX-XXXXX with the numbers for the matching vulnerability.

The CVE we're looking for is the first recorded remote code execution (RCE) vulnerability in 2021 in the Windows Print Spooler Service, which is available across desktop and server versions of Windows operating systems. The service is used to manage printers and print servers.

picoCTF{CVE-2021-34527}

file-run1



file-run1 | 100 points

Tags: picoCTF 2022 Reverse Engineering

AUTHOR: WILL HONG

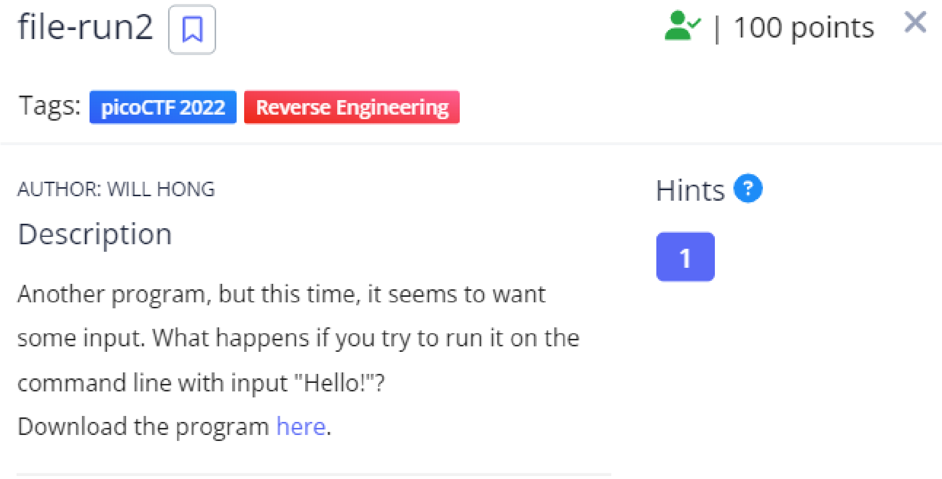
Description

A program has been provided to you, what happens if you try to run it on the command line?

Download the program here.

picoCTF{U51N6_Y0Ur_F1r57_F113_e5559d46}

file-run2



file-run2

| 100 points

Tags: picoCTF 2022 Reverse Engineering

AUTHOR: WILL HONG

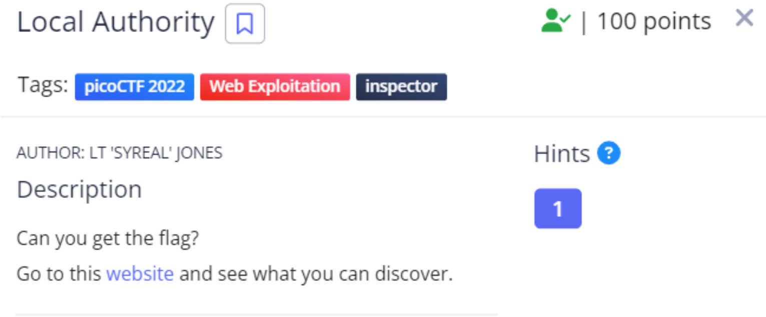
Description

Another program, but this time, it seems to want some input. What happens if you try to run it on the command line with input "Hello!"?

Download the program here.

picoCTF{F1r57_4rgum3n7_96f2195f}

localAuthority



Local Authority

| 100 points

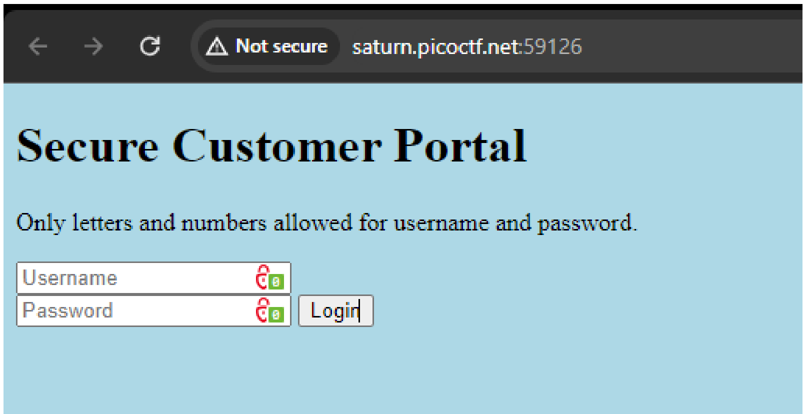
Tags: picoCTF 2022 Web Exploitation inspector

AUTHOR: LT 'SYREAL' JONES

Description

Can you get the flag?

Go to this website and see what you can discover.

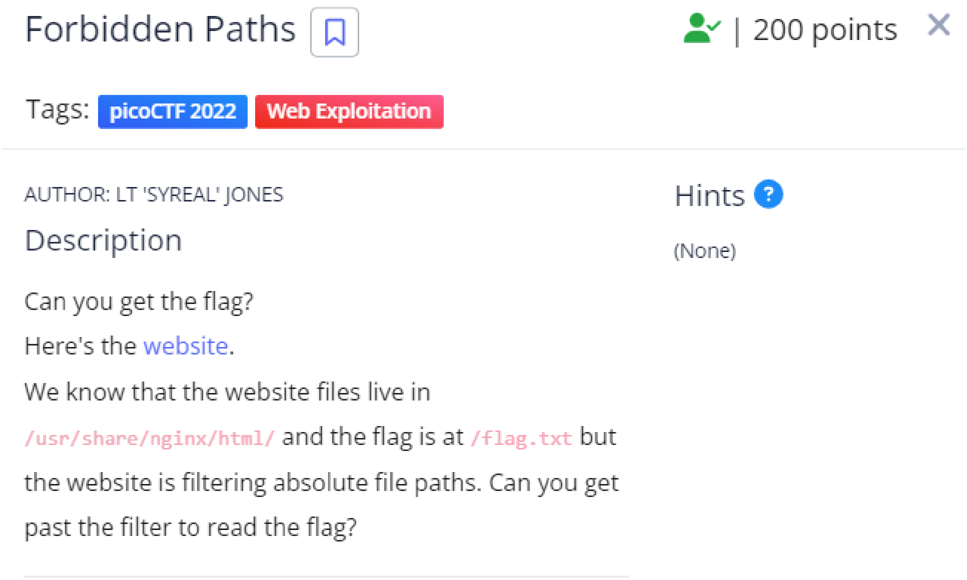


Secure Customer Portal

Only letters and numbers allowed for username and password.

picoCTF{j5_15_7r4n5p4r3n7_b0c2c9cb}

forbiddenPath



Forbidden Paths | 200 points

Tags: picoCTF 2022 Web Exploitation

AUTHOR: LT 'SYREAL' JONES

Description

Can you get the flag?
Here's the website.
We know that the website files live in `/usr/share/nginx/html/` and the flag is at `/flag.txt` but the website is filtering absolute file paths. Can you get past the filter to read the flag?

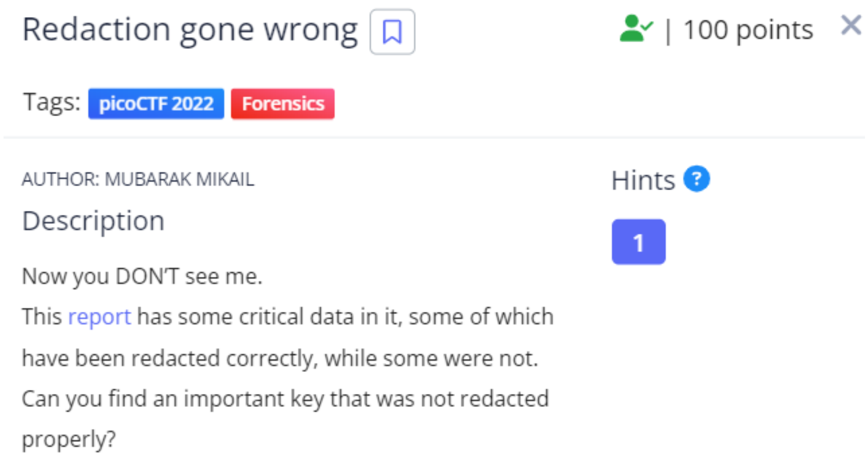
Hints

(None)

../../../../flag.txt

picoCTF{7h3_p47h_70_5ucc355_e5fe3d4d}

redaction gone wrong



Redaction gone wrong | 100 points

Tags: picoCTF 2022 Forensics

AUTHOR: MUBARAK MIKAIL

Description

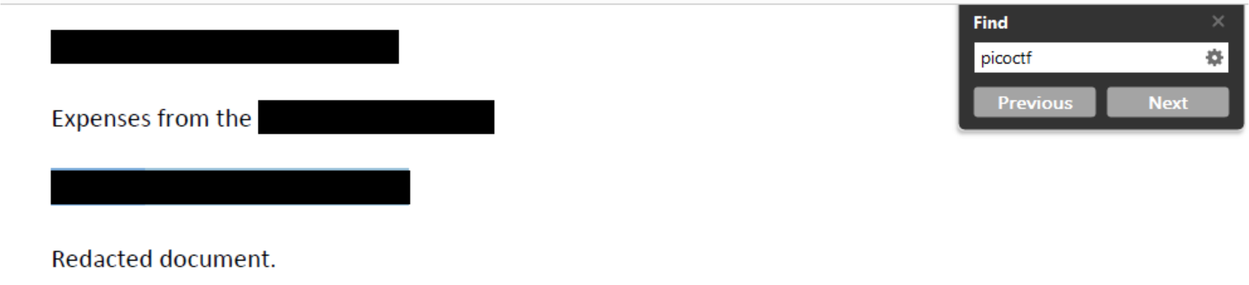
Now you DON'T see me.
This report has some critical data in it, some of which have been redacted correctly, while some were not.
Can you find an important key that was not redacted properly?

Hints

1

Searched for keyword "picoCT" in PDF viewer and copied highlighted area.

Flag is; picoCTF{C4n_Y0u_S33_m3_fully}



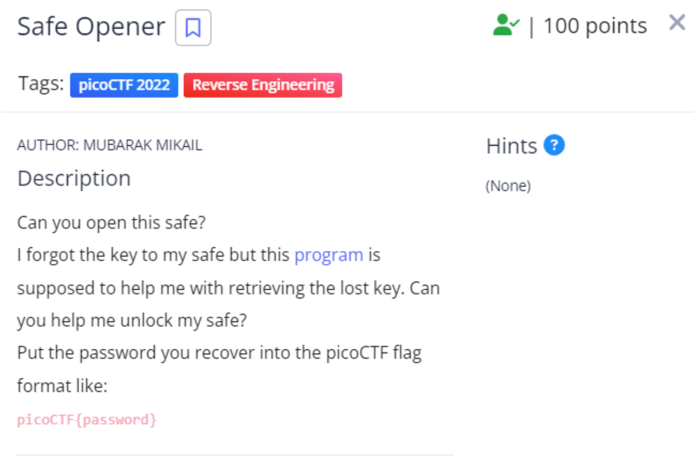
[redacted]

Expenses from the [redacted]

[redacted]

Redacted document.

safe opener



Safe Opener

| 100 points

Tags: picoCTF 2022 Reverse Engineering

AUTHOR: MUBARAK MIKAIL

Description

Can you open this safe?

I forgot the key to my safe but this program is supposed to help me with retrieving the lost key. Can you help me unlock my safe?

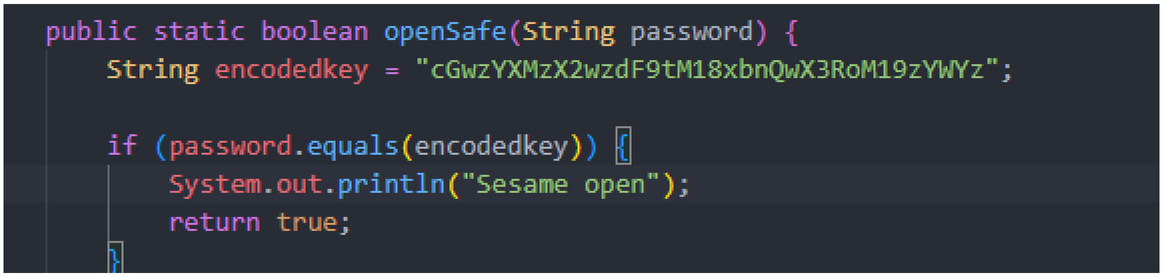
Put the password you recover into the picoCTF flag format like:

`picoCTF{password}`

Hints

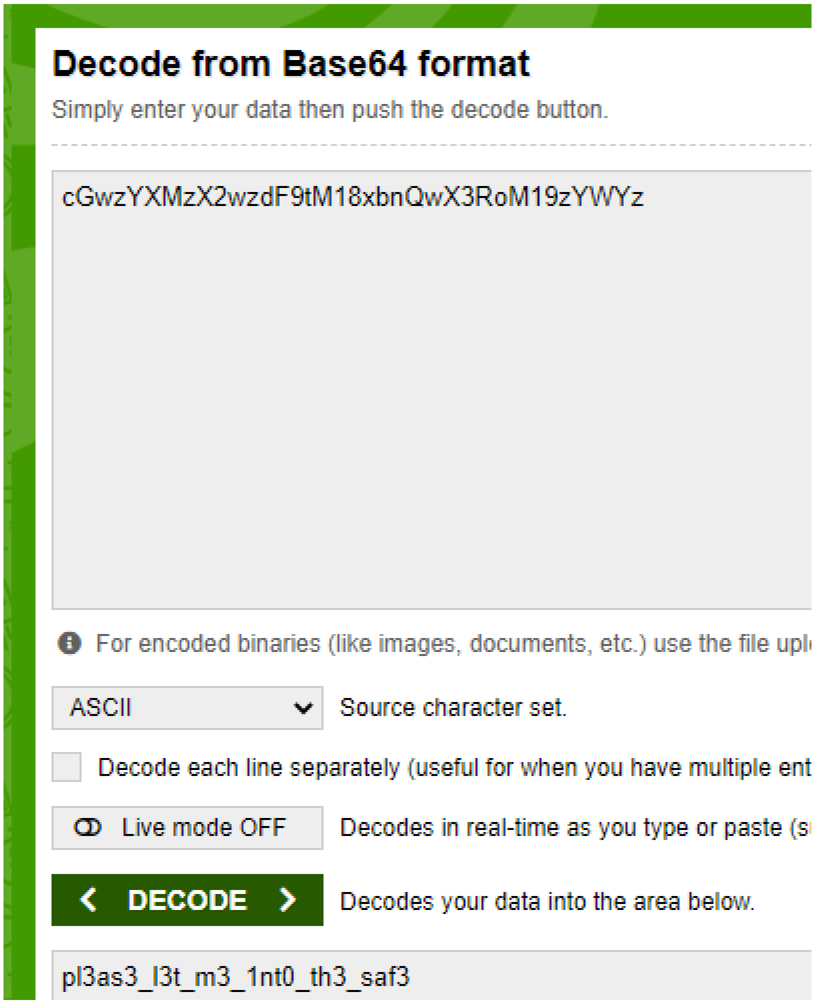
(None)

Opened source code in VSCode. “Encoded key’ string looks like a base64 because of letters and numbers.



```
public static boolean openSafe(String password) {
    String encodedkey = "cGwzYXMzX2wzdF9tM18xbnQwX3RoM19zYWYz";

    if (password.equals(encodedkey)) {
        System.out.println("Sesame open");
        return true;
    }
```

Decoding string shows result below



Decode from Base64 format

Simply enter your data then push the decode button.

cGwzYXMzX2wzdF9tM18xbnQwX3RoM19zYWYz

For encoded binaries (like images, documents, etc.) use the file upl

ASCII — Source character set.

□ Decode each line separately (useful for when you have multiple ent

Live mode OFF — Decodes in real-time as you type or paste (s

Decodes your data into the area below.

pl3as3_l3t_m3_1nt0_th3_saf3

Flag is; picoCTF{pl3as3_l3t_m3_1nt0_th3_saf3}