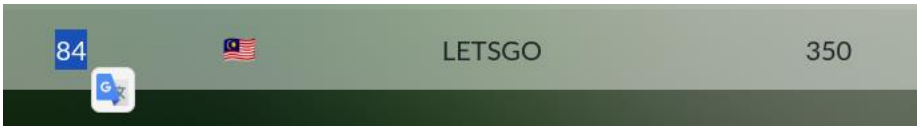


# m0leconCTF



## Table of Contents

1. Sanity Check-50 .....	2
2.Unguessable-50 .....	2
3.SecureAscess-50 .....	3
4.The wall.....	5
5.Polito Pay 2Win.....	6
6.Politoch(e)tbot.....	7
7.Strange extension-50.....	8
8. A sky full of 5t4r5.....	8

## 1. Sanity Check-50


Sanity Check

50 263

misc

Keep an eye on the announcements channel for any important communications on [Discord](#)?

Find the find in discord server

MatteB\_01 昨天21:01

Hello [@everyone](#). The third edition of the m0leCon beginner CTF starts right now. Thank you all for deciding to join, have fun solving and good luck!

ptm{w3lc0m3\_t0\_b3g1nner\_2021+2}

Flag: ptm{w3lc0m3\_t0\_b3g1nner\_2021+2}

## 2. Unguessable-50

Unguessable

50 277

web

You will never guess the number on this [website](#)!

Author: @filippo

View page source, we can get a directory

```
58 loader.style.width = "0%";
59 loader.parentElement.setAttribute("hidden", "");
70 }
71
72 function update(res) {
73   if (res === "wrong") {
74     card.style.backgroundColor = "red";
75     text.innerText = "Wrong, try again";
76   } else {
77     card.style.backgroundColor = "green";
78     fetch("/vjfYkHzyZGJ4A7cPNutFeM/flag")
79       .then((response) => response.text())
80       .then((str) => {
81         text.innerText = str
82       });
83   }
84 }
```

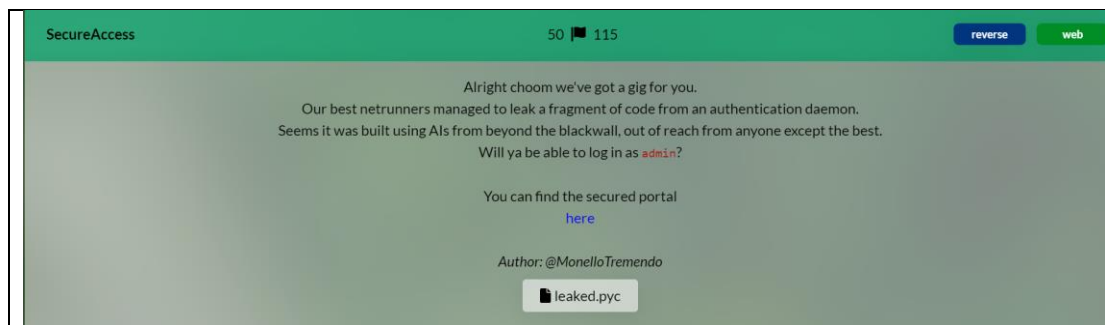
Copy the directory and paste on link

view-source:https://unguessable.challs.m0lecon.it/vjfYkHzyZGJ4A7cPNutFeM/flag

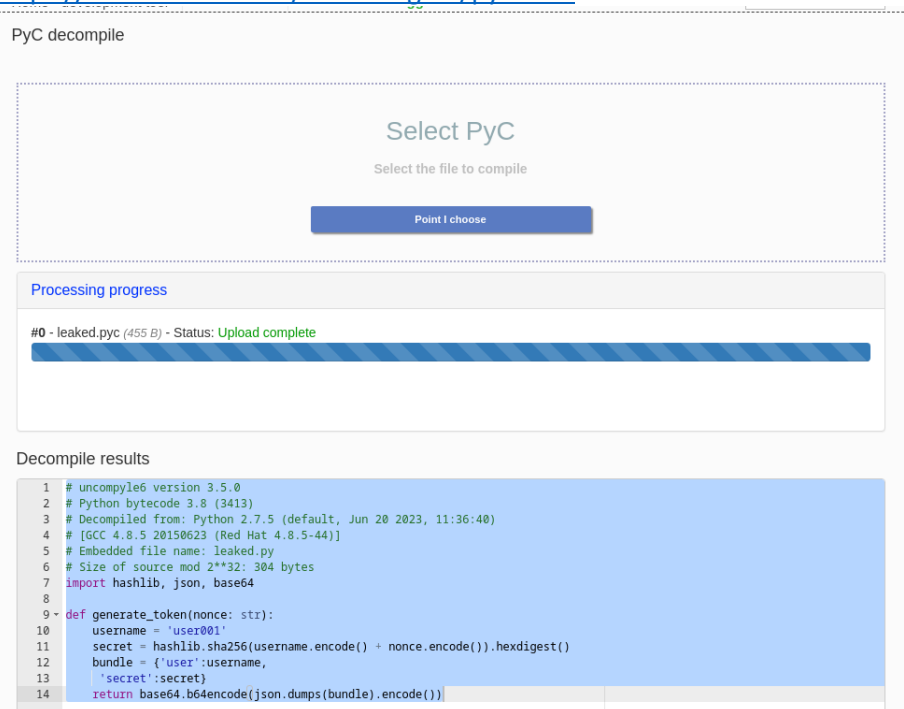
ptm{41w4y5\_ch3ck\_th3\_50urc3\_c0d3}

Flag:ptm{41w4y5\_ch3ck\_th3\_50urc3\_c0d3}

### 3. SecureAccess-50



We try to decompile the .pyc file using website  
<https://www.toolnb.com/tools-lang-en/pyc.html>




Inside the code function is no complete we try chatgpt to done the program

```
import hashlib
import json
import base64

def generate_token(nonce: str):
    username = 'admin'
    secret = hashlib.sha256((username + nonce).encode()).hexdigest()
    bundle = {'user': username, 'secret': secret}
    token = base64.b64encode(json.dumps(bundle).encode()).decode() # Added .decode() to get a string
    return token

# Example of how to use the function
nonce_example = '50A202CC-A33D-4E19-A7C5-1DF9B78D0912'
generated_token = generate_token(nonce_example)
print("Generated Token:", generated_token)
```

Based on question we know we need to login to admin and we will get a token so we change in into nonce\_example



GUEST\_01

USERNAME

ENTER

WELCOME ADMIN

PLEASE CALCULATE YOUR ACCESS TOKEN

E4B9227C-13C3-42C3-A7BD-2AF52016D666

ACCESS TOKEN

LOGIN

You after run python code you will get a access token try login

```

kali@kali:~/Downloads$ python3 test2.py
Generated Token: eyJ1c2VyIjogImFkbWlulWgInNlY3JldCI6ICJjMTQ5ZDgzODRkNWYSYWM1OTY1MzQ1N2ZlYjI4MTBhNDk5In0=

```

Here is the flag!!

```

ptm{m4yb3_7he_Als_4r3_n0t_th4t_5m4r7}

```

Flag:ptm{m4yb3\_7hr\_Als\_4r3\_n0t\_th4t\_5m4r7}

## 4.The wall

The Wall50 96pwn

A friend of mine told me about a peculiar bank. You gotta give it a try for me.  
nc nullwall.challs.m0lecon.it 1337

Author: @OrHy3

null\_wall

We can check the null\_wall file in ghidra

```
00000000 00 00 00 00  MOV     EAX,0x0
00101413 b8 00 00 00  MOV     EAX,0x0
00000000 00 00 00 00
00101418 e8 23 fd ff  CALL    <EXTERNAL>::read          ssize_t read(int __fd, void * __bu
0010141d 89 45 ec  MOV     dword ptr [RBP + local_1c],EAX
00101420 83 7d ec 14  CMP     dword ptr [RBP + local_1c],0x14
00101424 0f 85 3b    JNZ     LAB_00101365
00000000 ff ff ff ff
0010142a 0f b6 05    MOVZX   EAX,byte ptr [notaflagbuffer[19]]
00000000 22 2c 00 00
```

```
24 puts("2. Read note");
25 puts("3. Exit");
26 printf("\nChoose an option: ");
27 __isoc99_scanf(&A7_001020fa,&loca
28 if (local_20 != 1) break;
29 printf("\nShare some thoughts: ");
30 sVar1 = read(0,notaflagbuffer,0x10
31 local_1c = (int)sVar1;
32 if ((local_1c == 0x14) && (notafla
33 empty_stdin());
34 }
35 }
```

We can see that have say notafiahbuffer[19] so the mean is it save character more than 19  
it is buffer so we try enter number more than 19

Choose an option: 1

Share some thoughts: 12345678912345678999

1. Write note  
2. Read note  
3. Exit

Choose an option:

Try read note

Choose an option: 2

Here's what you've written: 12345678912345678999  
tm{ju57\_4n07h3r\_br1ck\_1n\_7h3\_w411}

1. Write note  
2. Read note  
3. Exit

Flag:ptm{ju57\_4n07h3r\_br1ck\_1n\_7h3\_w411}

5

## 5. Polito Pay 2Win

Polito Pay 2 Win5080reverse

PolITO can be quite challenging. To pass this exam session, you'll need to earn a significant number of ECTS. Do you think you can manage to do it?

Author: @syscall

game-windows.zipgame-linux.zip

Unzip game-linux.zip

```
game
game-linux.zip
```

```
(kali@kali)-[~/Downloads/game]
$ ls
assets  game.py  main.py  __pycache__  ui
Config.py  lib  market.py  requirements.txt  Wrappers.py
```

We try run main.py

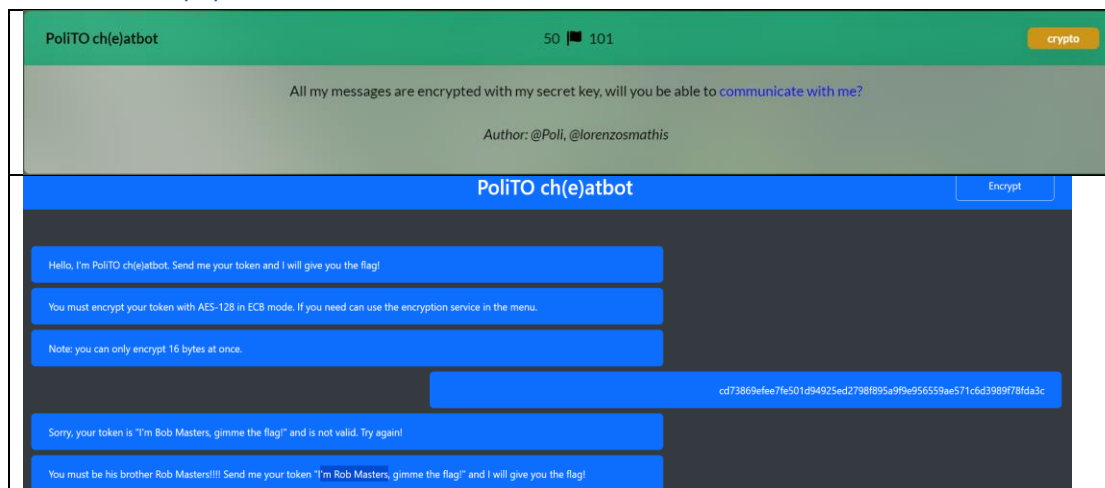
We can see in market got something hidden so we try to find the file market.py

```
et_elements[index].name.decode('utf-8')
lf.market_elements[index].desc.decode('utf-8')
flag\n: ptm{p4tch1ng_3xecut4bl3s_1s_fun}'
n)
```

Here its flag!

ptm{p4tch1ng\_3xecut4bl3s\_1s\_fun}

## 6.Politoch(e)tbot



In the chat we can know

I'm Bob Masters, gimme the flag!=

cd73869efee7fe501d94925ed2798f895a9f9e956559ae571c6d3989f78fda3c

The chat have say only encrypt 16 bytes at once so we try to encrypt "I'm Rob Masters,"

Encrypt something

Plaintext  
I'm Rob Masters,

Encrypt!!!!

1be39bf6015076ba70446ca402584e98

I'm Rob Masters, =1be39bf6015076ba70446ca402584e98

After we try encrypt "I'm Bob Masters"

Encryption

Encrypt something

Plaintext

Encrypt!!!!

cd73869efee7fe501d94925ed2798f89

cd73869efee7fe501d94925ed2798f895a9f9e956559ae571c6d3989f78fda3c

yellow is I'm Bob Masters,  
red is gimme the flag!

So based on question You must be his brother Rob Masters!!!! Send me your token "I'm Rob Masters, gimme the flag!".So the token will be blue+red

1be39bf6015076ba70446ca402584e985a9f9e956559ae571c6d3989f78fda3c

ptm{ECB\_bI0cks\_4re\_iNd3p3ndent}

Flag: ptm{ECB\_bI0cks\_4re\_iNd3p3ndent}

## 7.Strange extension-50

Strange extension

50 225

misc

I've found this strange file in our super secret project. Can you figure out where the flag is?

Author: @GabraIn24

strangefile.ptm

Try strings that file and grep "ptm"

```
(kali@kali)-[~/Downloads]
$ strings strangefile.ptm |grep "ptm"
ptm{m4k3_r3tr0_g4m1ng_gr34t_4g41n!!}
```

Flag: ptm{m4k3\_r3tr0\_g4m1ng\_gr34t\_4g41n!!}

## 8. A sky full of 5t4r5

A sky full of 5t4r5

71 53

misc


Deep space photos are amazing!

Author: @GabraIn24


a\_sky\_full\_of\_5t4r5.png

flag

Open the png and find a symbol ?



The flag on the symbol ?



Flag: ptm{0n3\_h0ur\_h3r3\_1s\_7\_d4ys\_0n\_34rth}