



Medium Reverse Engineering picoCTF 2022

AUTHOR: LT 'SYREAL' JONES

Hints ?

Description

(None)

Can you get the flag?

Run this [Python program](#) in the same directory as this [encrypted flag](#).

The screenshot shows a VS Code interface with the following details:

- EXPLORER:** Shows a folder named "PATCHME.PY" containing "flag.txt.enc" and "patchme.flag.py".
- CODE EDITOR:** Displays the content of "patchme.flag.py".

```
patchme.flag.py > level_1_pw_check
1  ### THIS FUNCTION WILL NOT HELP YOU FIND THE FLAG --LT #####
2  def str_xor(secret, key):
3      #extend key to secret length
4      new_key = key
5      i = 0
6      while len(new_key) < len(secret):
7          new_key = new_key + key[i]
8          i = (i + 1) % len(key)
9      return "".join([chr(ord(secret_c) ^ ord(new_key_c)) for (secret_c,new_key_c) in zip(secret,new_key)])
10 #####
11
12
13 flag_enc = open('flag.txt.enc', 'rb').read()
14
15
16
17 def level_1_pw_check():
18     user_pw = input("Please enter correct password for flag: ")
19     if user_pw == "ak98" + \
20         "--90" + \
21         "adfhqj321" + \
22         "sleuth9000":
23         print("Welcome back... your flag, user:")
24         decryption = str_xor(flag_enc.decode(), "utilitarian")
25         print(decryption)
26         return
27     print("That password is incorrect")
28
29
30
31 level_1_pw_check()
32
```
- TERMINAL:** Shows the command "patchme.py % python -u "Users/user/Documents/CyberSecurity/Reverse_Engineering/Latihan/PicoCTF/patchme.py/patchme.flag.py"" being run, followed by the output:

```
patchme.py % python -u "Users/user/Documents/CyberSecurity/Reverse_Engineering/Latihan/PicoCTF/patchme.py/patchme.flag.py"
Please enter correct password for flag: ak98--90adfsleuth9000
Welcome back... your flag, user:
picoCTF{p47ch1ng_l1f3_h4ck_c4a4688b}
```

Solusinya tinggal di running trus ikutin string password trus dimasukkin passwordnya.

Flag = picoCTF{p47ch1ng_l1f3_h4ck_c4a4688b}