

LinkedIn: [Kelvin Kimotho](#)

AUTHOR: LT 'SYREAL' JONES

Hints ?

Description

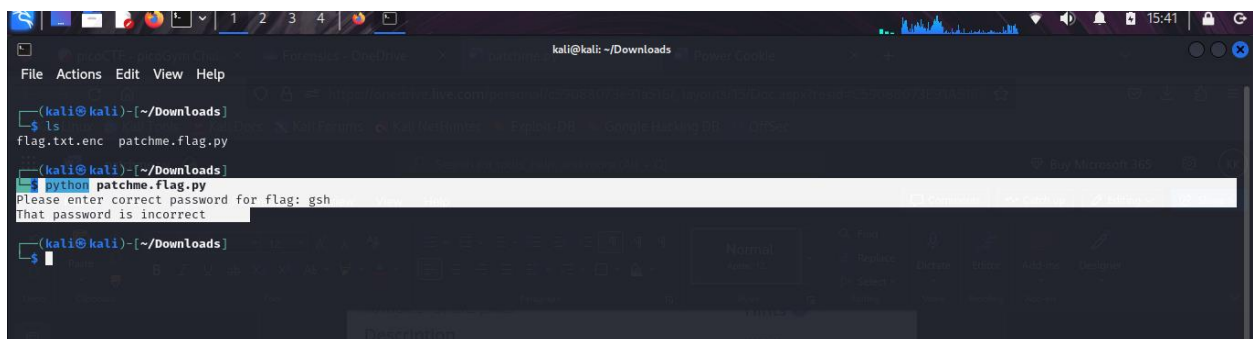
(None)

Can you get the flag?

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

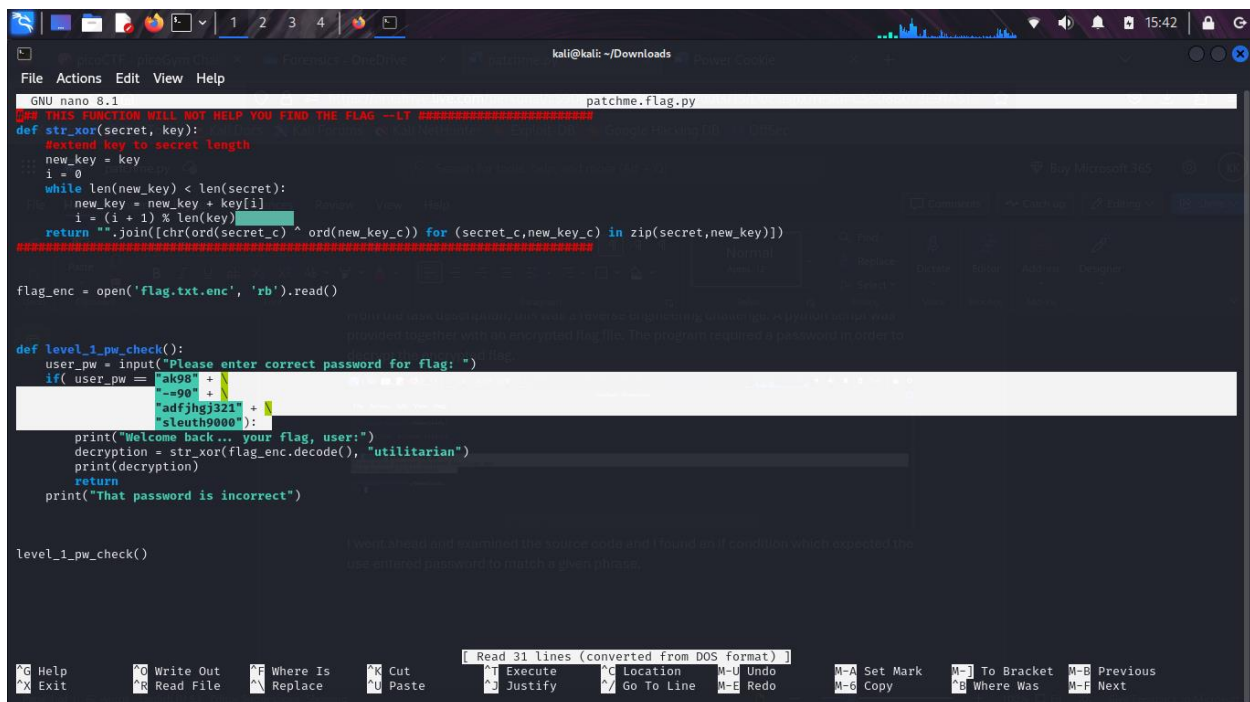
Solution

From the task description, this was a reverse engineering challenge. A python script was provided together with an encrypted flag file. The program required a password in order to decrypt the encrypted flag.



```
kali@kali: ~/Downloads
File Actions Edit View Help
(kali@kali)-[~/Downloads]
$ ls
flag.txt.enc  patchme.flag.py
(kali@kali)-[~/Downloads]
$ python patchme.flag.py
Please enter correct password for flag: gsh
That password is incorrect
(kali@kali)-[~/Downloads]
$
```

I went ahead and examined the source code and I found an if condition which expected the use entered password to match a given phrase.



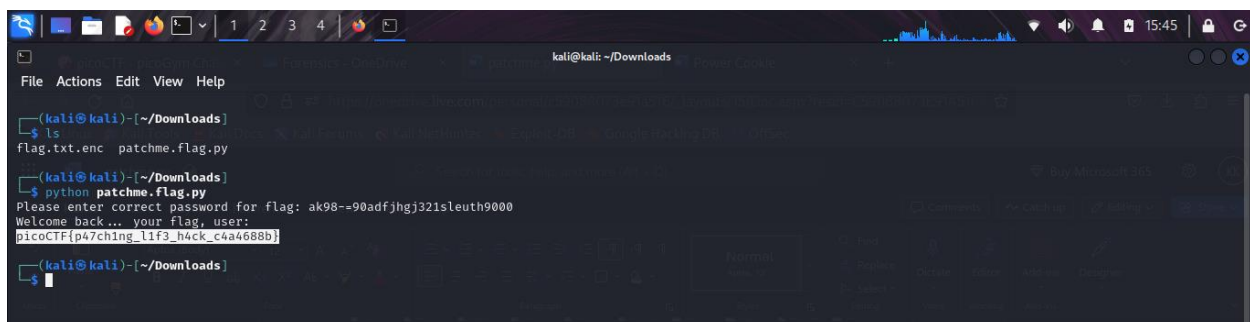
```
GNU nano 8.1 patchme.flag.py
def str_xor(secret, key):
    #extend key to secret length
    new_key = key
    i = 0
    while len(new_key) < len(secret):
        new_key = new_key + key[i]
        i = (i + 1) % len(key)
    return "".join([chr(ord(secret_c) ^ ord(new_key_c)) for (secret_c,new_key_c) in zip(secret,new_key)])

flag_enc = open('flag.txt.enc', 'rb').read()

def level_1_pw_check():
    user_pw = input("Please enter correct password for flag: ")
    if( user_pw == "ak98==90adfjhgj321sl euth9000" ):
        print("Welcome back... your flag, user:")
        decryption = str_xor(flag_enc.decode(), "utilitarian")
        print(decryption)
        return
    print("That password is incorrect")

level_1_pw_check()
```

The password required was "ak98==90adfjhgj321sl euth9000". I went ahead and used the password.



```
(kali@kali)-[~/Downloads]
$ ls
flag.txt.enc  patchme.flag.py
$ python patchme.flag.py
Please enter correct password for flag: ak98==90adfjhgj321sl euth9000
Welcome back... your flag, user:
picoCTF{p47ch1ng_l1f3_h4ck_c4a4688b}
```

And that's how I retrieved the flag.