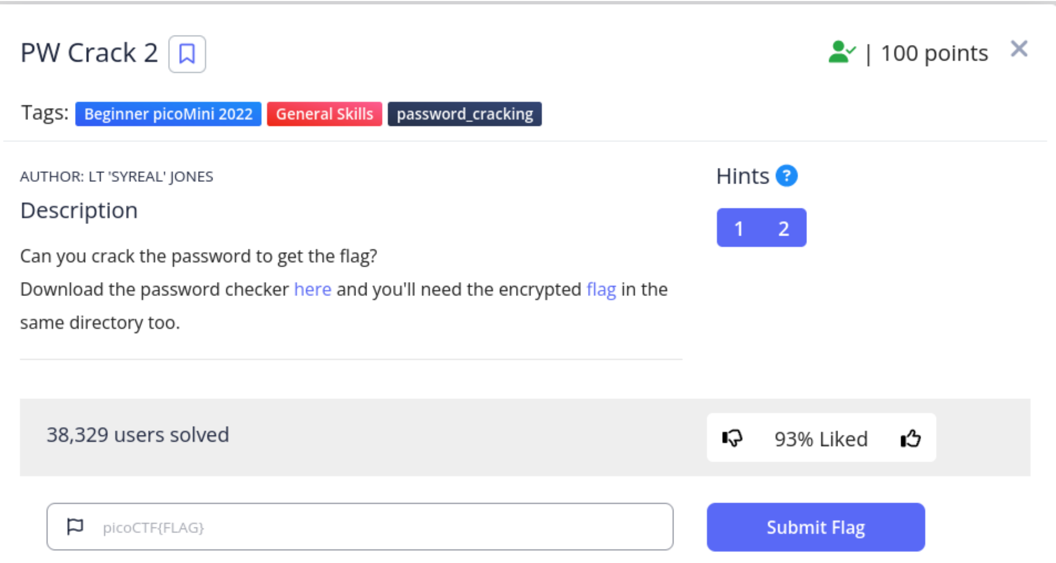
PW Crack 2



PW Crack 2

Tags: Beginner picoMini 2022 General Skills password_cracking

AUTHOR: LT 'SYREAL' JONES

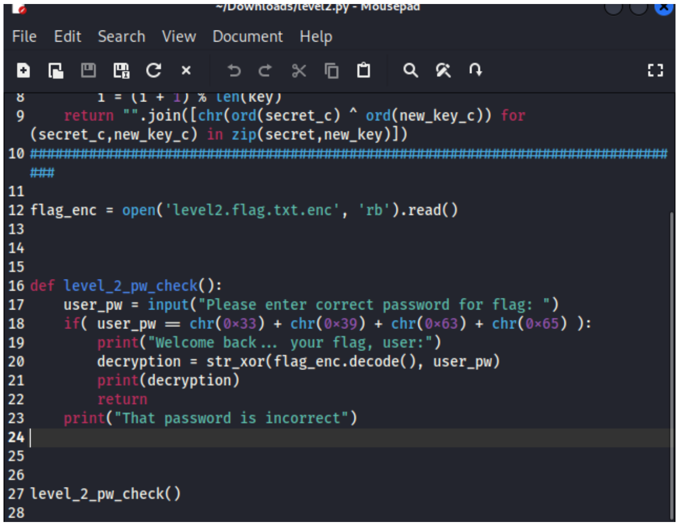
Description

Can you crack the password to get the flag?
Download the password checker here and you'll need the encrypted flag in the same directory too.

38,329 users solved

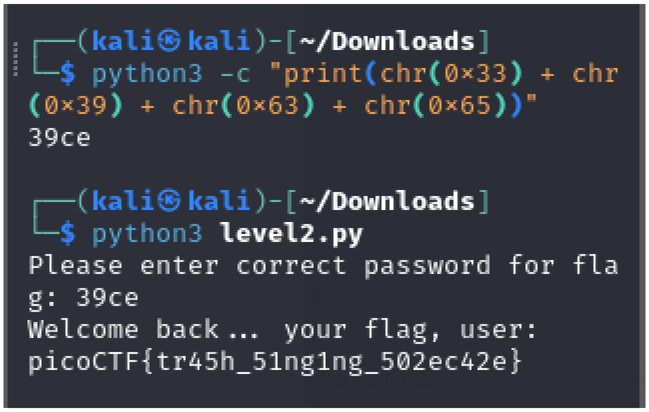
PW Crack 2 challenge

Another password cracking. Becuase we got the program that check the password, we should check it.



```
        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('level2.flag.txt.enc', 'rb').read()



def level_2_pw_check():
    user_pw = input("Please enter correct password for flag: ")
    if( user_pw == chr(0x33) + chr(0x39) + chr(0x63) + chr(0x65) ):
        print("Welcome back... your flag, user:")
        decryption = str_xor(flag_enc.decode(), user_pw)
        print(decryption)
        return
    print("That password is incorrect")



level_2_pw_check()
```

We can see that the if comparison to check the password is using the ASCII version of the hexadecimal. We can just check what is the hexadecimal in ASCII



```
┌──(kali㉿kali)-[~/Downloads]
└─$ python3 -c "print(chr(0×33) + chr
(0×39) + chr(0×63) + chr(0×65))"
39ce

┌──(kali㉿kali)-[~/Downloads]
└─$ python3 level2.py
Please enter correct password for fla
g: 39ce
Welcome back ... your flag, user:
picoCTF{tr45h_51ng1ng_502ec42e}
```