PW Crack 2

PicoCTF

Fares Zuleta

February 20, 2026

Contents

1 Description

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

2 Files

After downloading the files, we can see two files in our directory.

```
[Zer0th@Arch PWCrack2]$ ls
level2.flag.txt.enc level2.py
```

3 Python Code

```
### THIS FUNCTION WILL NOT HELP YOU FIND THE FLAG --LT
    ########################
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(’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()
```

4 Vulnerability Analysis

```
if( user_pw == chr(0x33) + chr(0x39) + chr(0x63) + chr(0x65) ):
```

After analyzing the application, we observe that the password is hardcoded using hexadecimal (Hex) values. This allows anyone with access to the source code to obtain the password.

4.1 Hex translation

Hex values

```
0x33  ’3’
0x39  ’9’
0x63  ’c’
0x65  ’e’
```

The echo command was used to pass the hexadecimal values to xxd, while xxd -r -p converts hexadecimal input into its ASCII representation.

```
[Zer0th@Arch ~]$ echo "0x33 0x39 0x63 0x65" | xxd -r -p
39ce
```

The reconstructed password is ”39ce”.

4.2 Proving our point

When executing the script, we enter the password previously discovered.

```
[Zer0th@Arch PWCrack2]$ python3 level2.py
Please enter correct password for flag: 39ce
Welcome back... your flag, user:
picoCTF{tr45h_51ng1ng_502ec42e}
```

As shown above, we successfully obtained the flag for this challenge.