PW Crack 1

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 Reading the password checker

After downloading the password checker and the encrypted flag in the same directory, the source code was analyzed.

```
nano level1.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('level1.flag.txt.enc', 'rb').read()



def level_1_pw_check():
    user_pw = input("Please enter correct password for flag: ")
    if( user_pw == "691d"):
        print("Welcome back... your flag, user:")
        decryption = str_xor(flag_enc.decode(), user_pw)
        print(decryption)
        return
    print("That password is incorrect")



level_1_pw_check()
```

4 Vulnerability Analysis

```
if( user_pw == "691d"):
```

By reading the source code, it is evident that ”691d” is the password that the user must enter.

5 Running the Code

After understanding the source code, we ran the Python file and entered the password when prompted.

```
[Zer0th@Arch PWCrack1]$ python3 level1.py
Please enter correct password for flag: 691d
```

After entering the password, the flag was obtained.

```
Welcome back... your flag, user:
picoCTF{545h_r1ng1ng_56891419}
```