

LinkedIn: [Kelvin Kimotho](#)

PW Crack 2

Easy

General Skills

Beginner picoMini 2022

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.

Hints ?

1

2

Does that encoding look familiar?

Solution

I downloaded the password checker and the encrypted flag using **wget** tool.

```
(kali@kali)-[~/Desktop]
└─$ wget https://artifacts.picoctf.net/c/13/level2.py
--2025-02-04 21:58:32-- https://artifacts.picoctf.net/c/13/level2.py
Resolving artifacts.picoctf.net (artifacts.picoctf.net)... 52.84.102.85, 2600:9000:2054:4e00:16:5ec5:2840:93a1
Connecting to artifacts.picoctf.net (artifacts.picoctf.net)|52.84.102.85|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 914 [application/octet-stream]
Saving to: 'level2.py'

level2.py 100%[=====] 914 --.-KB/s in 0s
2025-02-04 21:58:33 (11.5 MB/s) - 'level2.py' saved [914/914]

(kali@kali)-[~/Desktop]
└─$ wget https://artifacts.picoctf.net/c/13/level2.flag.txt.enc
--2025-02-04 21:58:45-- https://artifacts.picoctf.net/c/13/level2.flag.txt.enc
Resolving artifacts.picoctf.net (artifacts.picoctf.net)... 52.84.102.85, 2600:9000:2054:4e00:16:5ec5:2840:93a1
Connecting to artifacts.picoctf.net (artifacts.picoctf.net)|52.84.102.85|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 31 [application/octet-stream]
Saving to: 'level2.flag.txt.enc'

level2.flag.txt.enc 100%[=====] 31 --.-KB/s in 0s
2025-02-04 21:58:46 (21.1 MB/s) - 'level2.flag.txt.enc' saved [31/31]

(kali@kali)-[~/Desktop]
└─$ ls
level2.flag.txt.enc level2.py

(kali@kali)-[~/Desktop]
└─$
```

I opened the password checker via nano editor via terminal.

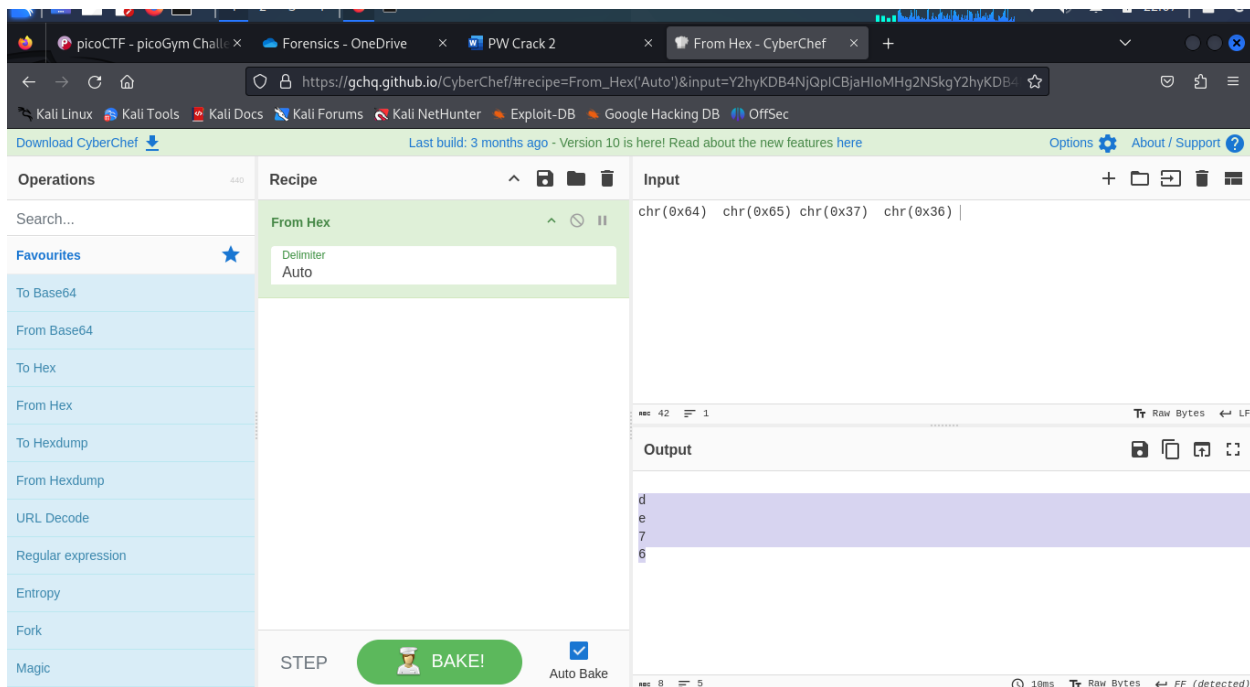
```
File Actions Edit View Help
GNU nano 8.1 level2.py
# THIS FUNCTION WILL NOT HELP YOU FIND THE FLAG --LT #####
def str_xor(secret, key):
    #extend key to secret length
    new_key = key
    i = 0
    while len(new_key) < len(secret):
        new_key = new_key + key[i]
        i = (i + 1) % len(key)
    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(0x64) + chr(0x65) + chr(0x37) + chr(0x36) ):
        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()
```

From this line `if(user_pw == chr(0x64) + chr(0x65) + chr(0x37) + chr(0x36)):`, the user was expected to enter a **four** characters password that was to be converted to hexadecimal to match the given . I used **cyberchef** an online service to decode hexadecimal back to plain text. The four characters password was **de76**.



Now that I had the password to decrypt the encrypted file, I ran the password checker program which prompted me to enter a password. I entered the password and that's how I decrypted the encrypted flag file and the flag was printed out as **picoCTF{tr45h_51ng1ng_489dea9a}**.

```
kali@kali: ~/Desktop
File Actions Edit View Help
ls
level2.flag.txt.enc level2.py
python level2.py
Please enter correct password for flag: de76
Welcome back... your flag, user:
picoCTF{tr45h_Singing_489dea9a}
```