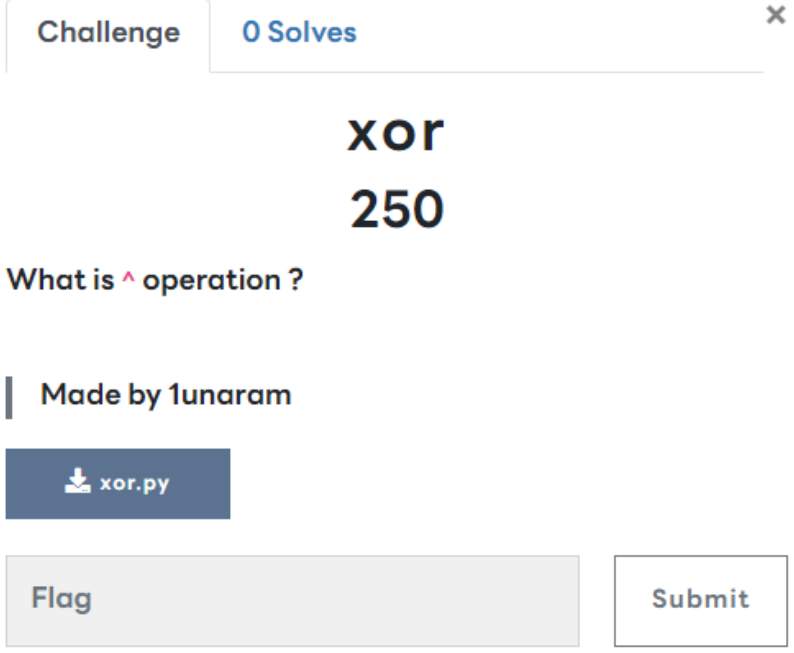
xor

> *Made by 1unaram*



문제 파악

```
# xor.py
enc_str = [0x49, 0x7c, 0x47, 0x81, 0x88, 0x79, 0x86, 0x6d, 0x79, 0x95, 0x73, 0x9e, 0x8d, 0xa6, 0xa1, 0x7d, 0x95, 0x95,
           0xad, 0xae, 0x9d, 0xb8, 0x8b, 0xb6, 0xbf, 0xb6, 0x93, 0xcf, 0xc6, 0xd5, 0xc6, 0xc3, 0xb0, 0xb8, 0xb1, 0xb5, 0xb6, 0xc7]

user_input = input("Enter the flag: ")

for i in range(len(enc_str)):

    if enc_str[i] != chr(((user_input[i] ^ i) + 3 * i)):
        print("Wrong flag")
        exit()

print("Correct flag")
```

문제 파일을 보면 16진수로 이루어진 enc_str 배열와 사용자의 입력 값을 어떠한 연산식을 거친 후에 비교를 한다.

if문의 비교식은 enc_str 배열에서 해당 index를 사용자의 입력 문자열의 해당 index와 xor 및 덧셈 곱셈 연산한 값과 비교한다. 따라서 역으로 연산하여 user_input 값으로 들어가야 할 올바른 문자열을 알아낼 수 있다.

Exploit

xor의 역연산을 이용하여 올바른 user_input 값을 구해보자

1. `enc_str[i] == (user_input[i] ^ i) + 3 * i`
2. `enc_str[i] - 3 * i == user_input[i] ^ i`
3. `(enc_str[i] - 3 * i) ^ i == user_input[i]`

이렇게 구해낼 수 있다. 이를 구하기 위한 python 코드를 구성하면 다음과 같다.

```
enc_str = [0x49, 0x7c, 0x47, 0x81, 0x88, 0x79, 0x86, 0x6d, 0x79, 0x95, 0x73, 0x9e, 0x8d, 0xa6, 0xa1, 0x7d, 0x95, 0x95,
           0xad, 0xae, 0x9d, 0xb8, 0x8b, 0xb6, 0xbf, 0xb6, 0x93, 0xcf, 0xc6, 0xd5, 0xc6, 0xc3, 0xb0, 0xb8, 0xb1, 0xb5, 0xb6, 0xc7]

flag = ""

for i in range(len(enc_str)):

    flag += chr((enc_str[i] - 3 * i) ^ i)
    print(flag)
```

```
I
Ix
IxC
IxC{
IxC{x
IxC{xo
IxC{xor
IxC{xor_
IxC{xor_i
IxC{xor_is
IxC{xor_is_
IxC{xor_is_v
IxC{xor_is_ve
IxC{xor_is_ver
IxC{xor_is_very
IxC{xor_is_very_
IxC{xor_is_very_u
IxC{xor_is_very_us
IxC{xor_is_very_use
IxC{xor_is_very_usef
IxC{xor_is_very_usefu
IxC{xor_is_very_useful
IxC{xor_is_very_useful_
IxC{xor_is_very_useful_f
IxC{xor_is_very_useful_fo
IxC{xor_is_very_useful_for
IxC{xor_is_very_useful_for_
IxC{xor_is_very_useful_for_e
IxC{xor_is_very_useful_for_en
IxC{xor_is_very_useful_for_enc
IxC{xor_is_very_useful_for_encr
IxC{xor_is_very_useful_for_encry
IxC{xor_is_very_useful_for_encryp
IxC{xor_is_very_useful_for_encrypt
IxC{xor_is_very_useful_for_encrypti
IxC{xor_is_very_useful_for_encryptio
IxC{xor_is_very_useful_for_encryption
IxC{xor_is_very_useful_for_encryption}
```

Flag 획득!