Unimod

NahamCon CTF 2022

The Problem:

I was trying to implement ROT-13, but got carried away.

The task has 2 files:

unimod.py

```
import random

flag = open('flag.txt', 'r').read()
ct = ''
k = random.randrange(0,0xFFFD)
for c in flag:
    ct += chr((ord(c) + k) % 0xFFFD)

open('out', 'w').write(ct)
```

out (I renamed out.txt)

饇饍饂饈饜餕饆餗餙饅餒餗饂餗餒饃饄餓饆饂餘餓饅餖饇餚餘餒餔餕餕饆餙餕饇餒餒饞飫

The Solve:

I examinated the coding procedure and the out(put).txt result file. The task name gave a hint too. Finally the range value 0xFFFD said we are working with unicode characters.
The coding procedure is weak. It generate only one shift value.
The “*k = random.randrange(0,0xFFFD)*” value adding is outside from the for loop.
So we need to know what is that exactly. We know the flag format, the first letter is ‘f’. Then read an ‘out.txt’ name file and calculate the shift in a string the first index is 0 “*cch = flag[0]*”. With this simple value increment method, we have got the value of k shift with condition: “*if cch == chr((ord('f') + i) % 0xFFFD):*”.
Finally we use value k for whole ‘flag’ string.

unirev.py

```
import string

flag = open('out.txt', 'r').read()
pt = ''
cch = flag[0]
```

```
print(str(ord(cch)))
for i in range(0,0xFFFD):
    if cch == chr((ord('f') + i) % 0xFFFD):
        k = i

print(str(k),"\n")
for cch in flag:
    print(str(ord(cch)))
    for ch in string.printable:
        if cch == chr((ord(ch) + k) % 0xFFFD):
            pt += ch
print(pt)
open('rev', 'w').write(pt)
```

Run:

python3 unirev.py

```
39239
39137 → (shift) value k

39239
39245
39234
39240
39260
39189
39238
39191
39193
39237
39186
39191
39234
39191
39186
39235
39236
39187
39238
39234
39192
39187
39237
39190
39239
39194
39192
39186
39188
```

39189
39189
39238
39193
39189
39239
39186
39186
39262
39147

After reverse we have the flag:
flag{4e68d16a61bc2ea72d5f971344e84f11}