buuctf_pyre

原创

下水道选手 于 2021-09-25 23:30:20 发布 104 收藏
文章标签： python

下载附件得到一个.pyc文件，这是.py文件经过编译生成的文件，所以解题第一步是将其反编译为.py文件，我用的uncompyle6反编译

uncompyle6反编译方法：

```
uncompyle6 xxx.pyc > xxx.py
```

uncompyle6安装方法：

```
pip install uncompyle6
```

也可以使用在线工具反编译：python反编译 - 在线工具

反编译后得到

```
# uncompyle6 version 3.7.4
# Python bytecode 2.7 (62211)
# Decompiled from: Python 3.8.5 (default, Sep  3 2020, 21:29:08) [MSC v.1916 64 bit (AMD64)]
# Embedded file name: encode.py
# Compiled at: 2019-08-19 21:01:57
print('Welcome to Re World!')
print('Your input1 is your flag~')
l = len(input1)
for i in range(l):
    num = ((input1[i] + i) % 128 + 128) % 128
    code += num

for i in range(l - 1):
    code[i] = code[i] ^ code[(i + 1)]

print(code)
code = ['\x1f', '\x12', '\x1d', '(', '0', '4', '\x01', '\x06', '\x14', '4', ',', '\x1b', 'U', '?', 'o', '6'
        '\x01', 'D', ';', '%', '\x13']
```

关于%需要注意的是，（a+b）%c=（a%c+b%c）%c

所以第10行((input1[i] + i) % 128 + 128) % 128

=((input1[i] + i) % 128%128 + 128%128) % 128

=（input1）[i]+i)%128

对于异或，l=len(code),异或的范围应该是range(l-1)，i的取值范围是l-1-1=l-2；因为code[0]到code[21]已经变化了，code[22]没有变，所以写脚本要从code[21]开始递减到code[0]，上脚本

```
code = ['\x1f', '\x12', '\x1d', '(', '0', '4', '\x01', '\x06', '\x14', '4', ',', '\x1b', 'U', '?', 'o', '6'
        '\x01', 'D', ';', '%', '\x13']
l = len(code)
# print(l)
flag = ''
for i in range(l - 2,-1,-1):
        code[i] = chr(ord(code[i]) ^ ord(code[i + 1]))
# print(code)
for i in range(l):
        code[i] = chr((ord(code[i]) - i) % 128)
        flag += code[i]
print(flag)
```

运行得出flag

```
GWHT{Just_Re_1s_Ha66y!}
```


将GWHT换成flag提交

```
flag{Just_Re_1s_Ha66y!}
```