BUUCTF Reverse [GWCTF 2019]pyre WriteUp

原创

PlumpBoy 于 2021-09-11 16:14:47 发布 39 收藏

分类专栏： BUUCTF 逆向题解 文章标签： 系统安全 安全

本文链接：https://blog.csdn.net/weixin_45723661/article/details/120228030

pyre-WP

首先发现是pyc文件，使用在线工具进行反编译，得到源码

```
#!/usr/bin/env python
# visit http://tool.lu/pyc/ for more information
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 #字符串拼接
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",
]
```

对此源码进行分析发现，其中要求输入的应该是flag，输入后将其与自己的位数相加，对128求余的目的是确保其在ASCII中，然后在将每一位与下一位进行异或，注意，最后一位未进行运算。

逆向分析，异或之后，我们有运算完的值，要求之前的值就将其与那个数字再进行一次异或（$a^{0=a}$,$a^a=0$,$a^b=a$）但是特别注意，要是逆序的才行，同时注意，a=(b-c)%d的逆运算为b=（a+c）%d，最终写出解密脚本。

```
code = [0x1f,0x12,0x1d,0x28,0x30,0x34,0x01,0x06,0x14,0x34,0x2C,0x1b,0x55,0x3F,0x6f,0x36,0x2a,0x3a,0x01,0x44,0x3b
,0x25,0x13]

a = len(code)
for i in range(a-2,-1,-1): #此处注意一点，range是包前不包后
    code[i] = code[i] ^ code[i + 1]

for i in range(a):
    print(chr((code[i] - i) % 128),end='')
```

最终结果`GWHT{Just_Re_1s_Ha66y!}`，但是要提交`flag{Just_Re_1s_Ha66y!}`