

buuctf逆向pyre

原创

g子荣 于 2021-10-13 13:12:25 发布 8 收藏

分类专栏: [笔记](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/weixin_50847719/article/details/120741801

版权



[笔记 专栏收录该内容](#)

9 篇文章 0 订阅

订阅专栏

2021.9.16 pm 2:07

```
0 l = len(input1)
7 for i in range(l):
8     num = ((input1[i] + i) % 128 + 128) % 128 ①
9     code += num
0 for i in range(l - 1):
1     code[i] = code[i] ^ code[i + 1] ②
```

$code[i] = code[i] \wedge code[i + 1]$
两次异或 ' \wedge ' 得到原结果 \swarrow 左右相换
 $code[i] \wedge code[i + 1] = code[i]$
 $len(code) = 23$
从最后一次运算开始逆推
 $code[21] = code[21] \wedge code[22]$
因为 $code[22]$ 不变

因为 $\text{code}[22]$ 不变

$$\text{code}[21] \wedge \text{code}[22] \wedge \text{code}[22] = \text{code}[21]$$

所以 从 $\text{code}[21]$ 到 $\text{code}[0]$

$$\text{code}[21] = \text{code}[22] \wedge \text{code}[21]$$

$$\text{code}[21] = \text{code}[21] \wedge \text{code}[22]$$

$$\text{code}[20] = \text{code}[20] \wedge \text{code}[21]$$

$$\text{code}[1] = \text{code}[1] \wedge \text{code}[2]$$

$$\text{code}[0] = \text{code}[0] \wedge \text{code}[1] \Rightarrow \text{此步 } i=0, \text{ 但} \leftarrow$$

for i in range(21, -1, -1)

-1 不执行

$$\text{code}[i] = \text{code}[i] \wedge \text{code}[i+1]$$

1/3

```
for i in range(1):
```

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

```
code += num
```

$$\text{num} = [(flag[i] + i) \% 128 + 128] \% 128 = \text{code}[i]$$

$$(a \% c + b \% c) \% c = (a + b) \% c =$$

$$[flag[i] + i] \% 128$$

```
flag = ''
for i in range(21, -1, -1):
    code[i] = chr(ord(code[i]) ^ ord(code[i + 1]))
for a in range(22):
    flag += chr((ord(code[a]) - a) % 128)
print(flag)
```

GWHT{Just_Re_1s_Ha66y!}

