# IDF实验室-python ByteCode writeup

转载

weixin_30652879 于 2016-11-26 19:58:00 发布 45 收藏
文章标签： python php
原文链接：http://www.cnblogs.com/zhengjim/p/6105071.html

题目地址：http://ctf.idf.cn/index.php?g=game&m=article&a=index&id=45

下载来发现是crackme.pyc

可以用uncompyle2反编译。也可以直接http://tool.lu/pyc/在这个网站反编译。

得到源代码：

```python
#!/usr/bin/env python
# encoding: utf-8
# 如果觉得不错，可以推荐给你的朋友! http://tool.lu/pyc

def encrypt(key, seed, string):
    rst = []
    for v in string:
        rst.append((ord(v) + seed ^ ord(key[seed])) % 255)
        seed = (seed + 1) % len(key)

    return rst

if __name__ == '__main__':
    print "Welcome to idf's python crackme"
    flag = input('Enter the Flag: ')
    KEY1 = 'Maybe you are good at decryptint Byte Code, have a try!'
    KEY2 = [
        124,
        48,
        52,
        59,
        164,
        50,
        37,
        62,
        67,
        52,
        48,
        6,
        1,
        122,
        3,
        22,
        72,
        1,
        1,
        14,
        46,
        27,
        232]
    en_out = encrypt(KEY1, 5, flag)
    if KEY2 == en_out:
        print 'You Win'
    else:
        print 'Try Again !'
```

程序加密函数：

```python
def encrypt(key, seed, string):
    rst = []
    for v in string:
        rst.append((ord(v) + seed ^ ord(key[seed])) % 255)
        seed = (seed + 1) % len(key)
```

flag加密后与KEY2比较 一样的话输出You Win

本来想逆向，但弄不来，就直接爆破了。

a-z A-Z 0-9 加上符号 可以有Ascll码遍历，然后编码转换回来，加入数组。

然后加密，与KEY数组的值比较。

代码如下：

```
#!/usr/bin/env python
# encoding: utf-8

def encrypt(key, seed, string):
    for v in string:
        a = (ord(v) + seed ^ ord(key[seed]) % 255)
        return a

KEY1 = 'Maybe you are good at decryptint Byte Code, have a try!'
KEY2 = [
    124,
    48,
    52,
    59,
    164,
    50,
    37,
    62,
    67,
    52,
    48,
    6,
    1,
    122,
    3,
    22,
    72,
    1,
    1,
    14,
    46,
    27,
    232]
s=[]
seed=5;
key= 'Maybe you are good at decryptint Byte Code, have a try!'
for i in range(33,127):
    j = chr(i)
    s.append(j)
for i in range(23):
    for j in s:
        aa = encrypt(key,seed,j)
        if aa == KEY2[i]:
            print j
    seed = (seed + 1) % len(key)
```

要注意的是seed 的改变要在flag与KEY2比较后。

转载于:https://www.cnblogs.com/zhengjim/p/6105071.html