

南邮CTF逆向题第三道Py交易解题思路

原创

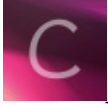
iqiqiya 于 2017-12-23 19:04:43 发布 3150 收藏 1

分类专栏: -----南邮CTF 我的CTF进阶之路 文章标签: 南邮CTF writeup 逆向

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/xiangshangbashaonian/article/details/78881637>

版权



-----南邮CTF 同时被 2 个专栏收录

6 篇文章 0 订阅

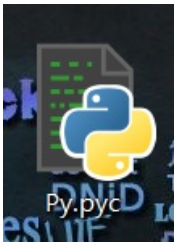
订阅专栏

我的CTF进阶之路

108 篇文章 18 订阅

订阅专栏

首先看题



下载后显示为Py.pyc 尝试notepad++打开显示乱码

```
1 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
2 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
3 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
4 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
5 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
6 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
7 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
```

所以直接百度

[python反编译 - 在线工具](#)

pyc反编译,py反编译,python反编译,python字节码反编译,支持所有python版本... pyc反编译,py反编译,python反编译,python字节码反编译,python代码美化搜索 ...

[tool.lu/pyc/](#) - 百度快照

选择<https://tool.lu/pyc/> 进行解密

```
1 #!/usr/bin/env python
2 # encoding: utf-8
3 import base64
4
5 def encode(message):
6     s = ''
7     for i in message:
8         x = ord(i) ^ 32
9         x = x + 16
10        s += chr(x)
11
12    return base64.b64encode(s)
13
14 correct = 'XlNkVmtUI1MgXWBZXCFeKY+AaXNt'
15 flag = ''
16 print 'Input flag:'
17 flag = raw_input()
18 if encode(flag) == correct:
19     print 'correct'
20 else:
21     print 'wrong'
```

```
#!/usr/bin/env python
# encoding: utf-8
import base64

def encode(message):
    s = ''
    for i in message:
        x = ord(i) ^ 32
        x = x + 16
        s += chr(x)

    return base64.b64encode(s)

correct = 'XlNkVmtUI1MgXWBZXCFeKY+AaXNt'
flag = ''
print 'Input flag:'
flag = raw_input()
if encode(flag) == correct:
    print 'correct'
else:
    print 'wrong'
```

所以我们只要将这个串"XlNkVmtUI1MgXWBZXCFeKY+AaXNt"解一次base64

再将每个字符ascii码都减下16

接着与32异或即可得到flag

解密代码如下：

```
import base64

correct = 'XlNkVmtUI1MgXWBZXCFeKY+AaXNt'

s = base64.b64decode(correct)

flag = ''

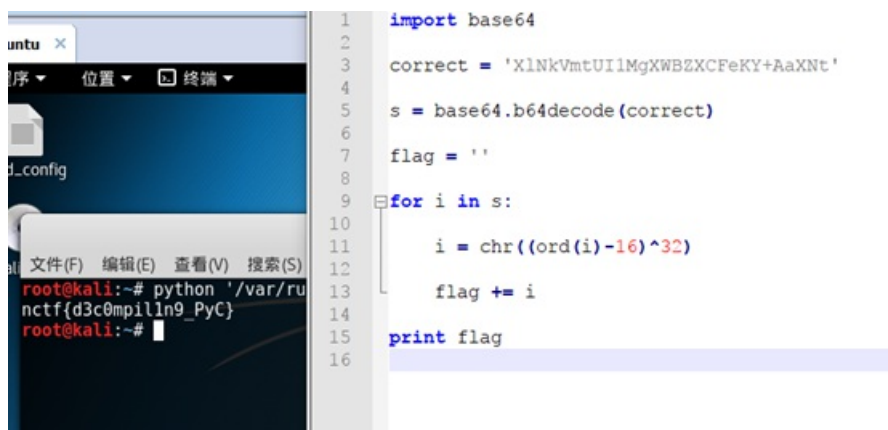
for i in s:

i = chr((ord(i)-16)^32)

flag += i

print flag
```

运行结果：



```
1 import base64
2
3 correct = 'XlNkVmtUI1MgXWBZXCFeKY+AaXNt'
4
5 s = base64.b64decode(correct)
6
7 flag = ''
8
9 for i in s:
10
11     i = chr((ord(i)-16)^32)
12
13     flag += i
14
15 print flag
16
```