XCTF 攻防世界 Reverse新手题(insanity, python-trade)

原创

sherlockjjobs 于 2020-12-12 15:42:48 发布 2361 收藏 2

分类专栏： 渗透测试 CTF 网络安全 文章标签： 网络安全 反汇编 反编译 安全 渗透测试

本文链接：https://blog.csdn.net/weixin_43456810/article/details/111063720

XCTF 攻防世界 Reverse新手题(insanity, python-trade)

1. insanity

这一题十分的简单，将下载下来的附件直接用IDA打开，查看Hey-View，在最右侧一栏进行查找，大概在后半部分，可以直接看到flag

2. python-trade

首先，这个题目没有用到IDA，因为看到下载的附件是.pyc后缀的，是python的字节码文件，可以先尝试pyc文件反编译。
有2种反编译的方法：

1. 使用在线工具：https://tool.lu/pyc/，直接将pyc文件上传，即可看到反编译后的代码
2. 使用命令行工具：uncompyle 安装和使用方法：

```
pip install uncompyle
uncompyle6 文件名.pyc > 文件名.py
```

接下来，分析源代码

```
def encode(message):
 s=''
 for i in message:
  x=ord(i)^32
  x=x+16
  s+=chr(x)
 return base64.b64encode(s)
```

分析可以得到：每个字符的ASCII码值先与32异或，然后加上16，最后进行base64编码，解码反过来即可：

```
import base64
correct='...'
message=base64.b64decode(correct)
s=''
for i in message:
 s+=chr((i-16)^32)
print(s)
```

这样就可以得到最终的flag了