

攻防世界 Crypto Broadcast

原创

==Microsoft== 于 2022-03-05 15:35:33 发布 2207 收藏

分类专栏: [Crypto](#) 文章标签: [安全](#) [密码学](#) [ctf](#)

本文为博主原创文章, 转载请加微信 CoderAllen, 未经允许不得转载!

本文链接: <https://blog.csdn.net/MrTreebook/article/details/123295672>

版权



[Crypto](#) 专栏收录该内容

17 篇文章 0 订阅

订阅专栏

攻防世界 Crypto Broadcast

1.打开文件夹

2.flag

1.打开文件夹

共享 查看

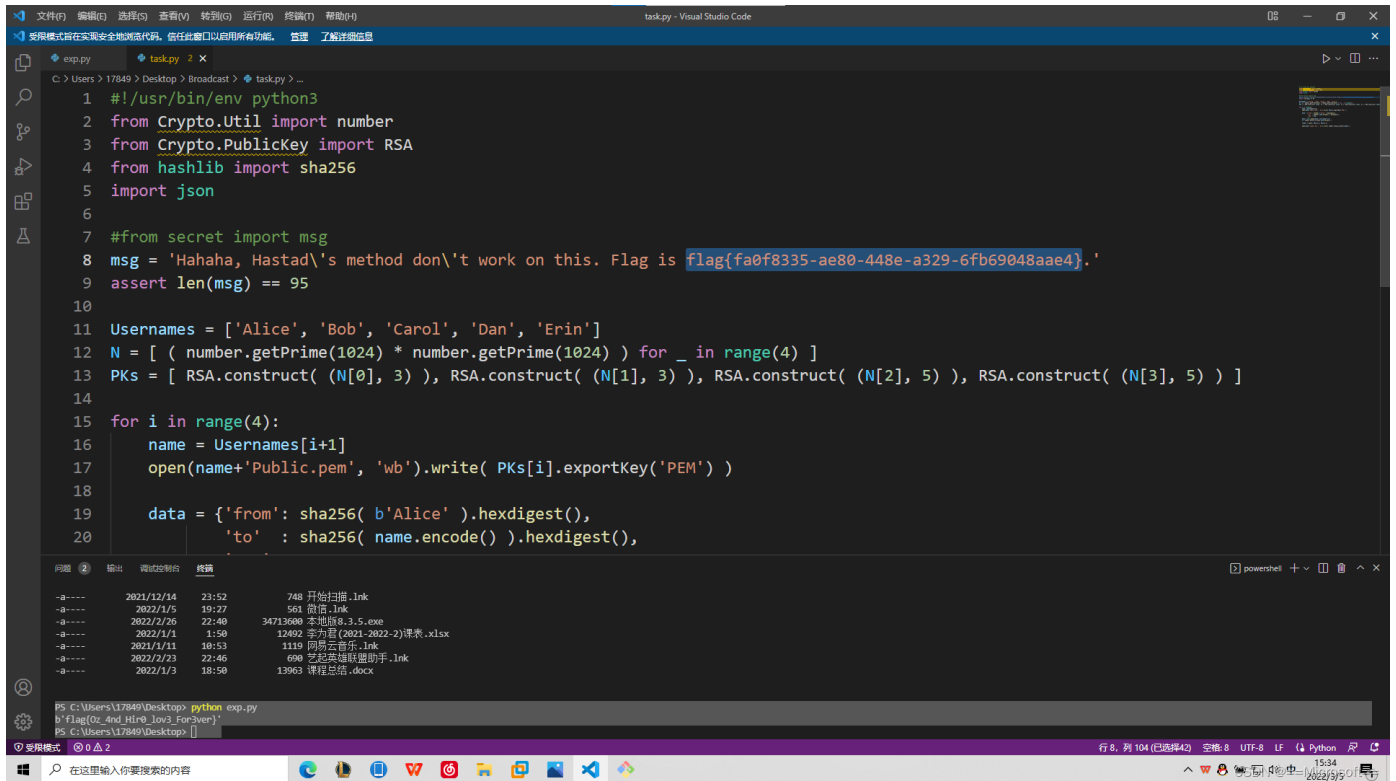
> Broadcast

名称	修改日期	类型	大小
BobCipher.enc	2022/3/5 15:32	Wireshark captu...	1 KB
BobPublic.pem	2022/3/5 15:32	PEM 文件	1 KB
CarolCipher.enc	2022/3/5 15:32	Wireshark captu...	1 KB
CarolPublic.pem	2022/3/5 15:32	PEM 文件	1 KB
DanCipher.enc	2022/3/5 15:32	Wireshark captu...	1 KB
DanPublic.pem	2022/3/5 15:32	PEM 文件	1 KB
ErinCipher.enc	2022/3/5 15:32	Wireshark captu...	1 KB
ErinPublic.pem	2022/3/5 15:32	PEM 文件	1 KB
task.py	2022/3/5 15:32	PY 文件	1 KB

统
- Persi

CSDN @==Microsoft==

- 看到一个.py
- 直接打开看看
- 看到一行flag
- 本以为是忽悠人的
- 没想到直接就对了



```
1 #!/usr/bin/env python3
2 from Crypto.Util import number
3 from Crypto.PublicKey import RSA
4 from hashlib import sha256
5 import json
6
7 #from secret import msg
8 msg = 'Hahaha, Hastad\'s method don\'t work on this. Flag is flag{fa0f8335-ae80-448e-a329-6fb69048aae4}.'
9 assert len(msg) == 95
10
11 Usernames = ['Alice', 'Bob', 'Carol', 'Dan', 'Erin']
12 N = [ ( number.getPrime(1024) * number.getPrime(1024) ) for _ in range(4) ]
13 PKs = [ RSA.construct( (N[0], 3) ), RSA.construct( (N[1], 3) ), RSA.construct( (N[2], 5) ), RSA.construct( (N[3], 5) ) ]
14
15 for i in range(4):
16     name = Usernames[i+1]
17     open(name+'Public.pem', 'wb').write( PKs[i].exportKey('PEM') )
18
19     data = {'from': sha256( b'Alice' ).hexdigest(),
20            'to' : sha256( name.encode() ).hexdigest(),
```

终端输出:

```
-a---- 2021/12/14 23:52 748 开始扫描 .lnk
-a---- 2022/1/5 19:27 561 微信 .lnk
-a---- 2022/2/26 22:40 34713680 本地版8.3.5.exe
-a---- 2022/1/1 1:50 12492 李为晋 (2021-2022-2)课表.xlsx
-a---- 2021/1/11 10:53 1110 网易云音乐 .lnk
-a---- 2022/2/23 22:46 690 芝士英雄辅助助手 .lnk
-a---- 2022/1/3 18:50 13963 课程总结.docx
```

```
PS C:\Users\17849\Desktop> python exp.py
b'Flag{0z_4nd_Hlr0_lov3_For3ver}'
PS C:\Users\17849\Desktop>
```

2.flag

flag{fa0f8335-ae80-448e-a329-6fb69048aae4}