CTF Broadcast

原创

艺博东 于 2020-09-25 23:38:21 发布 10359 收藏 6

分类专栏： 网络攻防 文章标签： CTF

本文链接：https://blog.csdn.net/HYD696/article/details/108805993

网络攻防 专栏收录该内容

24 篇文章 17 订阅

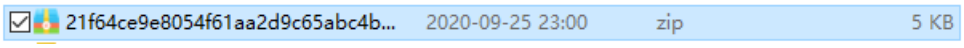
订阅专栏

题目来源： 2019_Redhat

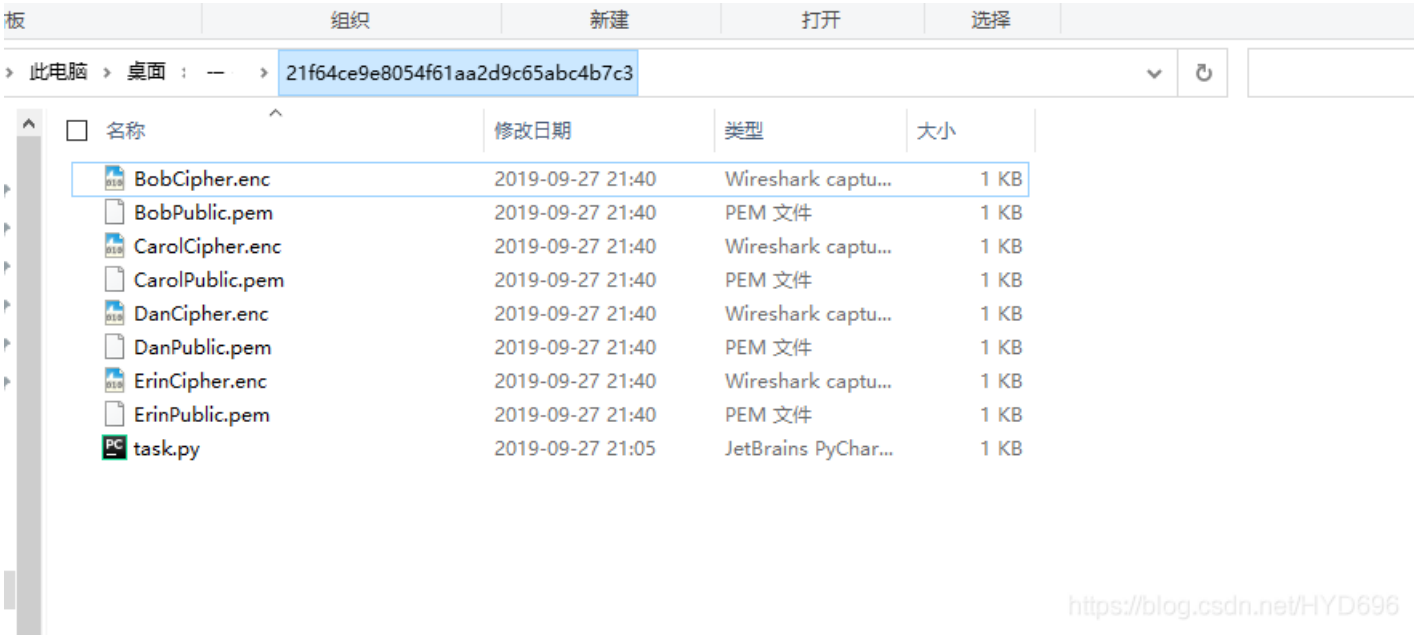
题目描述： 粗心的Alice在制作密码的时候，把明文留下来，聪明的你能快速找出来吗？

题目附件： 附件1

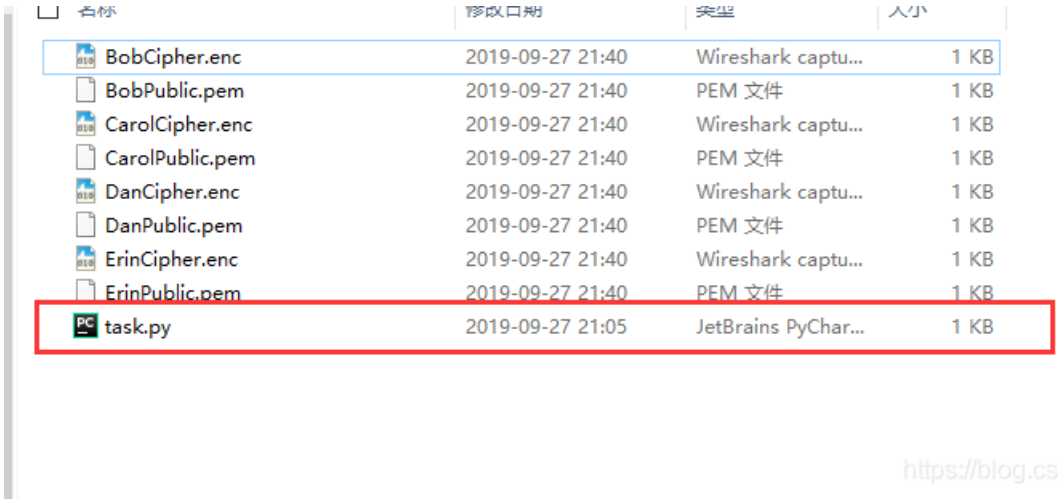
1、 附件1



2、解压后



3、选中“task.py”—>打开



4、可直接找到flag

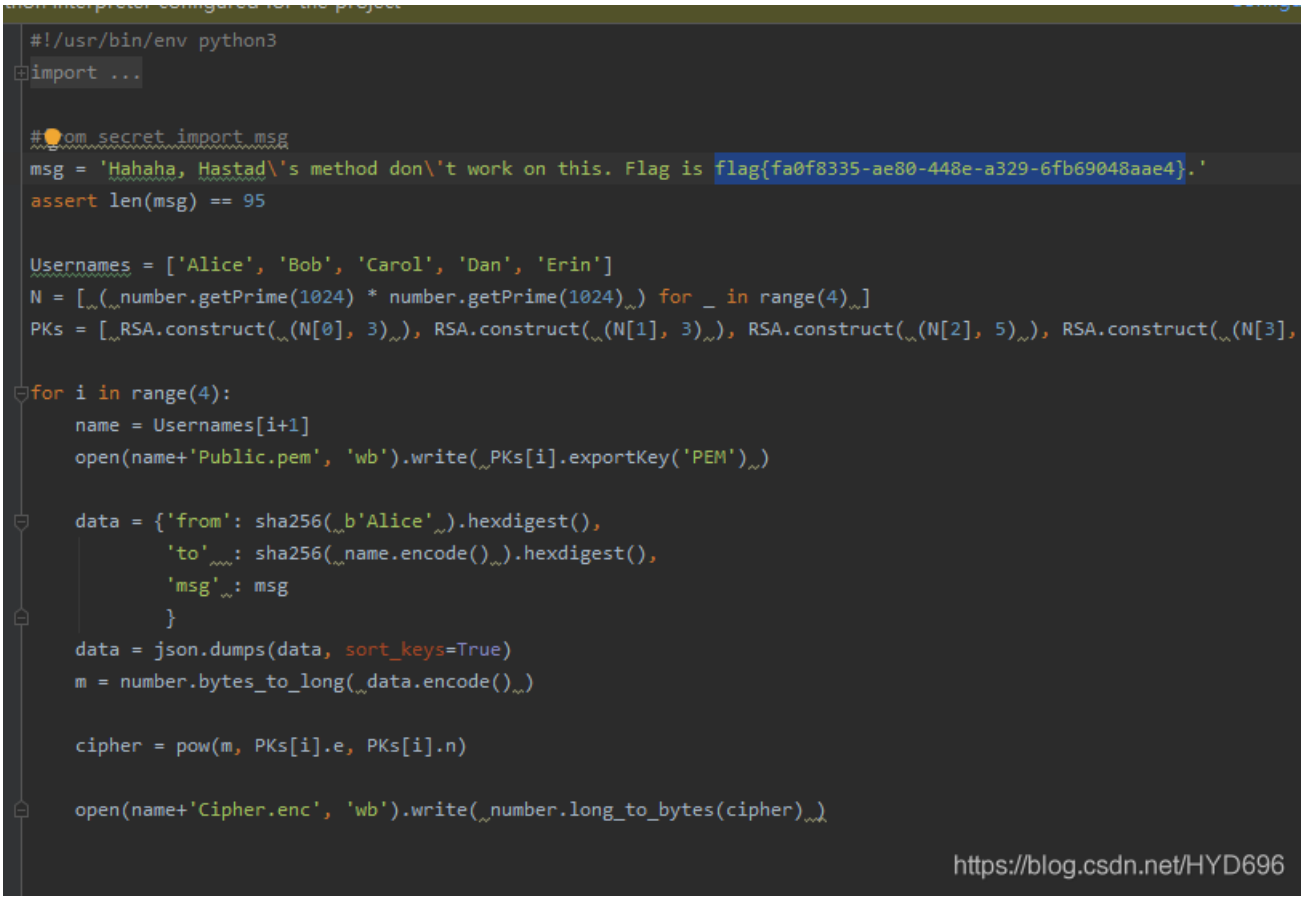
```
#!/usr/bin/env python3
from Crypto.Util import number
from Crypto.PublicKey import RSA
from hashlib import sha256
import json

#from secret import msg
msg = 'Hahaha, Hastad's method don't work on this. Flag is flag{fa0f8335-ae80-448e-a329-6fb69048aae4}.'
assert len(msg) == 95

Usernames = ['Alice', 'Bob', 'Carol', 'Dan', 'Erin']
N = [ ( number.getPrime(1024) * number.getPrime(1024) ) for _ in range(4) ]
PKs = [ RSA.construct( (N[0], 3) ), RSA.construct( (N[1], 3) ), RSA.construct( (N[2], 5) ), RSA.construct( (N[3], 5) ) ]
```

for i in range(4):
name = Usernames[i+1]
open(name+‘Public.pem’, ‘wb’).write(PKs[i].exportKey(‘PEM’))

data = {‘from’: sha256(b’Alice’).hexdigest(),
‘to’ : sha256(name.encode()).hexdigest(),
‘msg’ : msg
}
data = json.dumps(data, sort_keys=True)
m = number.bytes_to_long(data.encode())

cipher = pow(m, PKs[i].e, PKs[i].n)

open(name+‘Cipher.enc’, ‘wb’).write(number.long_to_bytes(cipher))



5、OK

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