攻防世界crypto高手题之RSA256

原创

沐一 · 林 于 2021-09-17 20:39:59 发布 47 收藏 1

分类专栏： CTF 密码学 文章标签： ctf

本文链接：https://blog.csdn.net/xiao__1bai/article/details/120356360

CTF 同时被 2 个专栏收录

167 篇文章 6 订阅

订阅专栏

密码学

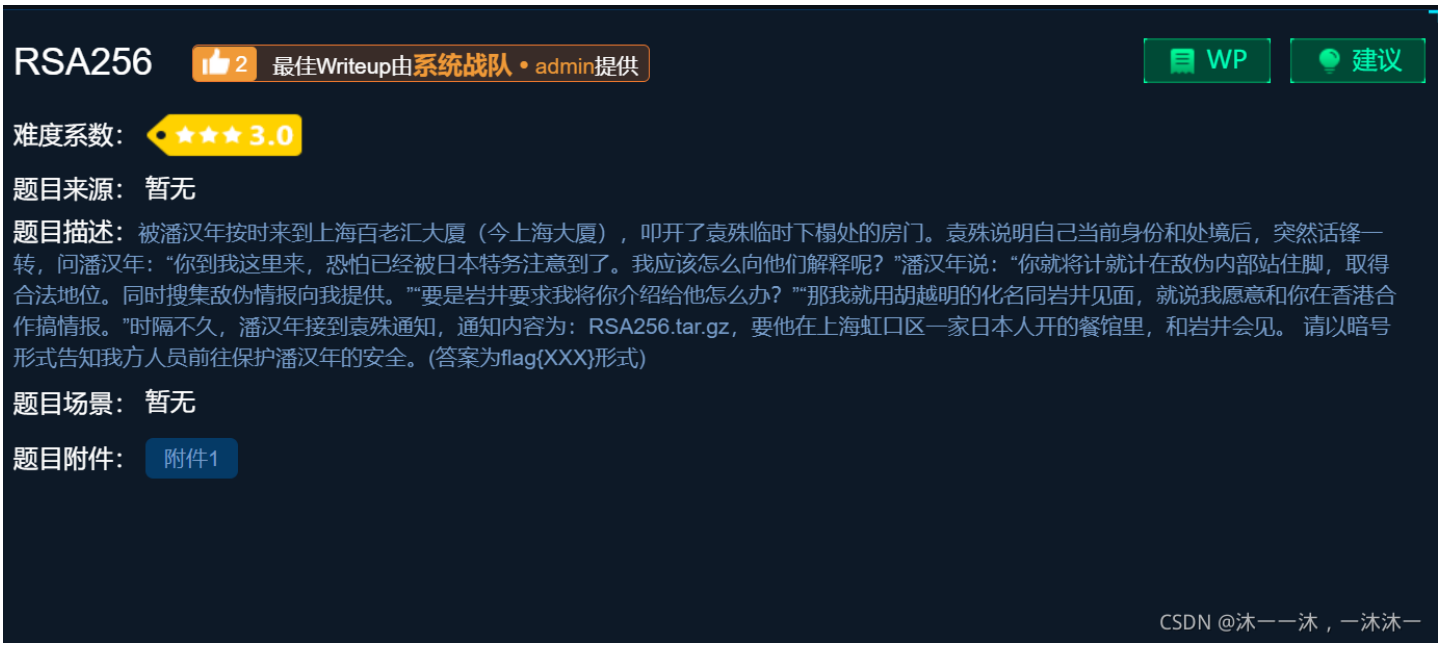
51 篇文章 1 订阅

订阅专栏

攻防世界crypto高手题之RSA256

继续开启全栈梦想之逆向之旅~

这题是攻防世界crypto高手题的RSA256



下载压缩包，解压，是两个附件，一个没有后缀，一个.txt文件，打开查看内容，感觉是RSA的密文密钥文件：

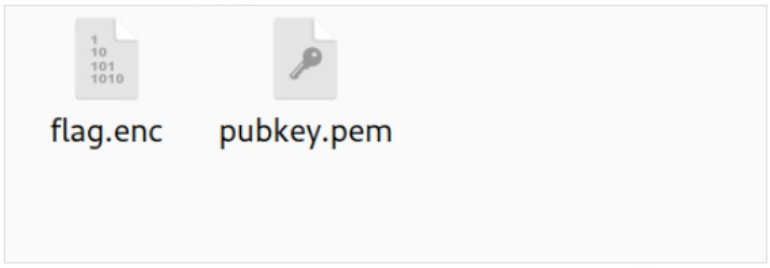
```
RSA256/                                                0000755 0000000 0000000 00000000000 13446064553
嵺??绘□癥W   Z闊□℃?嗷傌野□(?
BLIC KEY-----
MDwwDQYJKoZIhvcNAQEBBQADKwAwKAIhAKm9THp3YzcKBC/mvsfdyEFgLblCx6Ni
0bXTcqTQiRLZAgMBAAE=
-----END PUBLIC KEY-----
```

.

.

翻一下以前的笔记，这是对`CTF-RSA-tool`使用的示例，感觉题目类型就是这种密钥和密文的文件。

```
# factordb.com
python2 solve.py --verbose  -k examples/jarvis_oj_mediumRSA/pubkey.pem --decrypt
examples/jarvis_oj_mediumRSA/flag.enc
```




```
-----BEGIN PUBLIC KEY-----
MDowDQYJKoZIhvcNAQEBBQADKQAwJgIhAMJjauXD2OQ/+5erCQKPGqxsC/bNPXDr
yigb/+l/vjDdAgEC
-----END PUBLIC KEY-----
```

默认 (UTF-8, 部分) 其他： ISO-8859-1

```
n>·ß#îáÓ¾ºx ÈeÂ½=ImÚdA¹y
```

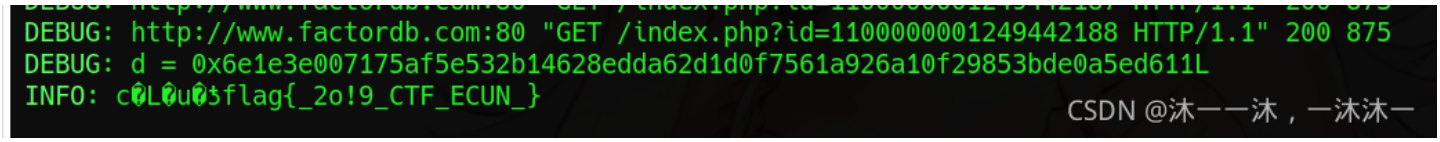

.

.

验证猜想，直接脚本跑一下：

```
└─$ python2 solve.py --verbose  -k /home/wdnmd/桌面/gy.key --decrypt /home/wdnmd/桌面/1.txt

DEBUG: factor N: try past ctf primes
DEBUG: factor N: try Gimmicky Primes method
DEBUG: factor N: try Wiener's attack
DEBUG: Starting new HTTP connection (1): www.factordb.com:80
DEBUG: http://www.factordb.com:80 "GET /index.php?query=767753333402239611394270507078404178
111569780851469703123158866715466662591 61 HTTP/1.1" 200 993
DEBUG: http://www.factordb.com:80 "GET /index.php?id=110000000012494421 87 HTTP/1.1" 200 873
```



.

.

得到flag。

.

.

总结：

> 无

解毕！敬礼！