

# 攻防世界 Crypto高手进阶区 3分题 wtc\_rsa\_bbq

原创

思源湖的鱼 于 2020-12-10 11:05:54 发布 491 收藏

分类专栏: [ctf](#) 文章标签: [ctf](#) [攻防世界](#) [crypto](#) [rsa](#)

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/weixin\\_44604541/article/details/110948708](https://blog.csdn.net/weixin_44604541/article/details/110948708)

版权

## CTF

[ctf 专栏收录该内容](#)

200 篇文章 23 订阅

订阅专栏

### 前言

继续ctf的旅程

攻防世界Crypto高手进阶区的3分题

本篇是wtc\_rsa\_bbq的writeup

发现攻防世界的题目分数是动态的

就仅以做题时的分数为准了

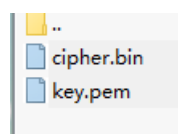
### 解题过程

得到一个无后缀文件

扔进winhex

```
00000000 | 50 4B 03 04 14 00 02 00 08 00 47 00 38 45 BA BA | PK          G 8E°°
00000016 | 16 D1 37 04 00 00 32 04 00 00 0A 00 00 00 63 69 | Ñ7 2      ci
00000032 | 70 68 65 72 2E 62 69 6E 01 32 04 CD FB 04 94 0E | pher.bin 2 Íû "
00000048 | 99 58 09 B8 34 6A 72 25 A4 EF 8F 17 5E F3 03 1D | ¢X ,4jr&mi ^ó
```

发现是个zip



那不就是个RSA

扔进kali

```
python3 RsaCtfTool.py --publickey key.pem --uncipherfile cipher.bin
```

```
Clear text : Congratulations! Here is a treat for you: flag{how_d0_you_7urn_this_0n?}
```

得到flag

## 结语

RSA