攻防世界 Crypto高手进阶区 3分题 cr4-poor-rsa

原创

思源湖的鱼 于 2020-12-13 14:08:12 发布 159 收藏 1

分类专栏： ctf 文章标签： ctf 攻防世界 rsa crypto

本文链接：https://blog.csdn.net/weixin_44604541/article/details/111109587

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cr4-poor-rsa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

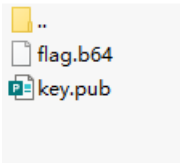
扔进winhex

00000000	66	6C	61	67	2E	62	36	34	00	00	00	00	00	00	00	00	flag.b64
00000016	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000032	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000048	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000064	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000096	00	00	00	00	30	30	30	30	36	34	34	00	30	30	30	31	0000644 0001
00000112	37	35	30	00	30	30	30	31	37	35	30	00	30	30	30	30	750 0001750 0000
00000128	30	30	30	30	31	30	35	00	31	33	30	32	33	32	31	33	0000105 13023213
00000144	36	30	32	00	30	31	32	34	32	30	00	20	30	00	00	00	602 012420 0
00000160	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

应该是个压缩文件

改后缀

解压



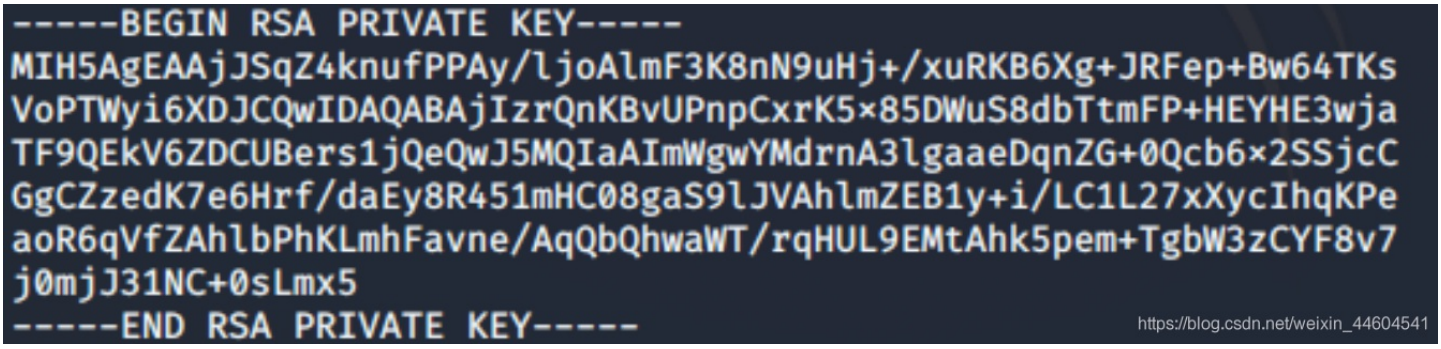
一个公钥和一个解密文件

尝试公钥解密

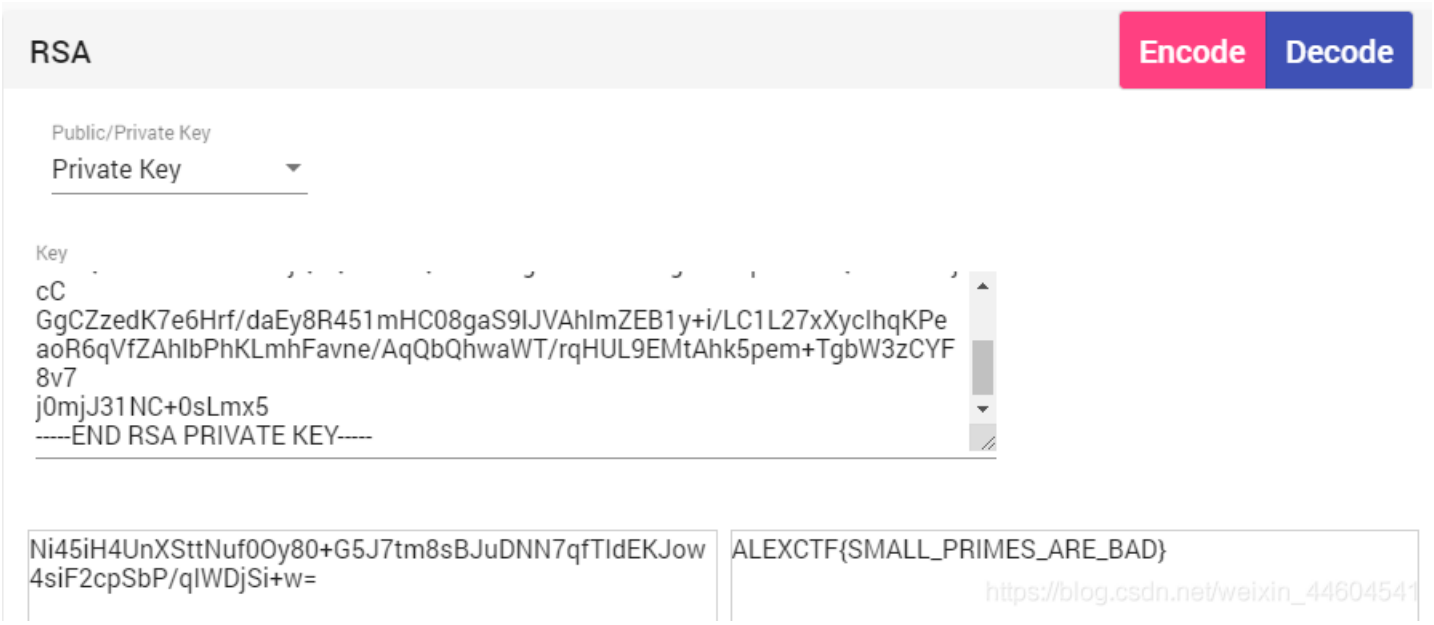
失败

那看来是要先生成私钥

```
python3 RsaCtfTool.py --publickey key.pub --privatekey
```



然后再扔进工具



得到flag

结语

RSA

两个工具

- RsaCtfTool
- CaptfEncoder