

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](#)

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/111109587

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

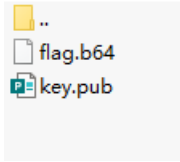
扔进winhex

00000000	66 6C 61 67 2E 62 36 34	00 00 00 00 00 00 00 00	flag.b6
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

RSA Encode Decode

Public/Private Key
Private Key

Key
-----BEGIN PUBLIC KEY-----
ME0wDQYJKoZIhvcNAQEBBQADPAAwOQlyUqmeJJ7nzzwMv5Y6AJZhdvJzfbh4/v
8
bkSgeI4PjURXqfgcOuEyrFaD01soulwyQkMCAwEAAQ==
-----END PUBLIC KEY-----

Ni45iH4UnXSttNuf0Oy80+G5J7tm8sBJuDNN7qfTIdEKJow false
4siF2cpSbP/qIWDjSi+w=

https://blog.csdn.net/weixin_44604541

失败

那看来是要先生成私钥

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

```
-----BEGIN RSA PRIVATE KEY-----  
MIH5AgEAAjJSqZ4knufPPAy/ljoAlmF3K8nN9uHj+/xuRKB6Xg+JRFep+Bw64TKs  
VoPTWyI6XDJCQwIDAQABAjIzrQnKBvUPnpCxrK5x85DWuS8dbTtmFP+HEYHE3wja  
TF9QEkV6ZDCUBers1jQeQwJ5MQIaAImWgwYMdrnA3lgaaeDqnZG+0Qcb6x2SSjcC  
GgCZzedK7e6Hrf/daEy8R451mHC08gaS9lJVAhlmZEB1y+i/LC1L27xXycIhqKPe  
aoR6qVfZAhlbPhKlmhFavne/AqQbQhwaWT/rqHUL9EMtAhk5pem+TgbW3zCYF8v7  
j0mjJ31NC+0sLmx5  
-----END RSA PRIVATE KEY-----
```

https://blog.csdn.net/weixin_44604541

然后再扔进工具

RSA

Encode

Decode

Public/Private Key

Private Key

Key

```
cC  
GgCZzedK7e6Hrf/daEy8R451mHC08gaS9IJVAhlmZEB1y+i/LC1L27xXyclhqKPe  
aoR6qVfZAhIbPhKlMhFavne/AqQbQhwaWT/rqHUL9EMtAhk5pem+TgbW3zCYF  
8v7  
j0mjJ31NC+0sLmx5  
-----END RSA PRIVATE KEY-----
```

```
Ni45iH4UnXSttNuf0Oy80+G5J7tm8sBJuDNN7qfTIdEKJow  
4siF2cpSbP/qlWDjSi+w=
```

```
ALEXCTF{SMALL_PRIMES_ARE_BAD}
```

https://blog.csdn.net/weixin_44604541

得到flag

结语

RSA

两个工具

- [RsaCtfTool](#)
- [CaptfEncoder](#)