

攻防世界-Misc萌新-5-1(xortool使用)-WDCTF-2017

原创

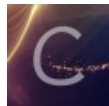
大千SS 于 2019-04-22 18:26:54 发布 4575 收藏 2

分类专栏: [隐写、杂项](#) [攻防世界](#) 文章标签: [攻防世界Misc](#) [xortool使用](#)

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/zz_Caleb/article/details/89457961

版权



[隐写、杂项](#) 同时被 2 个专栏收录

24 篇文章 1 订阅

订阅专栏



[攻防世界](#)

28 篇文章 1 订阅

订阅专栏

拿到文件, 照惯例winhex查看, 未知类型文件, xortool尝试:

```
root@kali:~# xortool -c 20 cipher
The most probable key lengths:
 2: 12.2%
 5: 11.9%
 9: 9.8%
13: 22.2%
20: 6.8%
22: 6.2%
26: 12.8%
30: 4.6%
39: 7.8%
52: 5.7%
Key-length can be 3*n
1 possible key(s) of length 13:
GoodLuckToYou
Found 1 plaintexts with 95.0%+ valid characters
See files filename-key.csv, filename-char used-perc valid.csv
root@kali:~#
```

尝试出了key: GoodLuckToYou, 对原文件进行异或, 脚本如下:

```
key = 'GoodLuckToYou'
flag = ''
with open('cipher') as f:
    con = f.read()
    for i in range(len(con)):
        flag += chr(ord(con[i]) ^ ord(key[i%13]))
f = open('flag.txt', 'w')
f.write(flag)
f.close()
```

输出的文件中看到flag: wdflag{You Are Very Smart}