xctf攻防世界 MISC高手进阶区 halo

原创

l8947943 于 2022-02-03 16:27:36 发布 10463 收藏

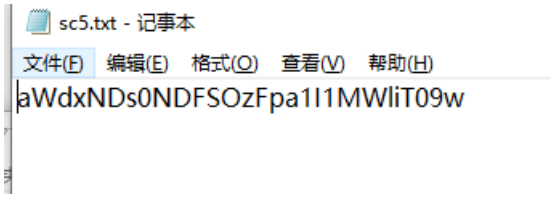
分类专栏： 攻防世界misc之路 文章标签： misc

本文链接：https://blog.csdn.net/l8947943/article/details/122776671

1. 进入环境，下载附件

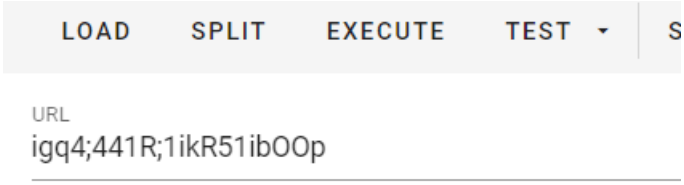
先说一下，这个题坑的一比，官方wp都是错的，人麻了

附件是一个压缩包，解压后里面是个txt文件，如图：



2. 问题分析

看起来像是base64之类的编码，尝试解码，如图：



没有什么思路，看了官方的wp后，发现是考察base64的异或用法，直接使用脚本：

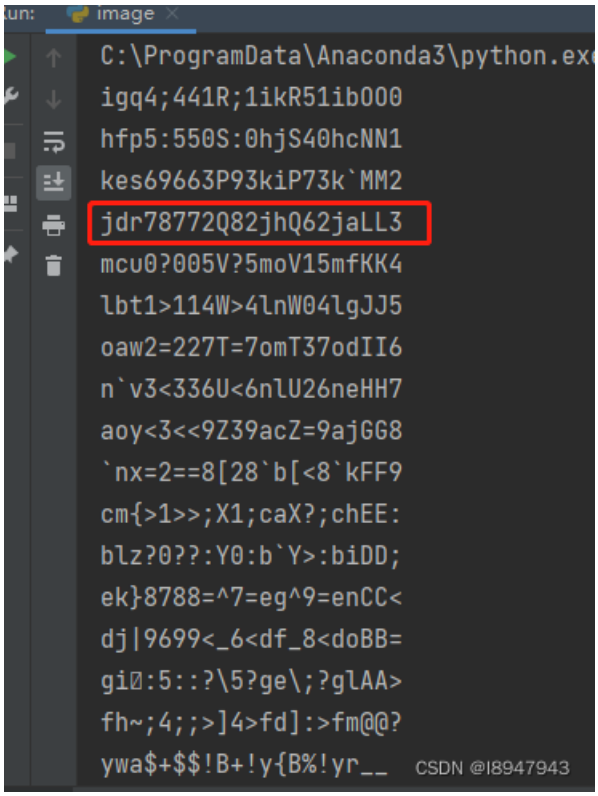
```
from base64 import *

b = b64decode('aWdxNDs0NDFSOzFpa1I1MWliT08w')

data = list(b)

for i in range(0, 200):
    key = ''
    for j in range(len(data)):
     # 注意，python3中已经不用ord去转了
        key += chr(data[j]^i)
    print(key)
```

输出结果如图：



一堆输出结果中只有这个是正常的，最终的答案为：`flag{jdr78772Q82jhQ62jaLL3}`

注意：附件中下载的数据是aWdxNDs0NDFSOzFpa1l1MWliT09w，而官方wp给的是aWdxNDs0NDFSOzFpa1l1MWliT08w。

感觉题目出的一点都不好！！！