

xctf攻防世界 MISC高手进阶区 halo

原创

[18947943](#) 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](#)

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/18947943/article/details/122776671>

版权



[攻防世界misc之路](#) 专栏收录该内容

68 篇文章 2 订阅

订阅专栏

1. 进入环境, 下载附件

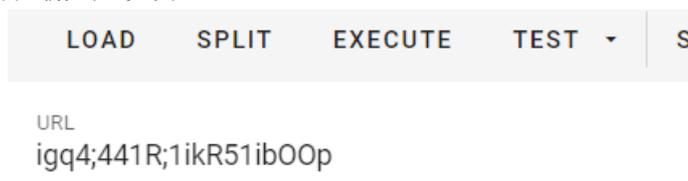
先说一下, 这个题坑的一比, 官方wp都是错的, 人麻了

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:

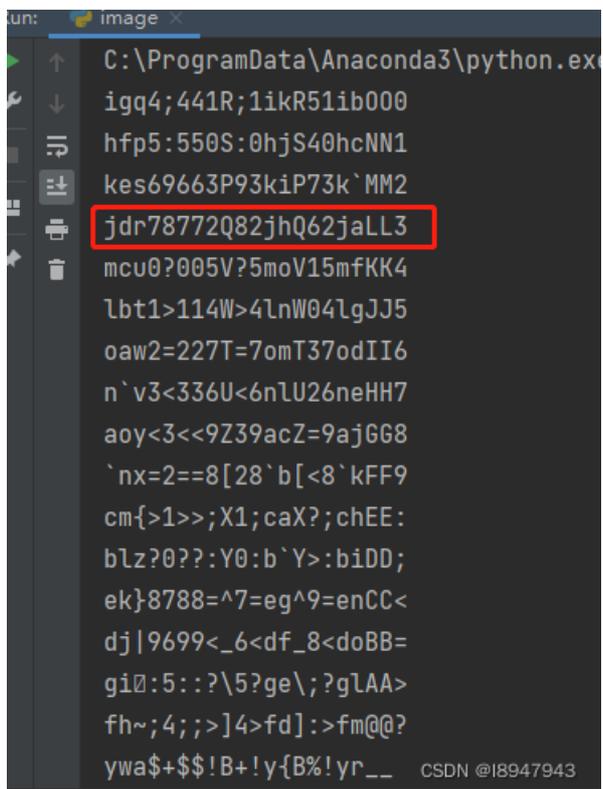
```
from base64 import *

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：



```
un: image x
C:\ProgramData\Anaconda3\python.exe
igq4;441R;1ikR51ib000
hfp5:550S:0hjs40hcNN1
kes69663P93kiP73k`MM2
jdr78772Q82jhQ62jaLL3
mcu0?005V?5moV15mfKK4
lbt1>114W>4lnW04lgJJ5
oaw2=227T=7omT37odII6
n`v3<336U<6nLU26neHH7
aoy<3<<9Z39acZ=9ajGG8
`nx=2==8[28`b[<8`kFF9
cm{>1>>;X1;caX?;chEE:
blz?0???:Y0:b`Y>:biDD;
ek}8788=^7=eg^9=enCC<
dj|9699<_6<df_8<doBB=
gi0:5::?\5?ge\;?g\AA>
fh~;4;;>]4>fd]:>fm@0?
ywa$+$!B+!y{B%!yr__ CSDN @18947943
```

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 `aWdxNDs0NDFSOzFpa1I1MWliT09w`，而官方wp给的是 `aWdxNDs0NDFSOzFpa1I1MWliT08w`。

感觉题目出的一点都不好!!!