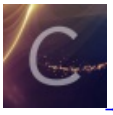
i春秋网鼎杯网络安全大赛advanced题目writeup

原创

iqiqiya 于 2018-10-13 21:09:31 发布 2238 收藏 4
分类专栏： 我的逆向之路 我的CTF之路 ------2018i春秋网鼎杯 我的CTF进阶之路 文章标签： 2018i春秋网鼎杯CTF第一场逆向题目advanced的w advanced的writeup


我的逆向之路 同时被 3 个专栏收录
108 篇文章 10 订阅
订阅专栏


我的CTF之路
92 篇文章 5 订阅
订阅专栏


------2018i春秋网鼎杯
6 篇文章 0 订阅
订阅专栏

今天打了护网杯

发现啥也不会 悲伤　就想起来了未完成的网鼎杯　来补坑(通过观摩大佬writeup)

file命令查看是一个64位的ELF文件　运行后无交互动作　只输出

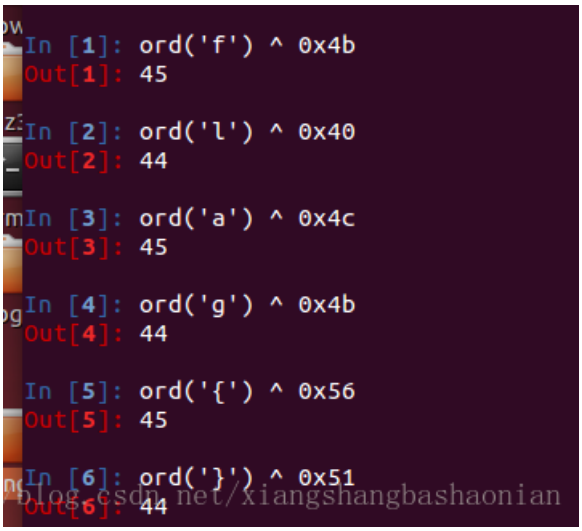
welcome, here is your identification, please keep it in your pocket:
4b404c4b5648725b445845734c735949405c414d5949725c45495a51

```
iqiqiya@521:~/Desktop/wangdingbei$ file src
src: ELF 64-bit LSB  shared object, x86-64, version 1 (SYSV), dynamically linked (uses shared
 libs), for GNU/Linux 3.2.0, BuildID[sha1]=c87b49d516e19f9b4d01673c90ac79283f6672a2, stripped
iqiqiya@521:~/Desktop/wangdingbei$ ./src
welcome, here is your identification, please keep it in your pocket: 4b404c4b5648725b44584573
4c735949405c414d5949725c45495a51
iqiqiya@521:~/Desktop/wangdingbei$
                                                    https://blog.csdn.net/xiangshangbashaonian
```

到这里 平常的思路是打开IDA 进行分析(当时我就是这么做的。。。)

而大佬们则是一眼看出这是异或flag{********}之后得到的

于是上python　挑出前几位**f l a g {**与最后一位 **}** 分别与对应位置的十六进制进行异或

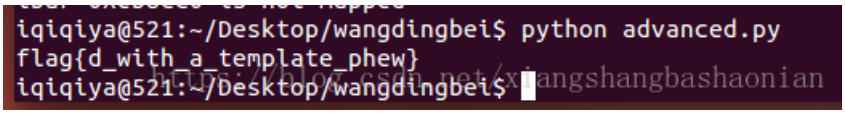


然后就可以发现有规律 每次得到的结果只会是44或者45

根据异或的性质 我们将奇数位与45异或 偶数位与44异或 就可以得到flag

代码如下：

```
import libnum
enc = libnum.n2s(0x4b404c4b5648725b445845734c735949405c414d5949725c45495a51)
#将十六进制转成字符串
flag = ''
for i in range(len(enc)):
 if i % 2 == 0:
  flag += chr(ord(enc[i]) ^ 45)
 else:
  flag += chr(ord(enc[i]) ^ 44)
print flag
```



这应当算是非预期思路了 等哪天弄懂了常规思路怎么做 再来补坑 告辞

参考链接：https://xz.aliyun.com/t/2608#toc-12