2018网鼎杯re-advance复现笔记

原创

木木or沐沐 于 2018-08-23 17:39:15 发布

拿到程序运行一下，可以看到输出一个16进制的串，我们感觉这应该是一个字符串加密后的结果，尝试把这个16进制的串转换成字符串，这里看到writeup中有用python的libnum库，可以很方便的实现这个操作。

这是libnum库的安装和使用方法：https://www.cnblogs.com/pcat/p/7225782.html

```
>>> libnum.n2s(0x4b404c4b5648725b445845734c735949405c414d5949725c45495a51)
'K@LKVHr[DXEsLsYI@\\AMYIr\\EIZQ'
```

看到这里尝试一下异或

d = a ⊕ b ⊕ c 可以推出 a = d ⊕ b ⊕ c.

```
>>> ord('f')^0x4b
45
>>> ord('l')^0x40
44
>>> ord('a')^0x4c
45
>>> ord('g')^0x4b
44
```

可以看出奇数位异或45，偶数位异或44

```
s='K@LKVHr[DXEsLsYI@\\AMYIr\\EIZQ'
flag=""
for i in range(len(s)):
    if i%2==0:
        flag+=chr(ord(s[i])^45)
    else:
        flag+=chr(ord(s[i])^44)
print flag
```

flag{d_with_a_template_phew}

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