

蓝鲸ctf 逆向0x1 Warmup

原创

Startr4ck 于 2018-04-10 18:55:41 发布 568 收藏

分类专栏: [ctf](#) 文章标签: [逆向](#) [蓝鲸ctf writeup](#)

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/shakeyin1998/article/details/79885818>

版权



[ctf](#) 专栏收录该内容

17 篇文章 0 订阅

订阅专栏

Warmup

【题目链接】 <http://whalectf.xin/challenges#Warmup>

【解题流程和思路】

打开IDA之后搜索对比成功和对比失败的字符串, 然后转到程序对比处

```
}
if ( !strcmp(&v17, aLdyv1qmzhuyCqQ) )
{
    u8 = (void *)sub_401700(&unk_417CF8, aContratulation);
    sub_401900(u8, &v17);
}
```

将v17溯源, 发现了v17是输入的字符进行变化得到的

```
*(&v17 + u6) ^= 0x11;
++u6;
```

直接将v17的数值再进行一次异或, 就可以得到flag

```
src = "LDYVLQNZHuY: |cQ[~Qyo|cQ{~QYO\CQ[~/s"
dis = ""
nm = 14
```