# 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



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, aLdyvlqmzhuyCqQ) )
{
  v8 = (void *)sub_401700(&unk_417CF8, aContratulation);
```

将v17溯源，发现了v17是输入的字符进行变化得到的

```
*(&v17 + v6) ^= 0x
++v6;
```

直接将v17的数值再进行一次异或，就可以得到flag

```
src = "LDYVLQMZHuY:|cQ[^Qyo|cQ{^QYO\CQ[^/s"
dis = " "
nn = 14
```