Bugkuctf--逆向第三题游戏过关题解

原创

Air_cat 于 2019-04-01 22:12:23 发布 1675 收藏
分类专栏： 逆向工程 二进制CTF 文章标签： Bugkuct ctf writeup

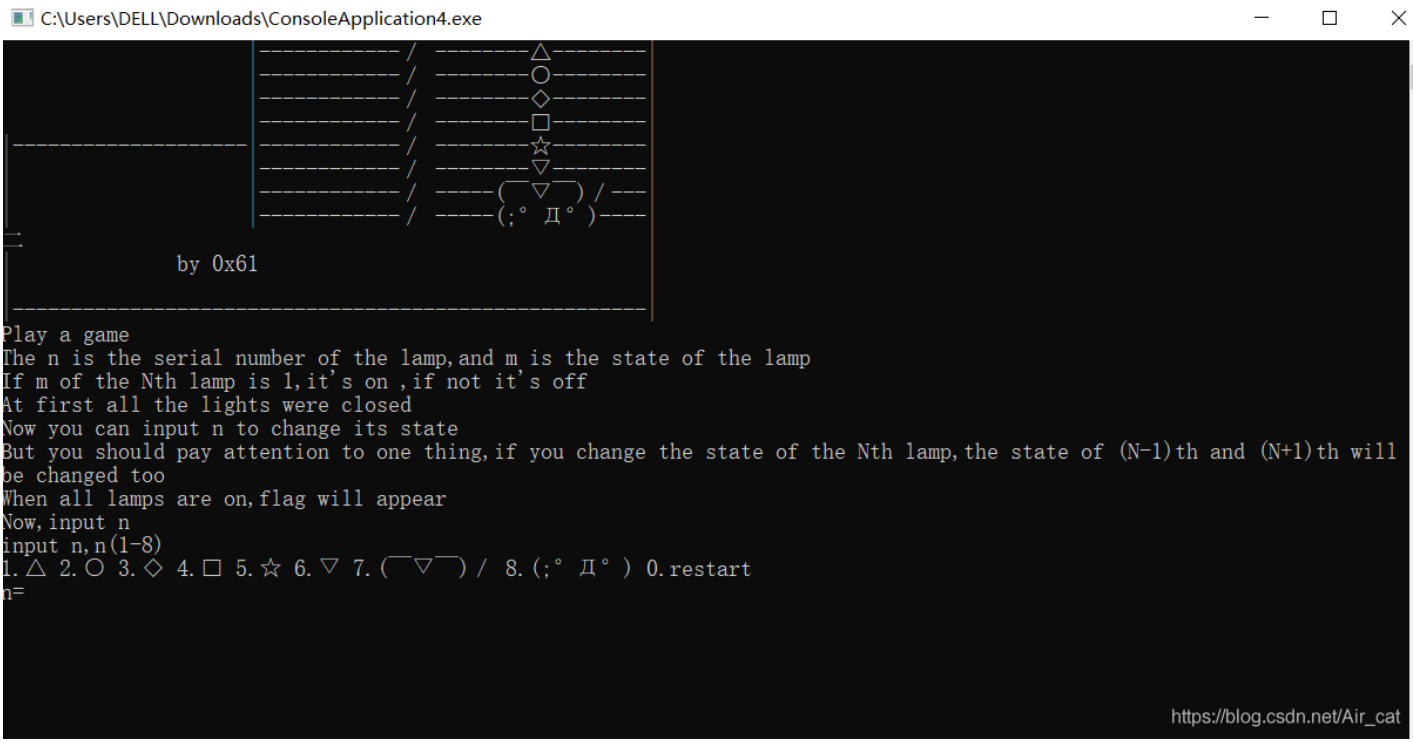
本文链接：https://blog.csdn.net/Air_cat/article/details/88958097


逆向工程 同时被 2 个专栏收录
25 篇文章 0 订阅
订阅专栏

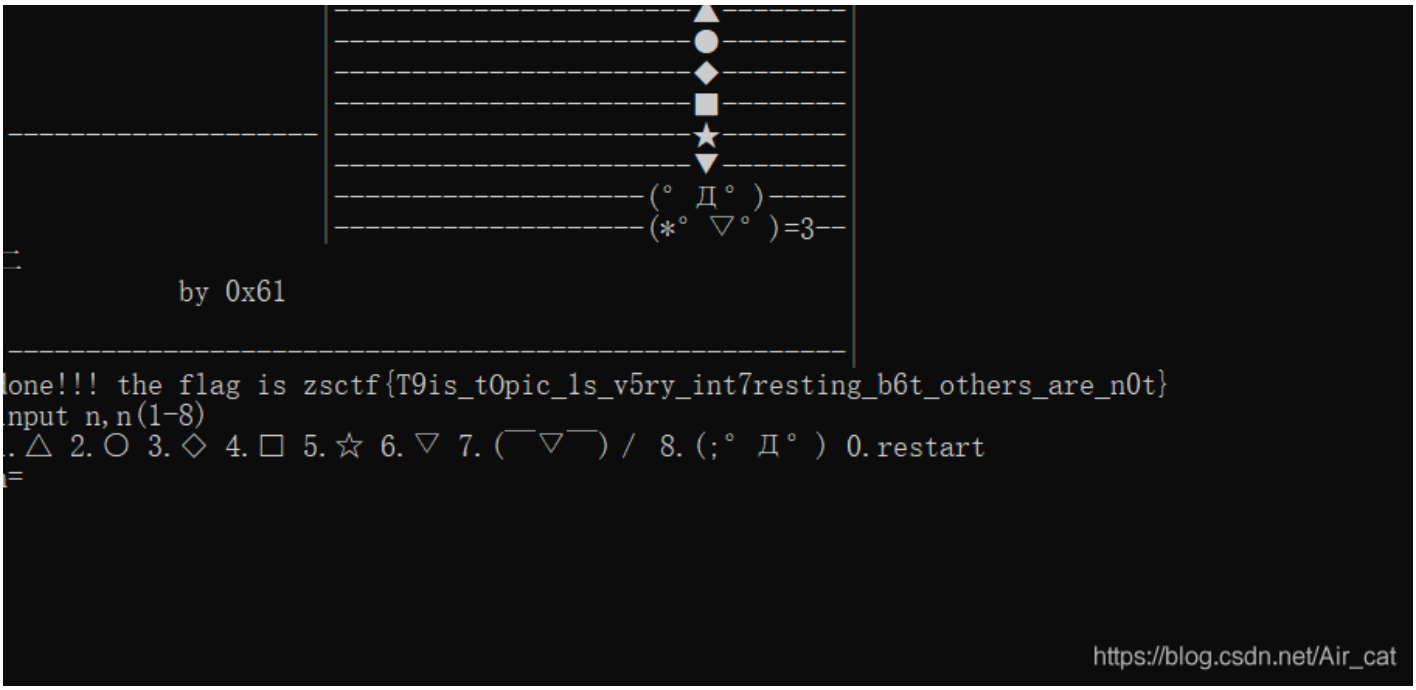

二进制CTF
21 篇文章 0 订阅
订阅专栏

题目链接：https://ctf.bugku.com/challenges

先让我们来打开文件



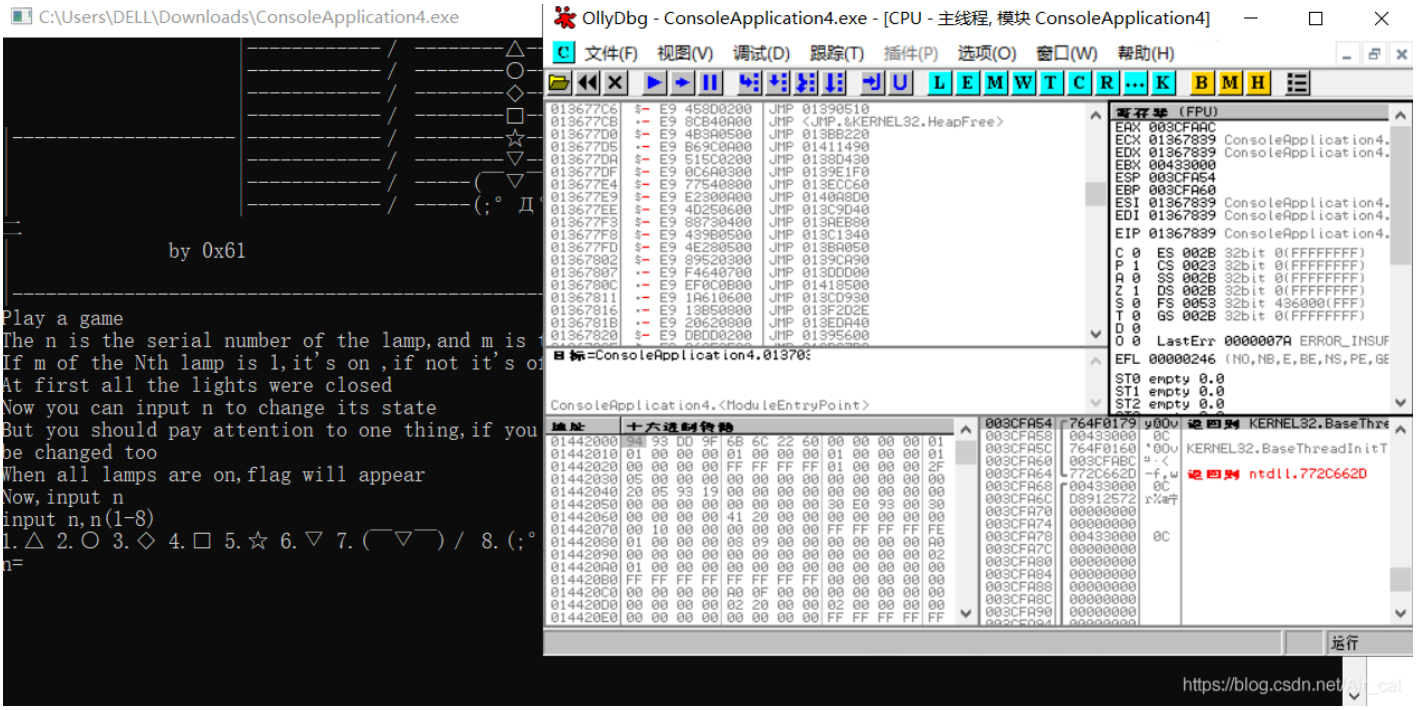
既然题目都说是游戏过关了，那就玩玩这个游戏呗（雾



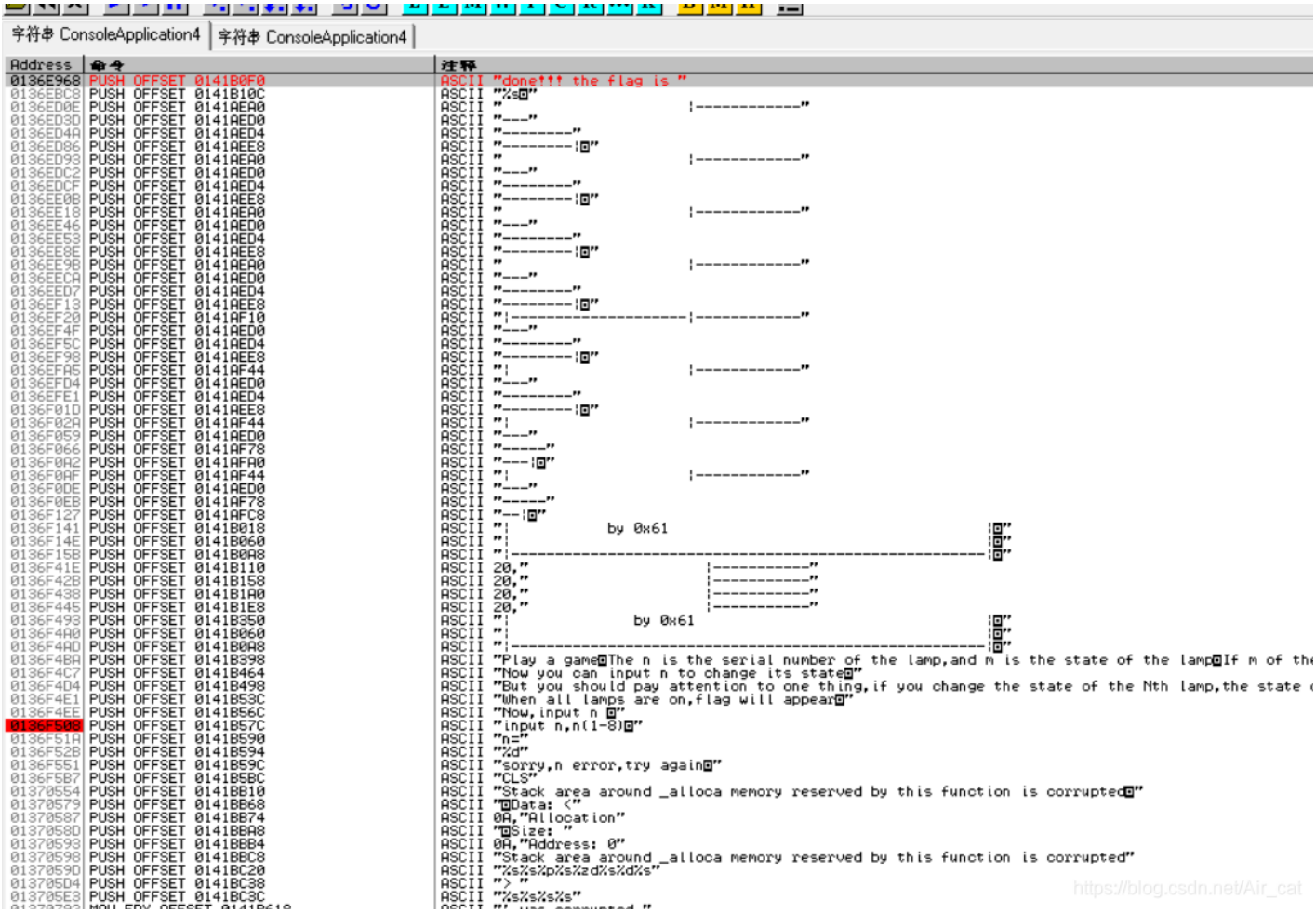
游戏还是很简单的，但显然这道题应该用逆向的思维来做（废话

正式部分：

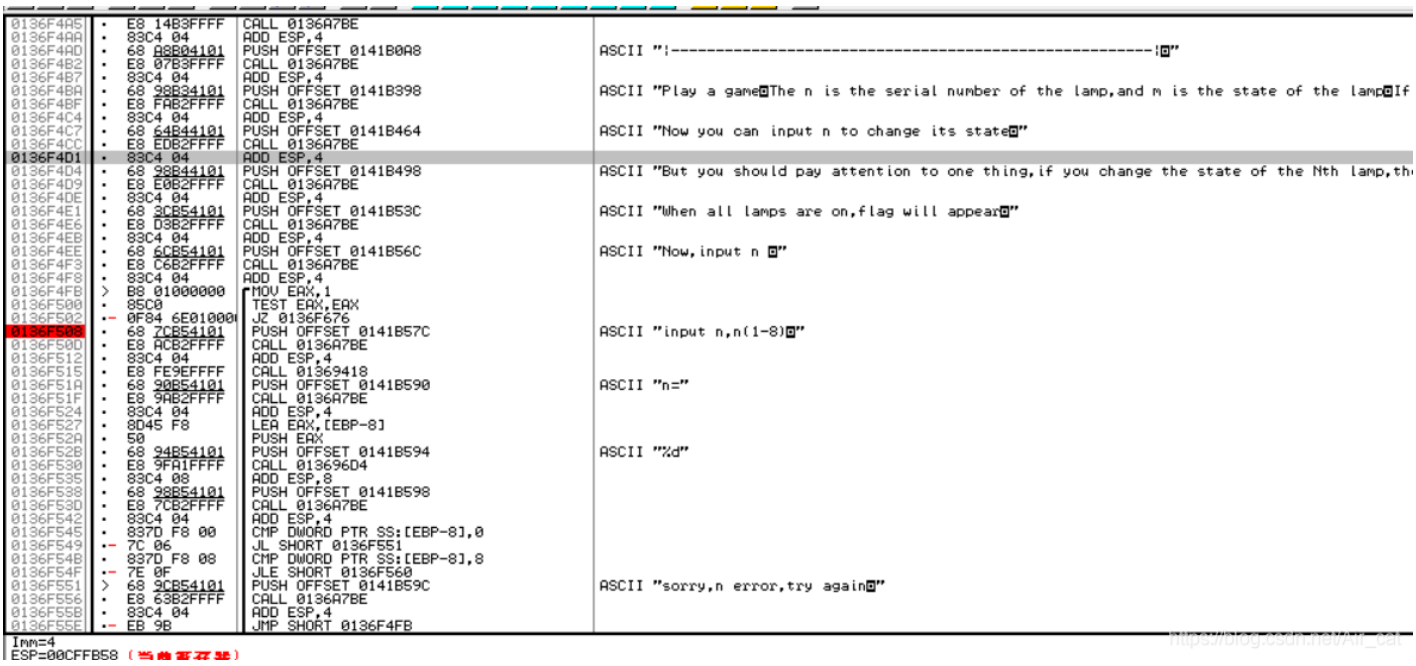
逆向的题拿到手一般能考虑的工具（方法）就是通过ida（静态分析）或者通过od（动态分析），因为ida还搞不太懂（菜鸟），然后看了下盲猜这题是要求运行的时候就能直接跳结果，开始od



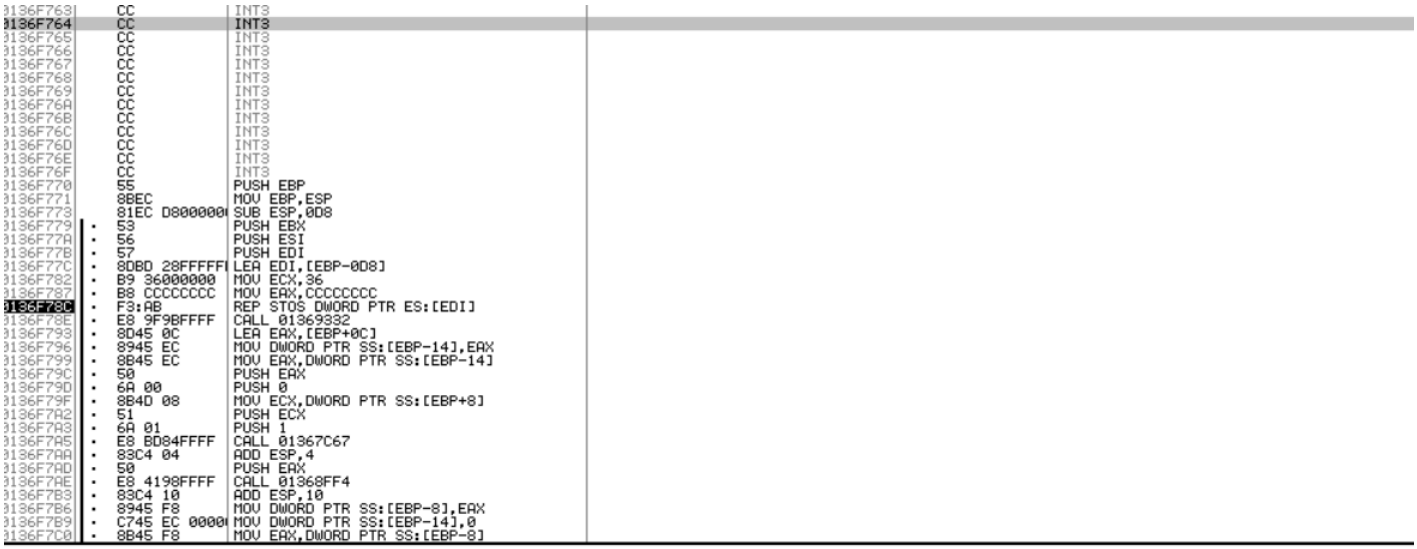
开始的界面是这样的，字符串这么多，查个串呗



这里查到input那里，设置断点

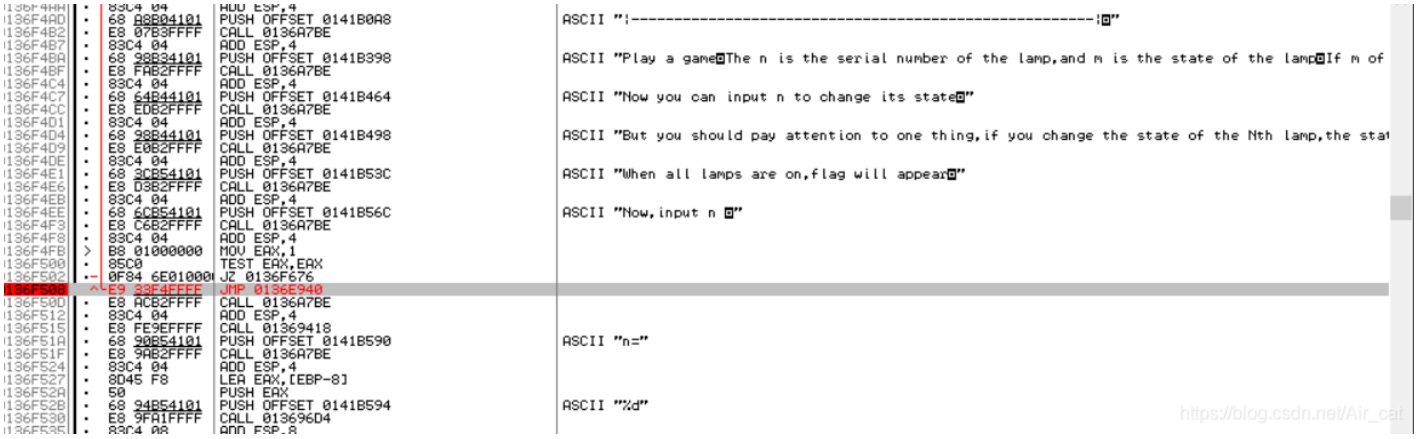


同时可以发现第一行出现了”done！！！the flag is“的字符串，跳进去



选择复制0136F779，呆会我们要跳进这个地方，需要注意的是有些题解说跳进done flag的那行，但具体操作起来可能会行不通，（大概是代码段的入口点？）个人水平实在有限暂时无法解答，先将这个疑问记下来。

后来稍稍查证了一下，该处确实为该代码段的入口



之后，让我们随便找一行代码改成跳转到刚才复制下来的地址，F8F8F8，完成。