之前的逆向（2）-bin 100 etctf

原创

Startr4ck 于 2018-04-28 06:58:51 发布 181 收藏
分类专栏： ctf 文章标签： 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/80115368
版权

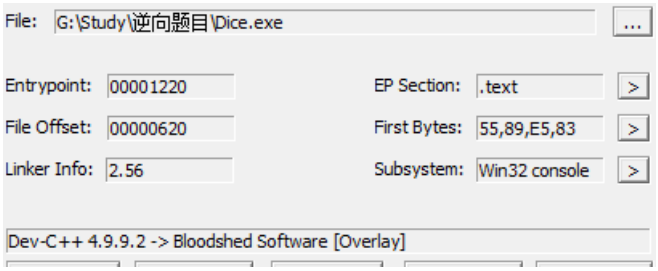
ctf 专栏收录该内容
17 篇文章 0 订阅
订阅专栏

利用 od 进行逆向

http://www.shiyanbar.com/ctf/1747

使用od 进行修改 程序的汇编代码 从而得到flag

首先使用peid 查看该编译代码的 语言



发现是 c艹 嗯 不会

使用 od 进行反编译

打开od 之后 搜索 文本 ， 找到判断的 汇编跳转指令

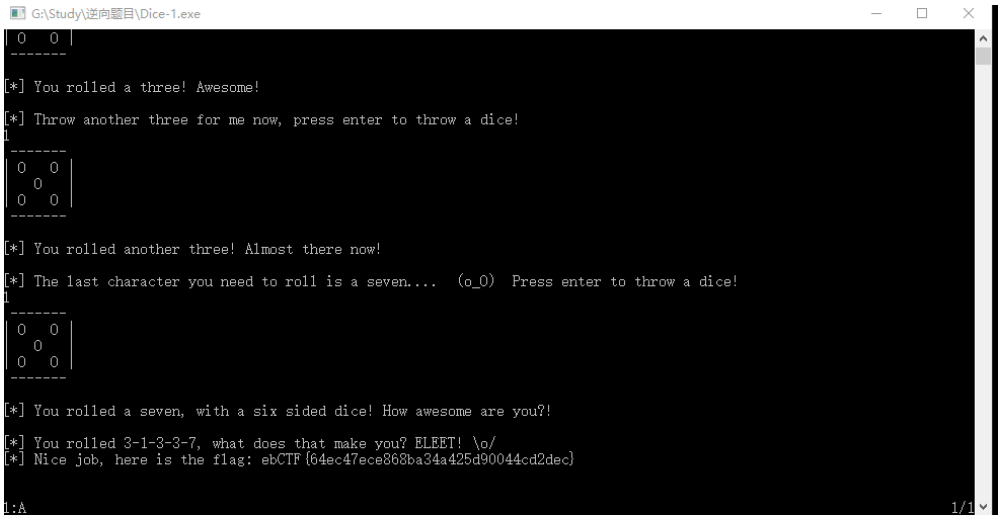
只要将 汇编跳转指令换成nop就是不执行 就可以不执行 判断 那一部分

所以 修改程序 至nop

所以无论你是否输入符合题目的要求你都会通过判断因为 程序并没有进行跳转

也就是没有进行判断

所以可以顺利得到flag



修改的时候 是 通过文本框 寻找到 跳转指令的！