**实验3 Game夺旗赛（CTF）**

1. **实验目的**
   1. 熟悉静态反汇编工具IDA Pro；
   2. 熟悉动态反汇编工具OllyDbg；
   3. 掌握对二进制代码内部逻辑关系的分析；
   4. 掌握对二进制代码的修改和保存。
2. **实验原理**
3. CTF

CTF是一种流行的信息安全竞赛形式，可意译为“夺旗赛”。其大致流程是，参赛团队之间通过进行攻防对抗、程序分析等形式，率先从主办方给出的比赛环境中得到一串具有一定格式的字符串或其他内容，并将其提交给主办方，从而夺得分数。

CTF竞赛模式具体分为以下三类：

一、解题模式（Jeopardy）

在解题模式CTF赛制中，参赛队伍可以通过互联网或者现场网络参与，这种模式的CTF竞赛与ACM编程竞赛、信息学奥赛比较类似，以解决网络安全技术挑战题目的分值和时间来排名，通常用于在线选拔赛。题目主要包含**逆向分析**、漏洞挖掘与利用、Web渗透、密码、取证、隐写、安全编程等类别。

二、攻防模式（Attack-Defense）

在攻防模式CTF赛制中，参赛队伍在网络空间互相进行攻击和防守，挖掘网络服务漏洞并攻击对手服务来得分，修补自身服务漏洞进行防御来避免丢分。

三、混合模式（Mix）

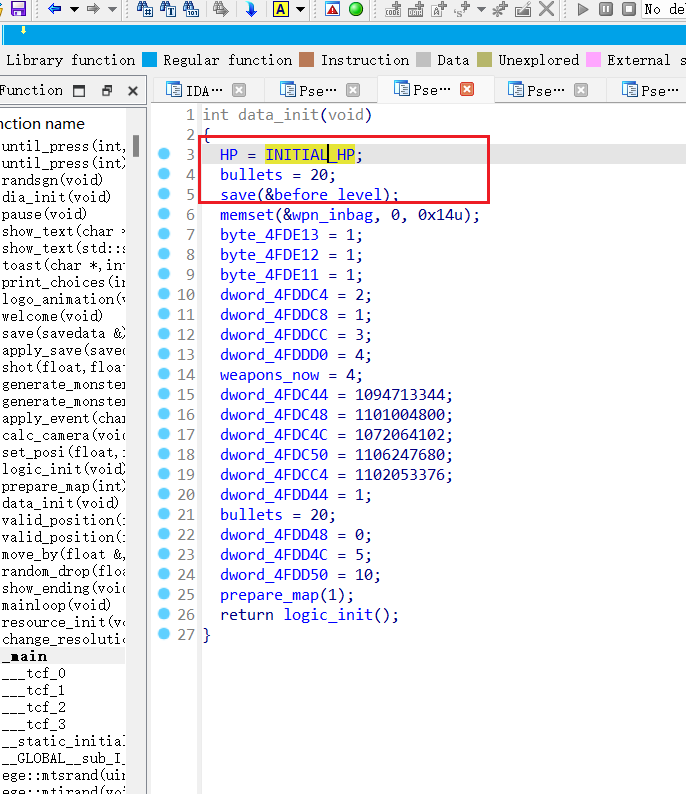
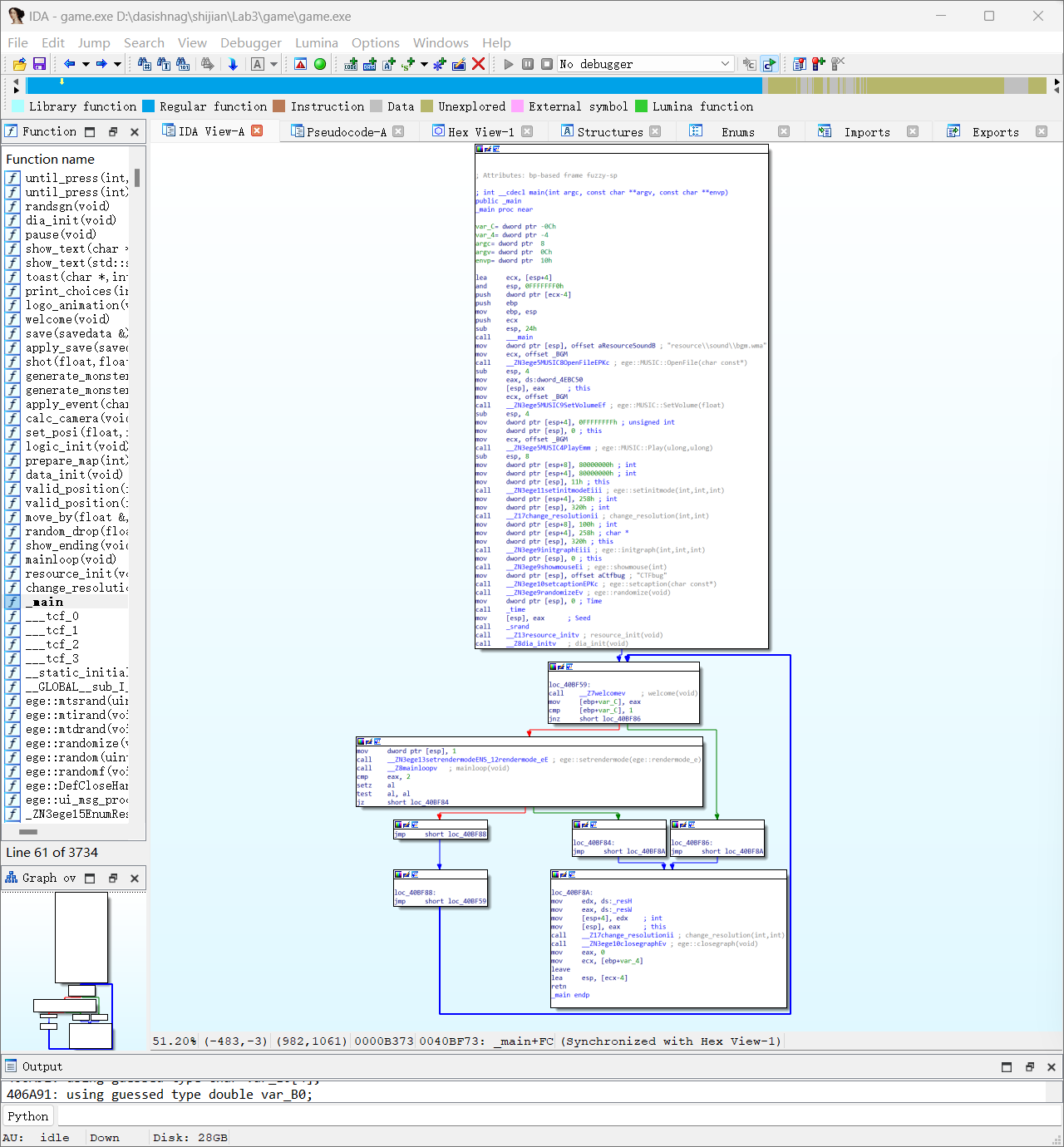
结合了解题模式与攻防模式的CTF[赛制](https://baike.baidu.com/item/%E8%B5%9B%E5%88%B6)，比如参赛队伍通过解题可以获取一些初始分数，然后通过攻防对抗进行得分增减的零和游戏，最终以得分高低分出胜负。

1. 解题

Flag隐藏在game.exe的二进制代码中。通过对game.exe的修改，使game.exe能够顺利的执行，完成对Flage的解密。

1. **实验报告**
2. 逆向分析game.exe二进制代码的主要逻辑结构和重要数据。
3. 修改game.exe二进制代码，获得最后的Flag。实验报告要说明逆向分析、代码修改的具体过程，以及最后获得的Flag。
4. **主要逻辑**

从main进入，然后会init\_data，这里处理了一些角色的属性，地图等，然后welcome，是最初看到的界面。

****

重点应该关注mainloop函数，这里发现了KEY：：，分四次写key，最后FINAL\_DECRYPT解出，所以我刚开始尝试将if（\_\_END\_\_）的jz改为jnz直接实现最终的解题是不行。

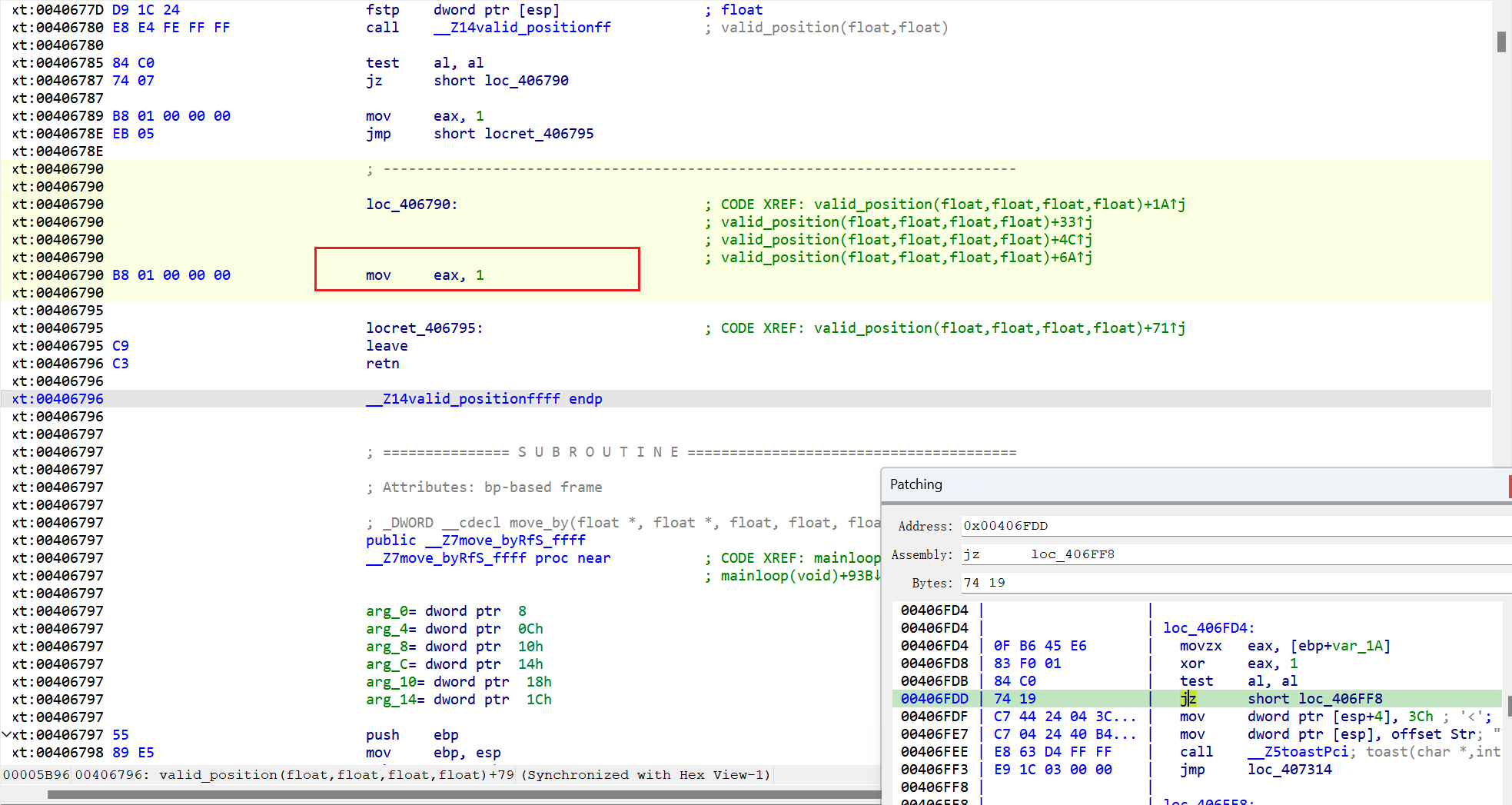
**遇到问题：**

刚开始直接运行所给的game.exe时总是在第二个界面卡住，



于是尝试其他低版本的系统，发现并不是这个原因。

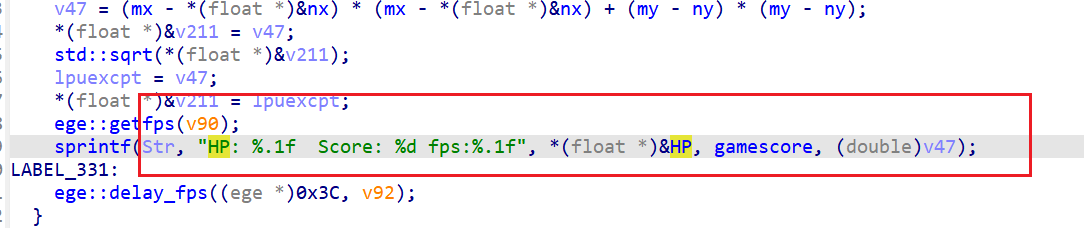
最终，对源代码再次进行仔细分析，定位到mainloop中的valid\_position函数，当其返回一时才行。于是进行如下修改。



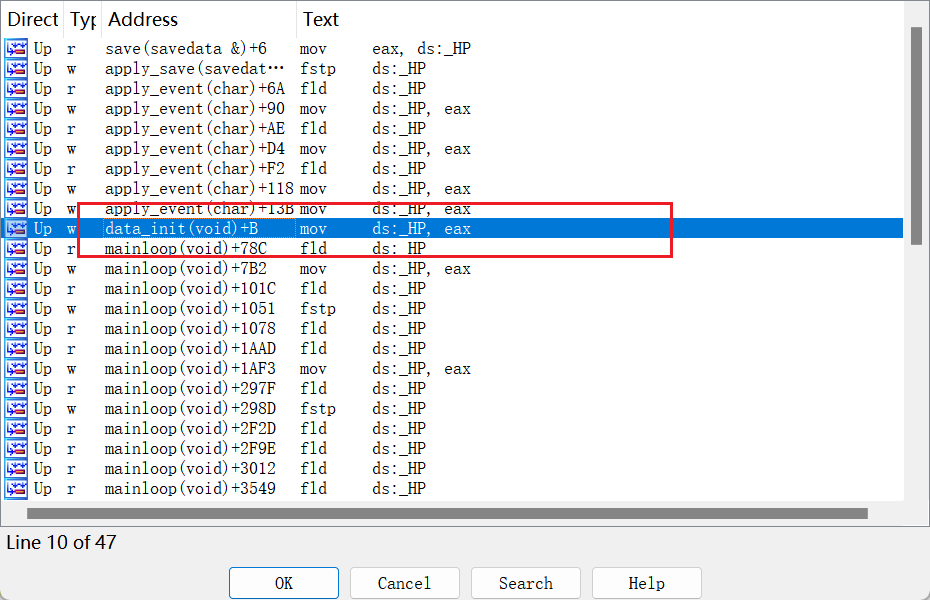
修改默认返回值为1。成功解决问题。

解题步骤：

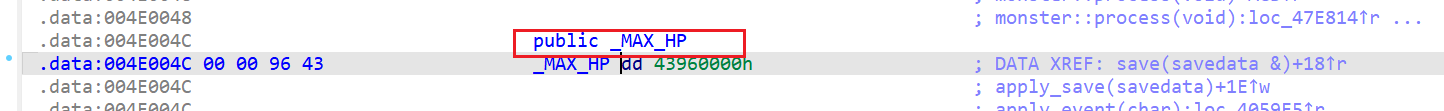
找到mainloop中有关HP的部分

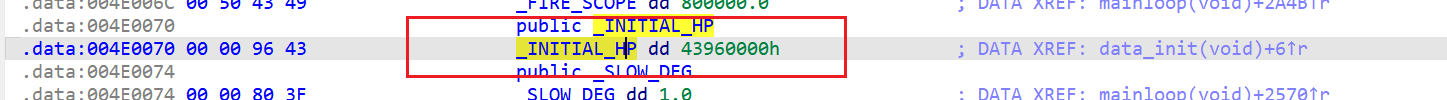


查看在哪里会修改HP，data\_init先去看看



最终定位到MAX\_HP，和INITIAL\_HP，一看数值正好是300

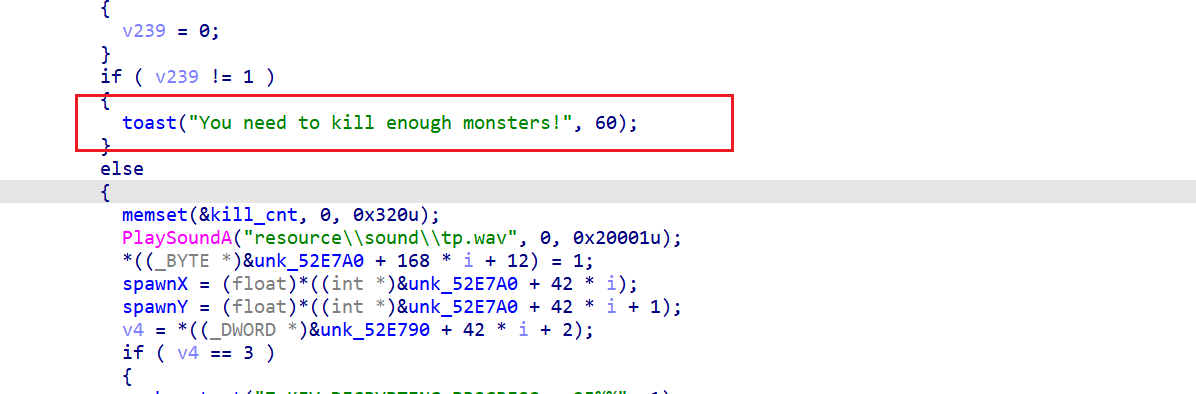




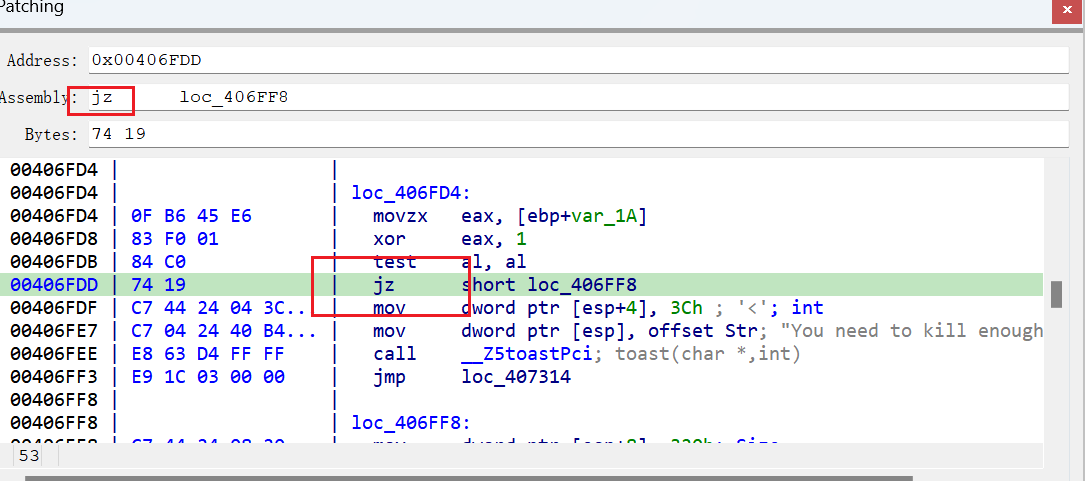


直接修改数值F8 02 15 50，小端序float9999999999

结果发现好像得打怪，查看代码，



修改if



直接把jz改成jmp，直接跳转。

最后在地图里走几圈就行了



最终结果。