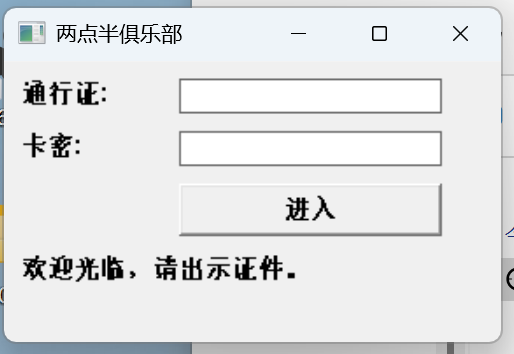
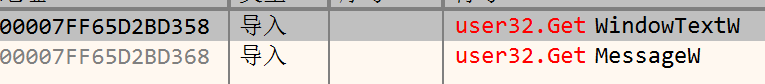
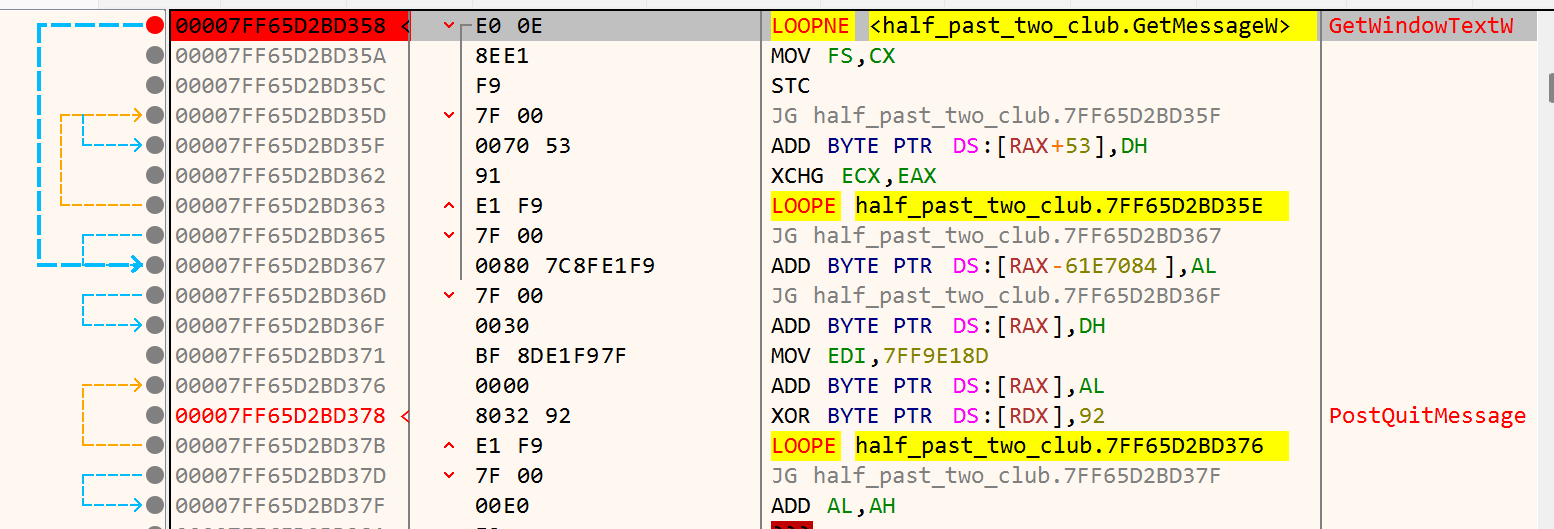
首先打开程序，发现是对话框程序，因此使用x64dbg调试



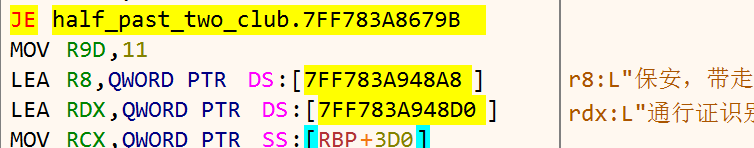
在调试中找到弹出对话框的地址处



在此处下断点



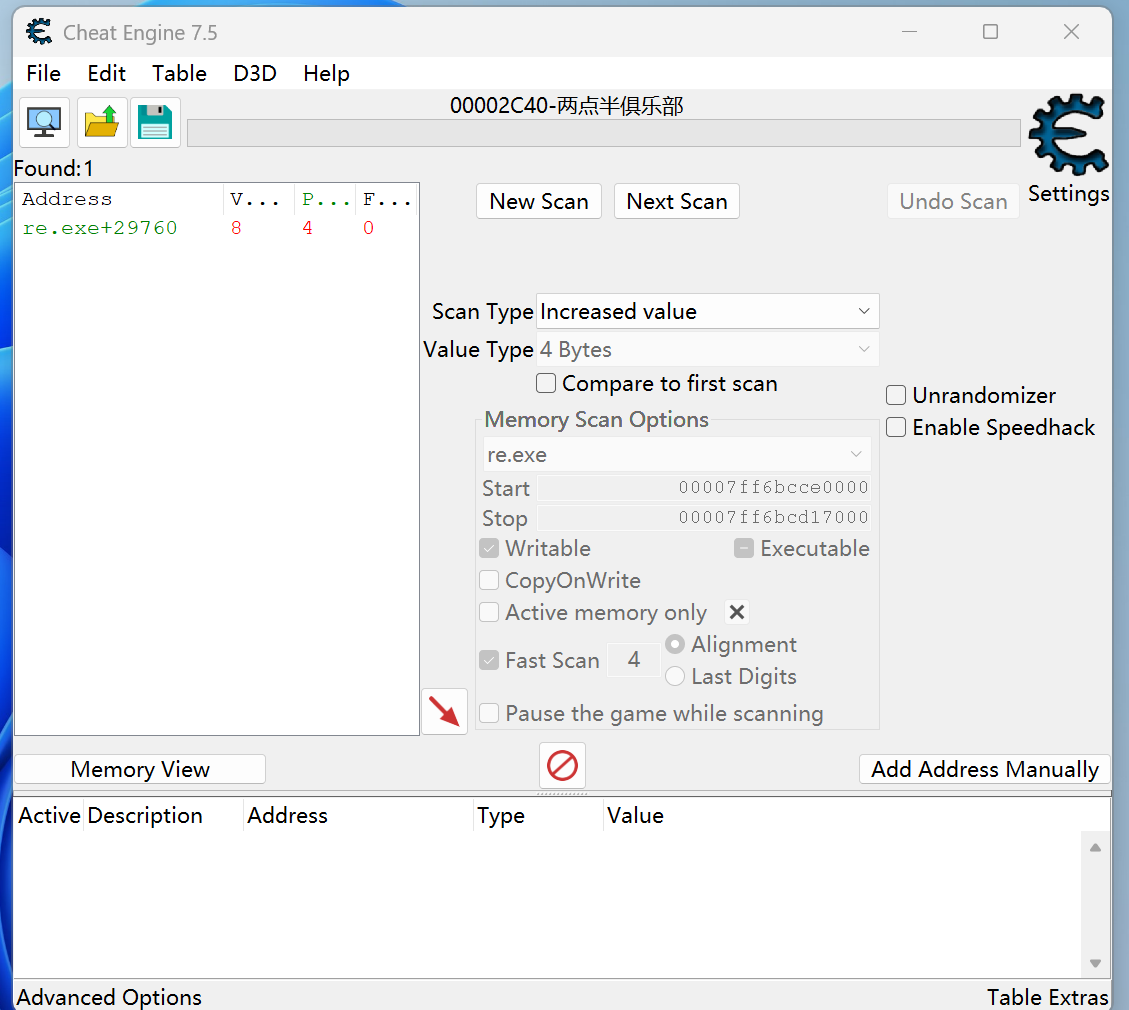
将此处和后面的关键条JE汇编码改为JNE，后修补文件



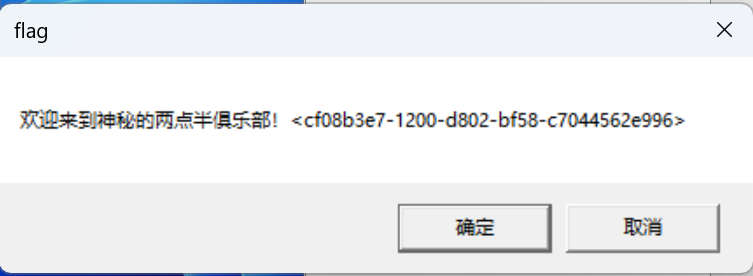
成功进入程序



之后使用cheat engine监控按下按钮后程序的行为



找到每次按下按钮后增加的进程，改为最大值，查看程序反应



更改值后得到的弹窗得到flag