## OD破解入门教程

1. 编写一个MFC应用程序，其中有一个按钮，运行后界面如图：



1. 在初始化函数OnInitDialog()里面添加简单的几句话，以用来进行破解，初始化逻辑很简单，就是让按钮处于不可点击的状态，同时按钮显示的文字改变。

int flag = 10;

flag = 10 + flag;

flag -= 10;

if (flag == 10)

{

this->m\_btn\_creack.EnableWindow(FALSE);

this->m\_btn\_creack.SetWindowText(\_T("未经授权的，禁止使用"));

}

else

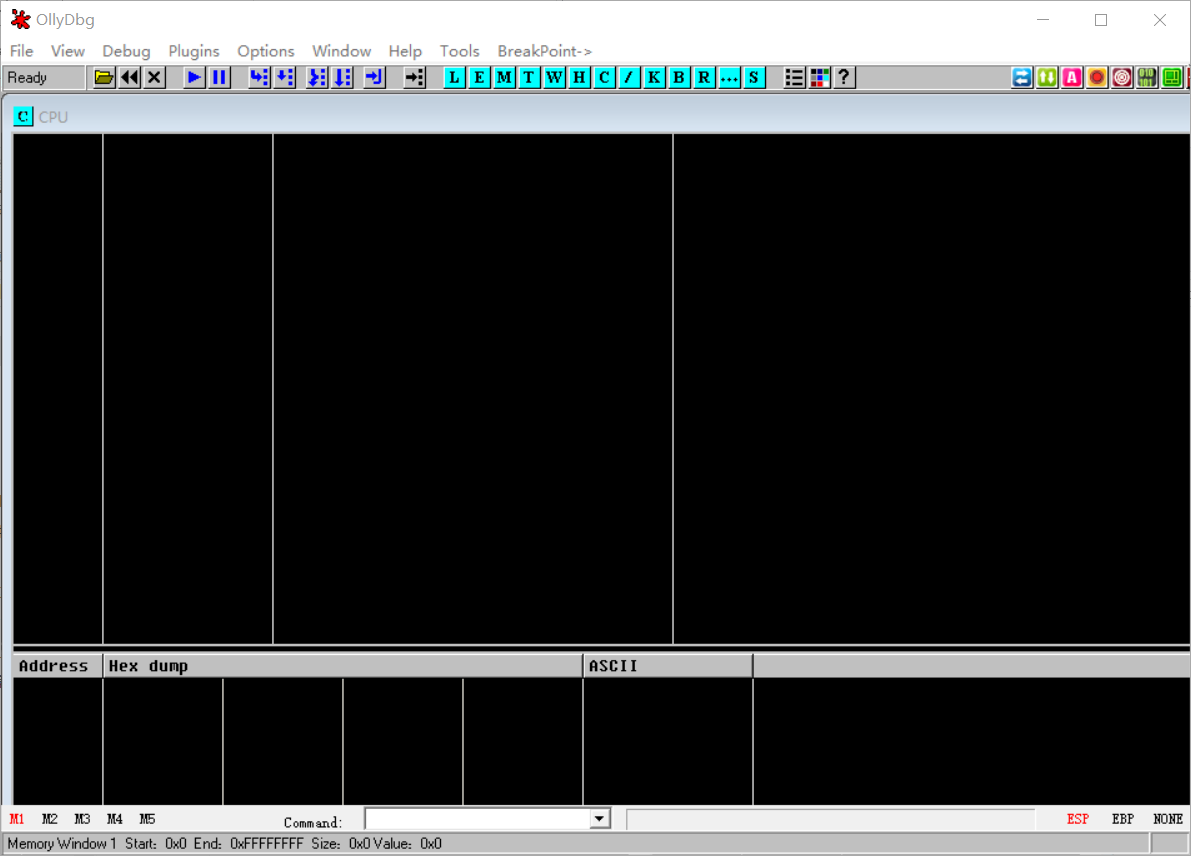
{

this->m\_btn\_creack.EnableWindow(TRUE);

this->m\_btn\_creack.SetWindowText(\_T("已授权，请使用"));

}

1. 打开OllyDbg动态调试程序

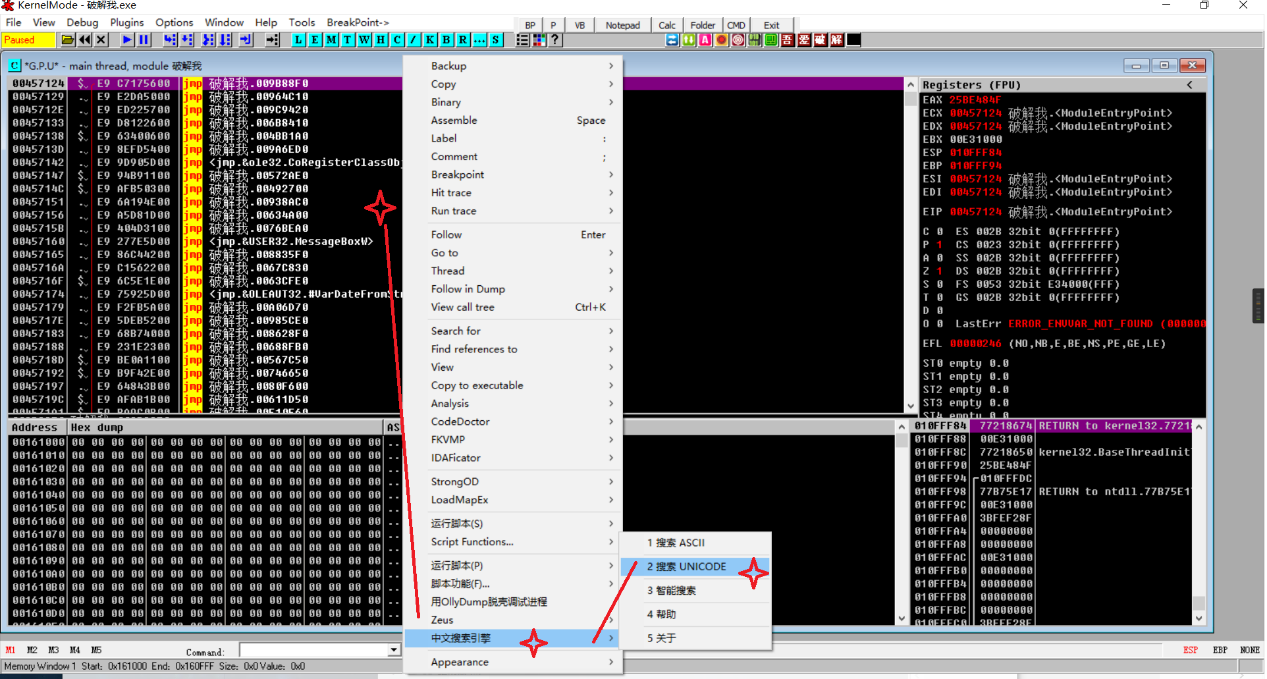


1. 加载目标程序：File-Open-选中测试测序（或者在此页面直接拖入测试程序）
2. 在汇编窗口右键-选择中文搜索引擎-选择搜索Unicode

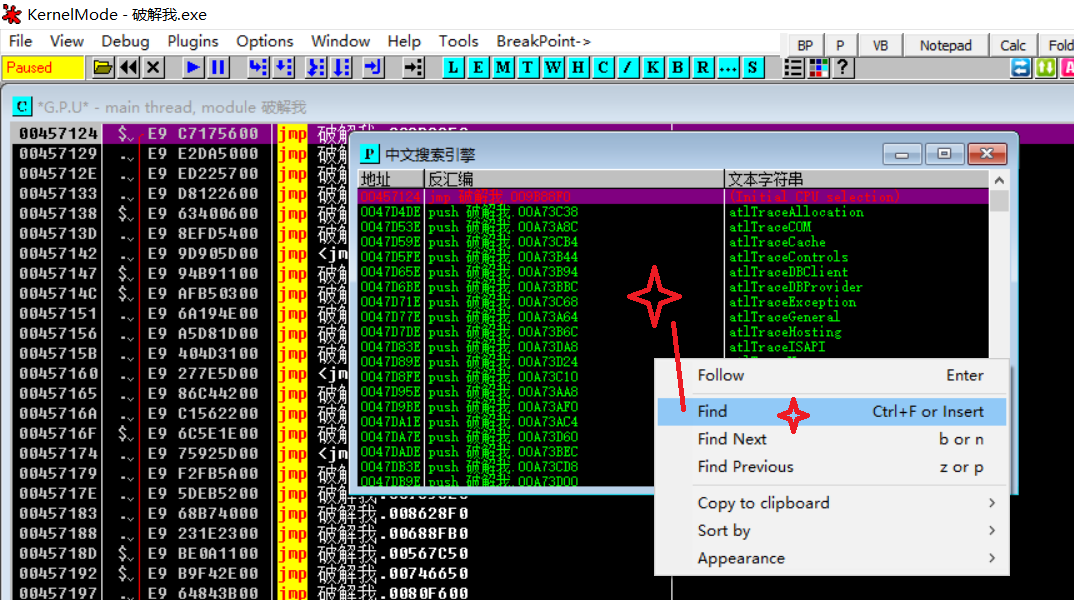
破解思路：

对于这样的验证授权的软件，一般来说都是有一个判断语句，在C语言里面是IF语句，对应在汇编里面就是条件跳转语句，因此，只要能够找到和这个判断相关的代码，去找最近的一个条件跳转语句，检查相关的标志寄存器的值，那么就可以实现破解。

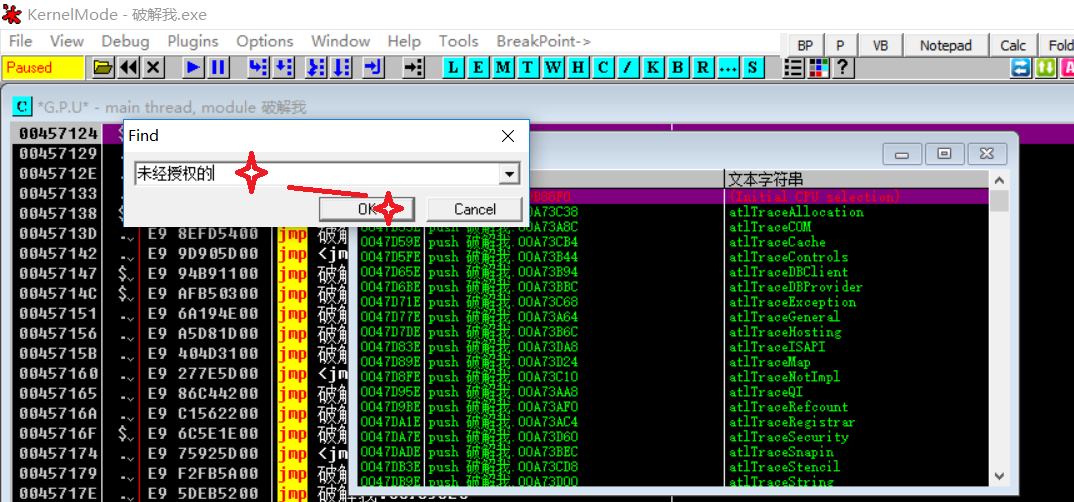
当然，这里更简单了，我们已经知道了实现的代码，非常的简单，就是一个if-else语句。判断语句里面写了更新是否授权的字符串更改代码，存在字符串常量，那么，就直接搜索这个字符串。



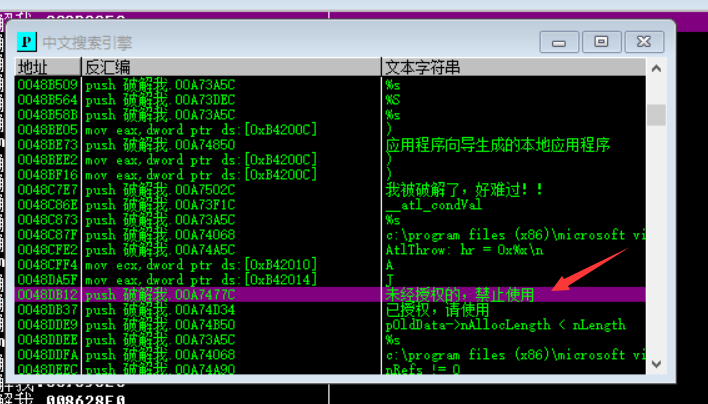
1. 在弹出的窗口中右键-find



1. 在弹出的输入框-输入要找的关键字-确认

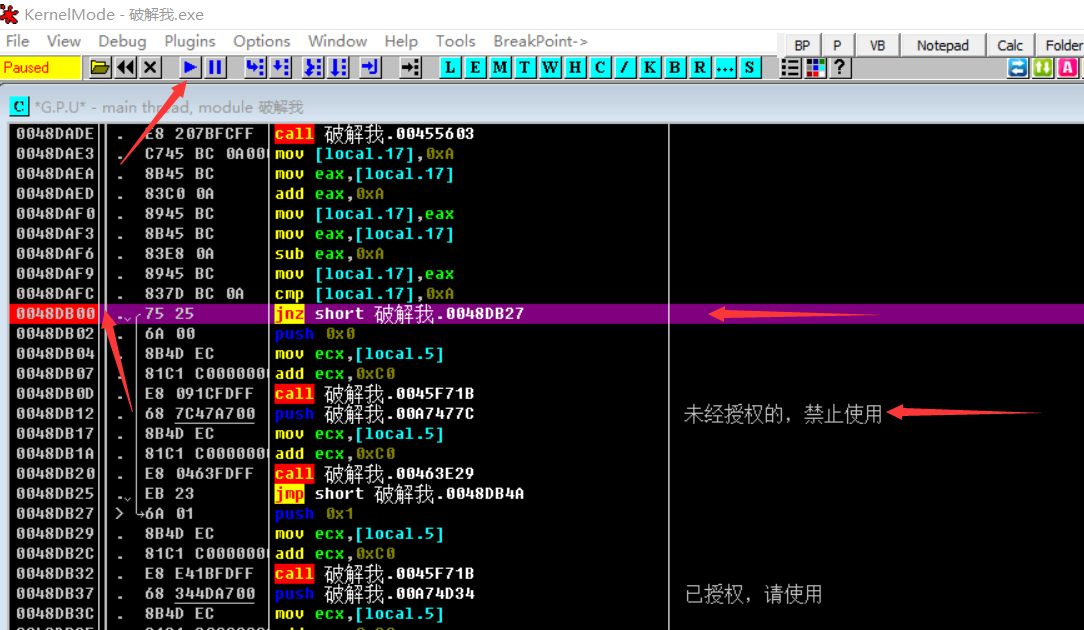


1. 已经查找到结果了，同时连提示授权成功的字符串也找到了，双击此行

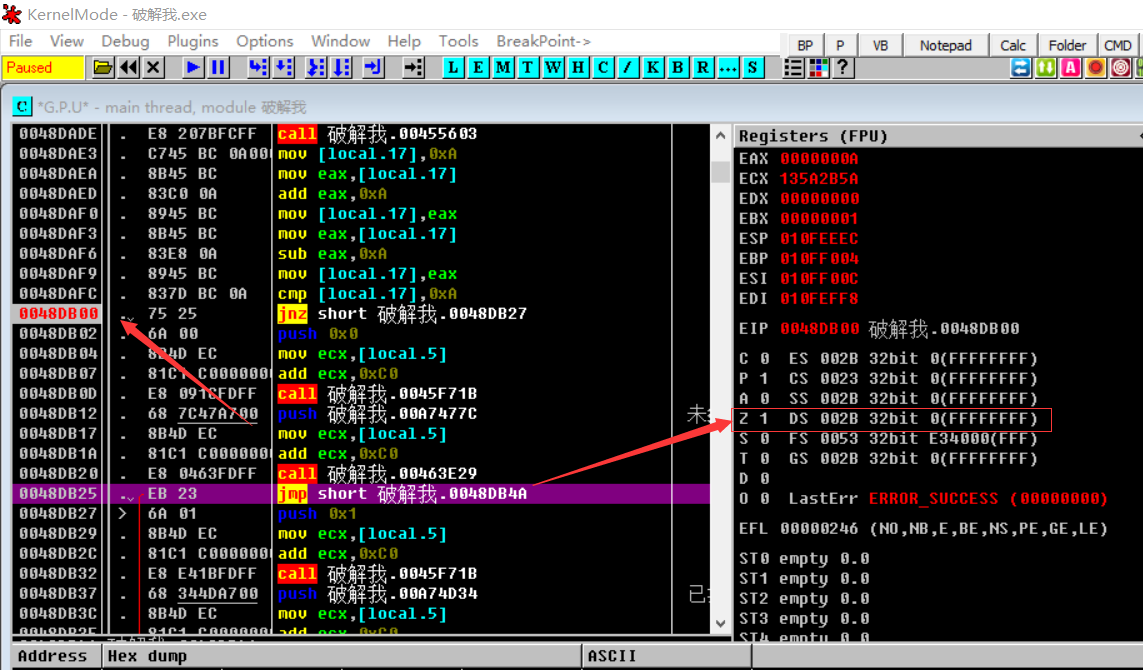


1. 汇编窗口自动跳转到此行提示的位置，网上找到第一个条件跳转语句JNZ，在此行双击，看到左边变成红色，这就下了一个断点，然后点击上方工具栏的运行按钮，程序便会运行到此断点

找到授权修改字符串相应的代码之后，往前找第一个条件跳转语句，找到了一个JNZ，标识不相等时（标志寄存器ZF=0时）发生跳转（本意是不等于0时发生跳转，由于比较相等的实现实际上是一个减法），因此只要在程序执行到此处的时候能够中断一下，手动修改一下标志寄存器的值即可完成授权破解。



1. 此时，断点处的地址变成灰色，右边的标志寄存器ZF的值为1，当JNZ发生跳转时，ZF的值需要为0，因此原本不会发生跳转，也就是原本会禁用按钮，现在双击右侧的Z行的1，让1变成0，然后再次点击运行



1. 现在，就可以看到原本未授权的程序，已经授权了，可以使用了。

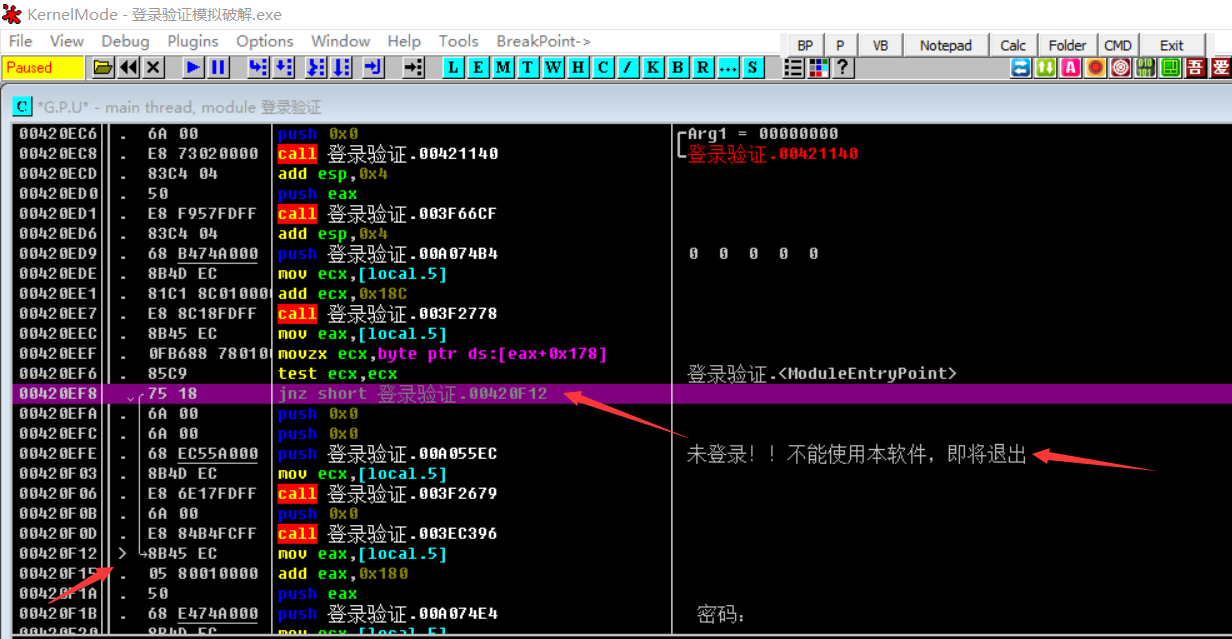


1. 这种直接手动修改标志位的破解方式称为暴力破解，也有其他的方式，比如将条件跳转语句修改为无条件跳转JMP语句，修改影响标志位的指令方式等。

现在已经会了基本的破解，去试试另一个登录模拟程序的破解吧。

首先运行程序之后发现有一个登陆框，登陆了之后才能使用，不登陆就会提示“未登录”的提示后程序就关闭了。

那么根据前面的经验，同样去查找字符串和对应代码之前的跳转语句，如下图：

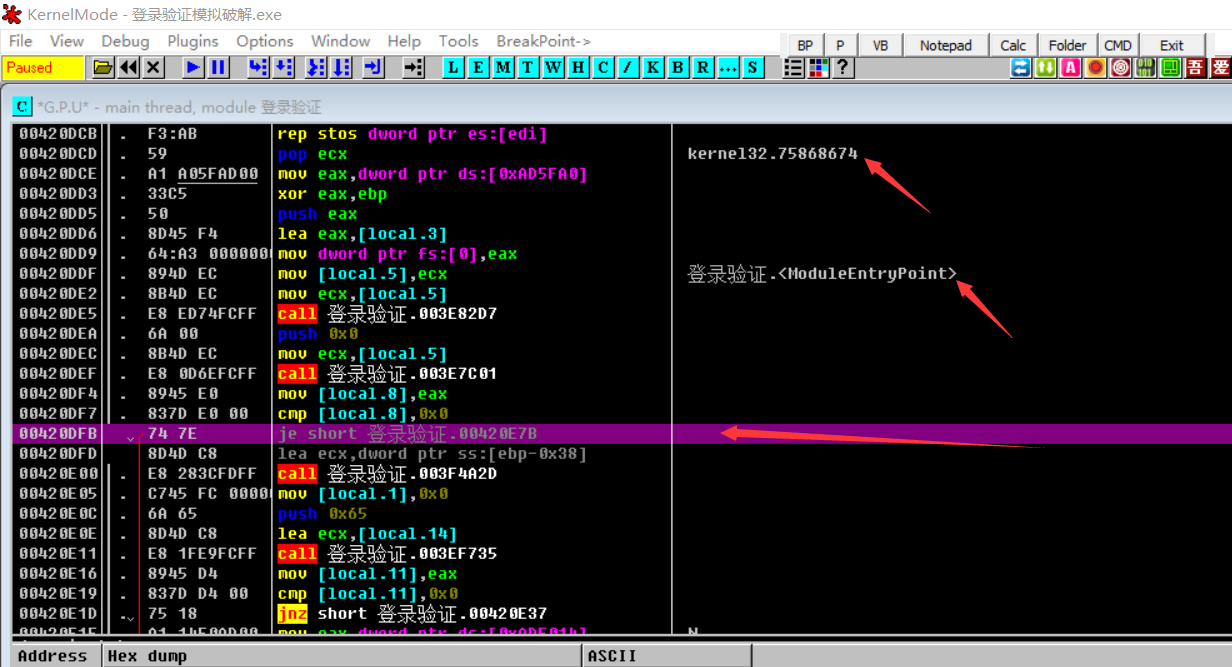


同样是jnz，同样是修改ZF标志位即可，事实也确实就是这样，成功的不用输入用户名密码直接登录就进入了主页面。

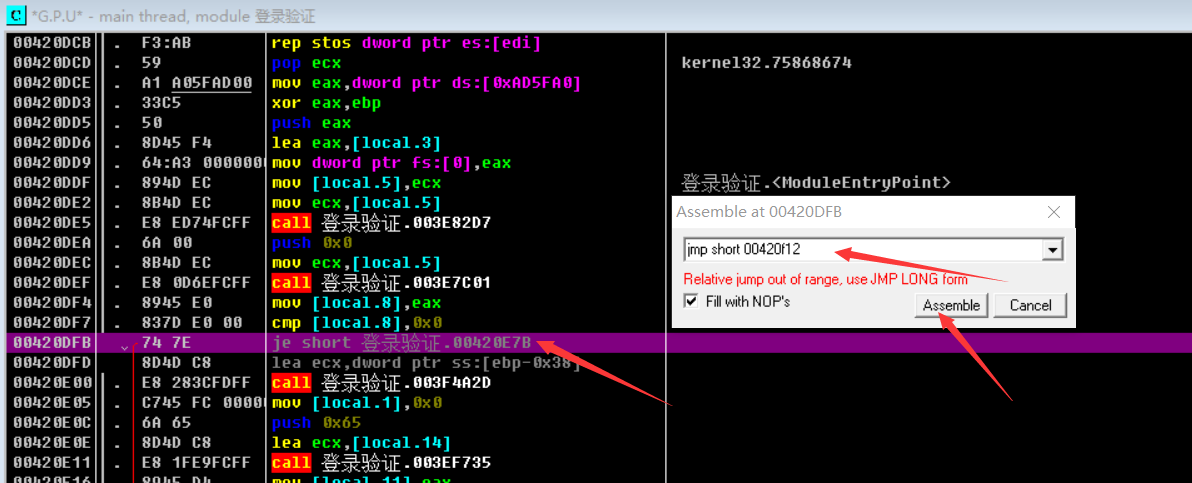
这里不演示这种方法了，对于这种登录对话框来说，一般的原理都是：

在主功能窗口的初始化快结束的时候，跳转到登录对话框进行验证登录，登录成功之后初始化完毕，正常使用，登录失败，直接退出程序。

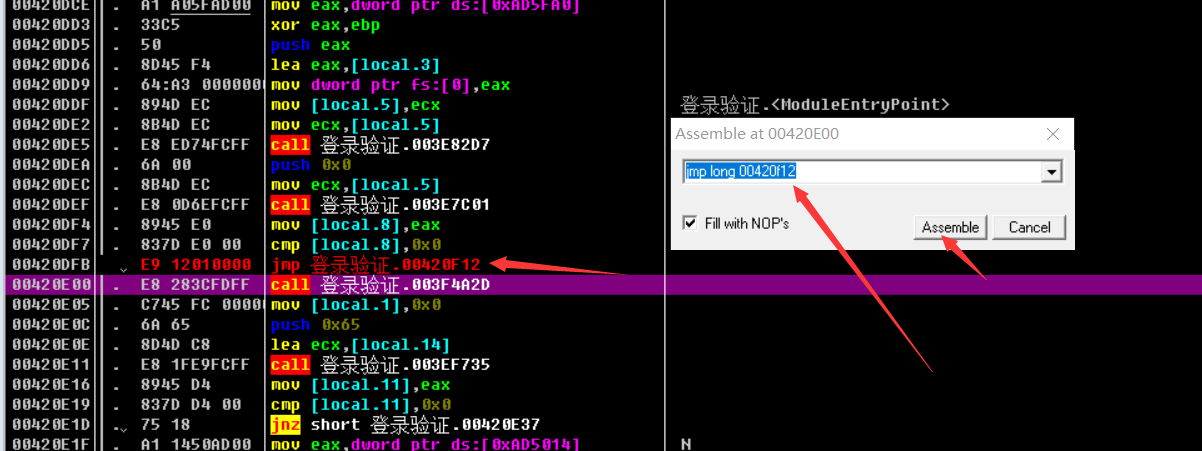
那么我们就可以让它直接跳转到初始化结束的位置，直接跳过登录对话框，可不可以呢？当然是可以的。注意到上图中的跳转的目标地址“jnz short 00420f12”,也就是说，进入主页面的地址在00420f12,那么只需要在进入登录对话框之前，跳转到这里即可，可以想到“jmp short 00420f12”,那我们往前找一下哪里合适，优先考录有跳转语句的地方。找到如下位置：



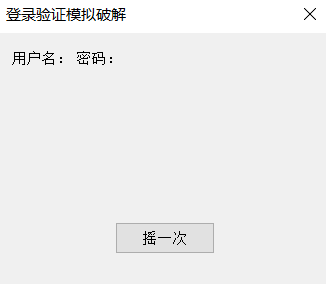
可以看到，此跳转之前，是一个模块的入口点和内核调用，那就应该大体在这个位置，试一下修改，在这句的汇编代码上双击，把弹出的编辑框代码改为“jmp short 00420f12”



嗯，输入完毕点击汇编按钮的时候，出错了，为什么呢？因为目标地址离这个地址太远了，short方式跳转不了，需要用long方式，那我们改一下，重新点击汇编按钮。



可以看到，修改成功了，那我们关闭这个输入框，运行程序试一下。



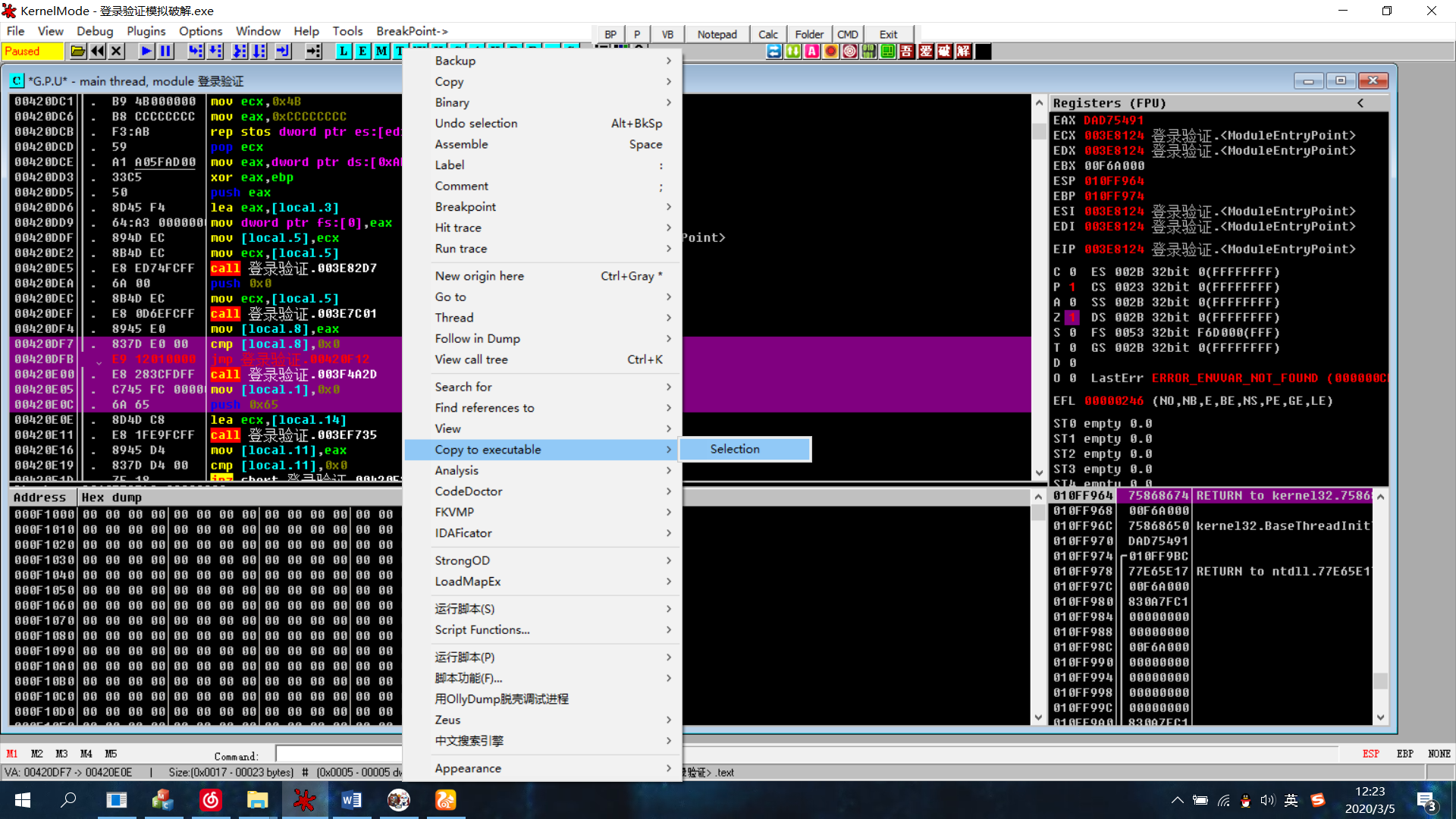
成功了，没有弹出登录窗口，只是里面的一些初始化内容丢失了，那点击按钮运行一下，看下是否正常。

运行正常，那就破解完毕了，当然如果还需要哪些初始化语句，那就去更精确的找一下位置，对应修改即可。

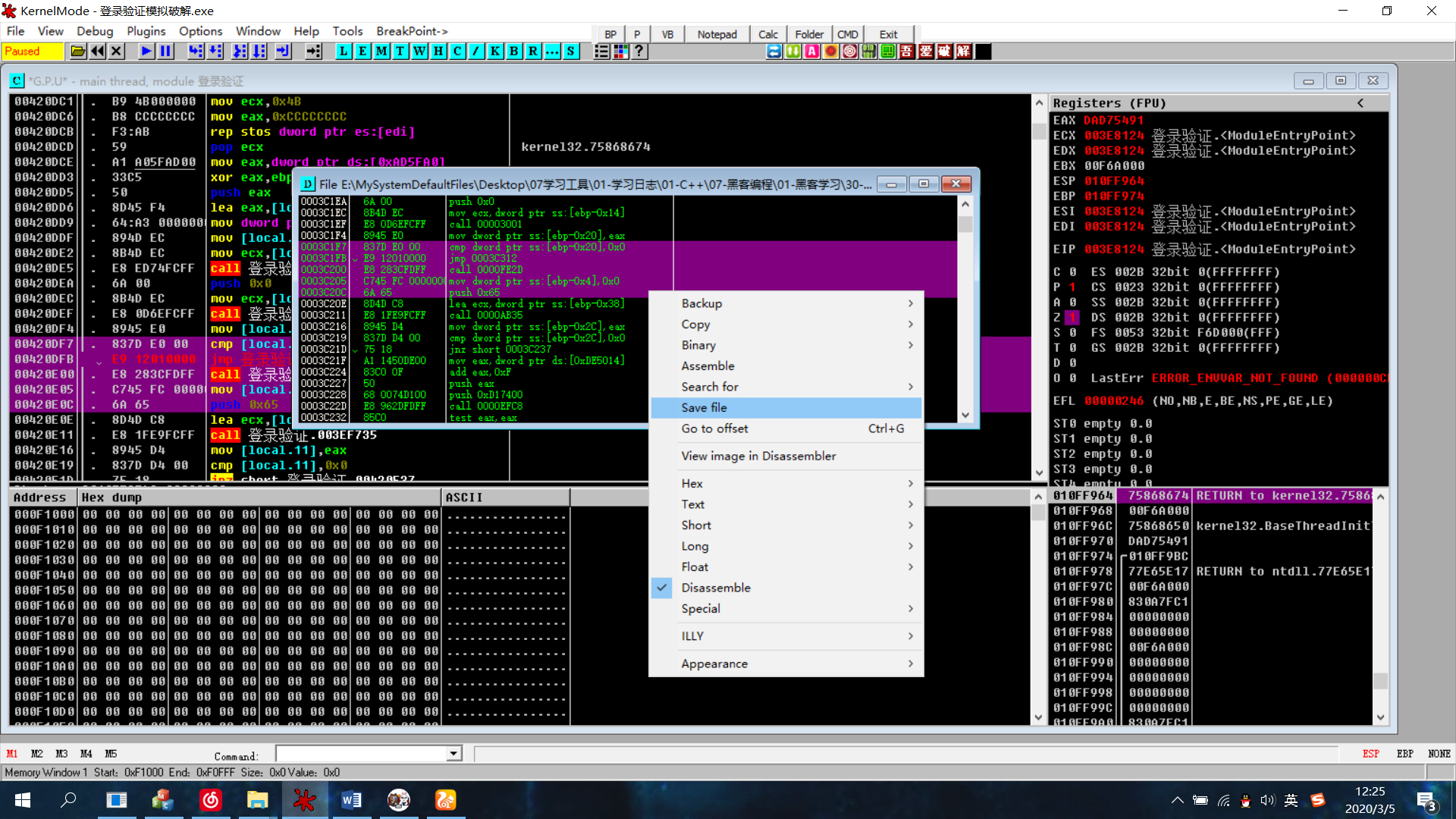
那么问题来了，修改完了，在OD里面是破解了，但是，为什么去运行程序，还是未破解呢？

原因很简单，没有进行保存破解，怎么保存呢？如下图

选中修改了的汇编代码，右键，拷贝到可执行文件，选择



在弹出的代码选框中，可以看到刚才选中的代码，右键，保存到文件



在弹出的文件选框中，输入要保存的名字，点击保存即可

