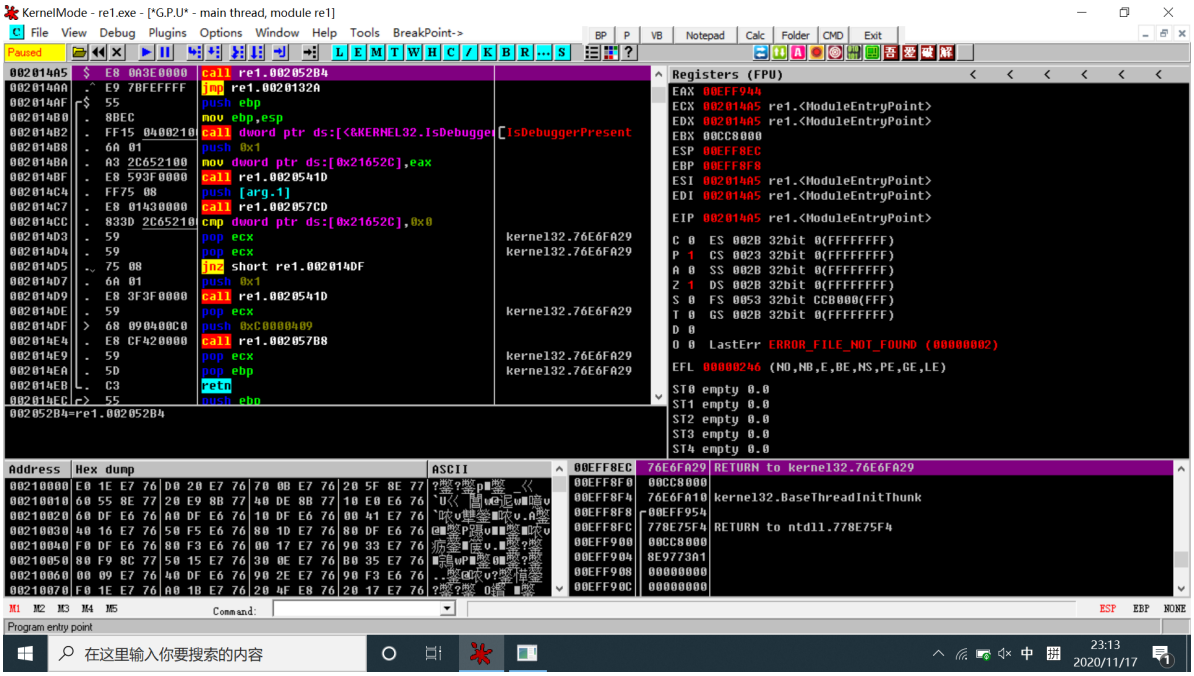
# Bugku：Easy_Re

## 第一步：下载程序，并用OllyDbg打开



## 第二步：搜索字符串

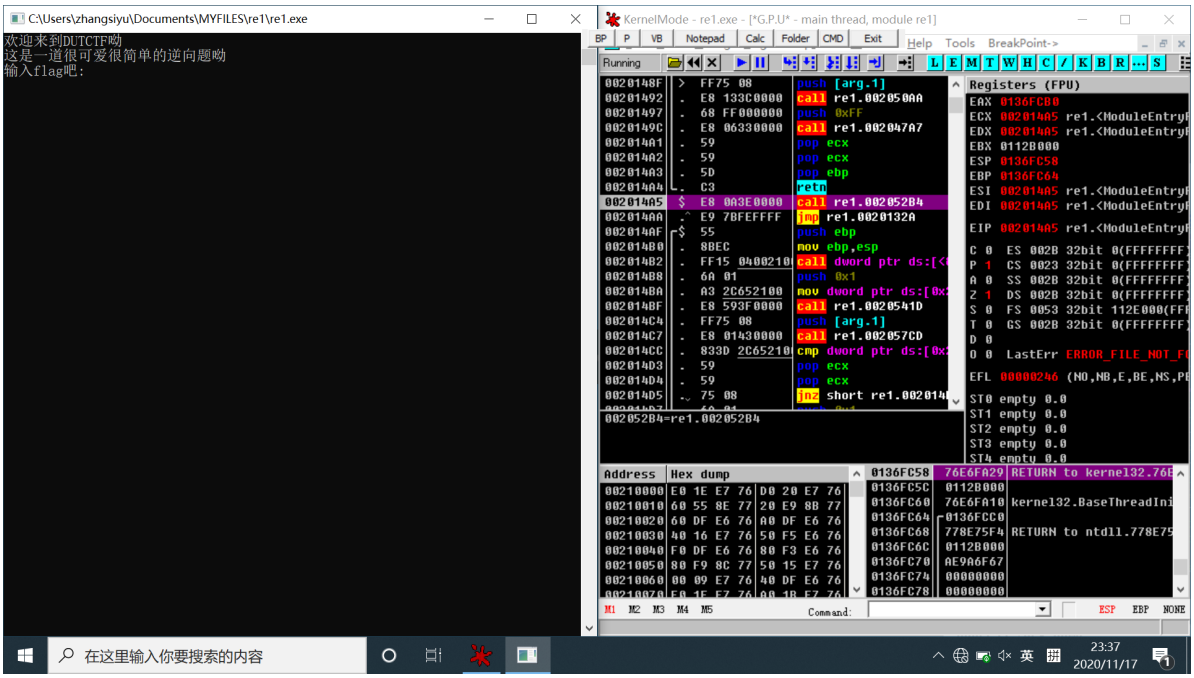
右键点击 **Search for -> All referenced text strings**，找到ASCII "flag get√\n"一行，双击。
可以看到如下代码

```
0020108F    . / 75 07         jnz short re1.00201098
00201091    .|  68 903E2100   push re1.00213E90              ;  ASCII "flag
get√\n"
00201096    .|  EB 05         jmp short re1.0020109D
00201098    > \ 68 9C3E2100   push re1.00213E9C              ;  ASCII "flag不太对
呦，再试试呗，加油呦\n"
```

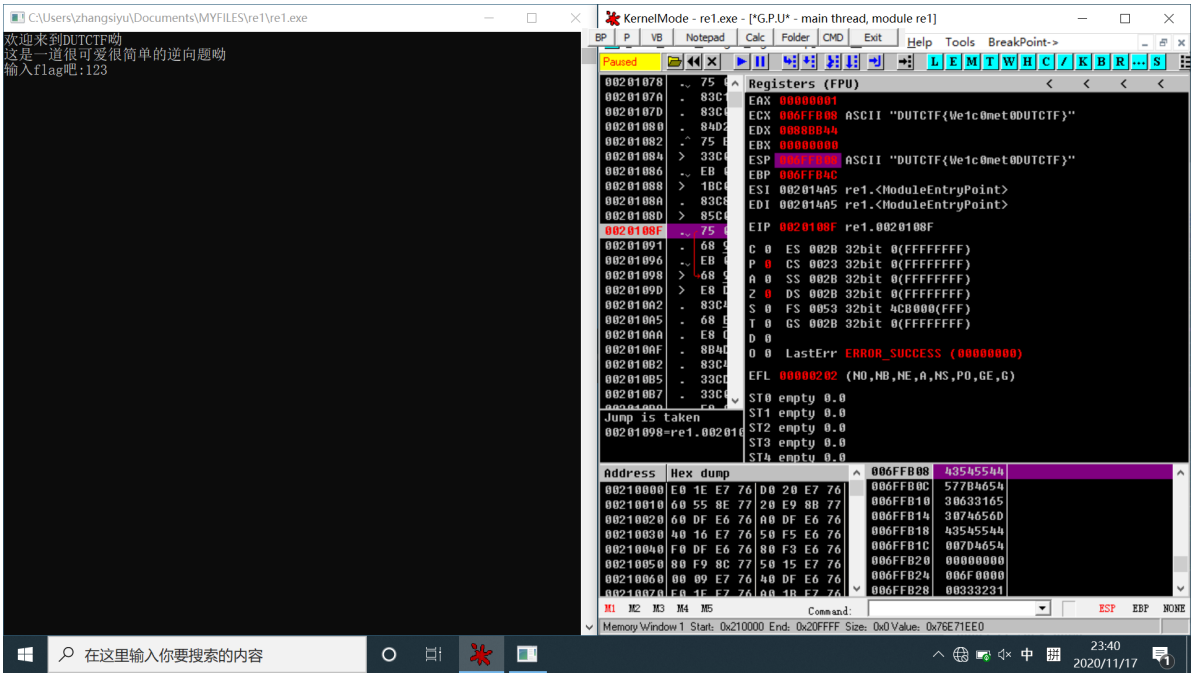
其中的`jnz`指令是判断是否不为零，为真则跳转到地址`00201098`，也就是执行指令`push re1.00213E9C`。

## 第三步：设置断点、运行程序

在 `jnz short re1.00201098` 处设置断点（F2），然后运行程序。




按（F9）运行程序，输入一个任意字符串，程序会在断点处暂停，同时查看寄存器的ESP行。




DUTCTF{We1c0met0DUTCTF} 即为flag。