# 《软件安全技术》综合实验

## 实验四：破解注册登录功能

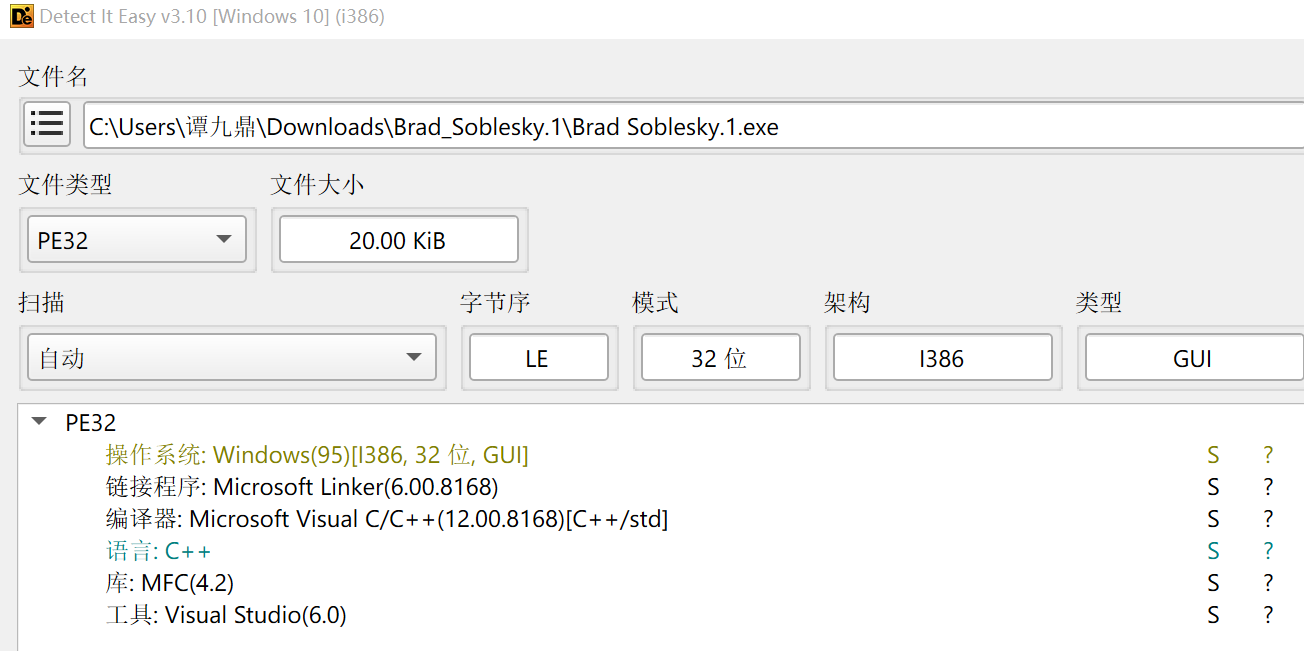
## 作者：谭九鼎

## 学号：522024320137

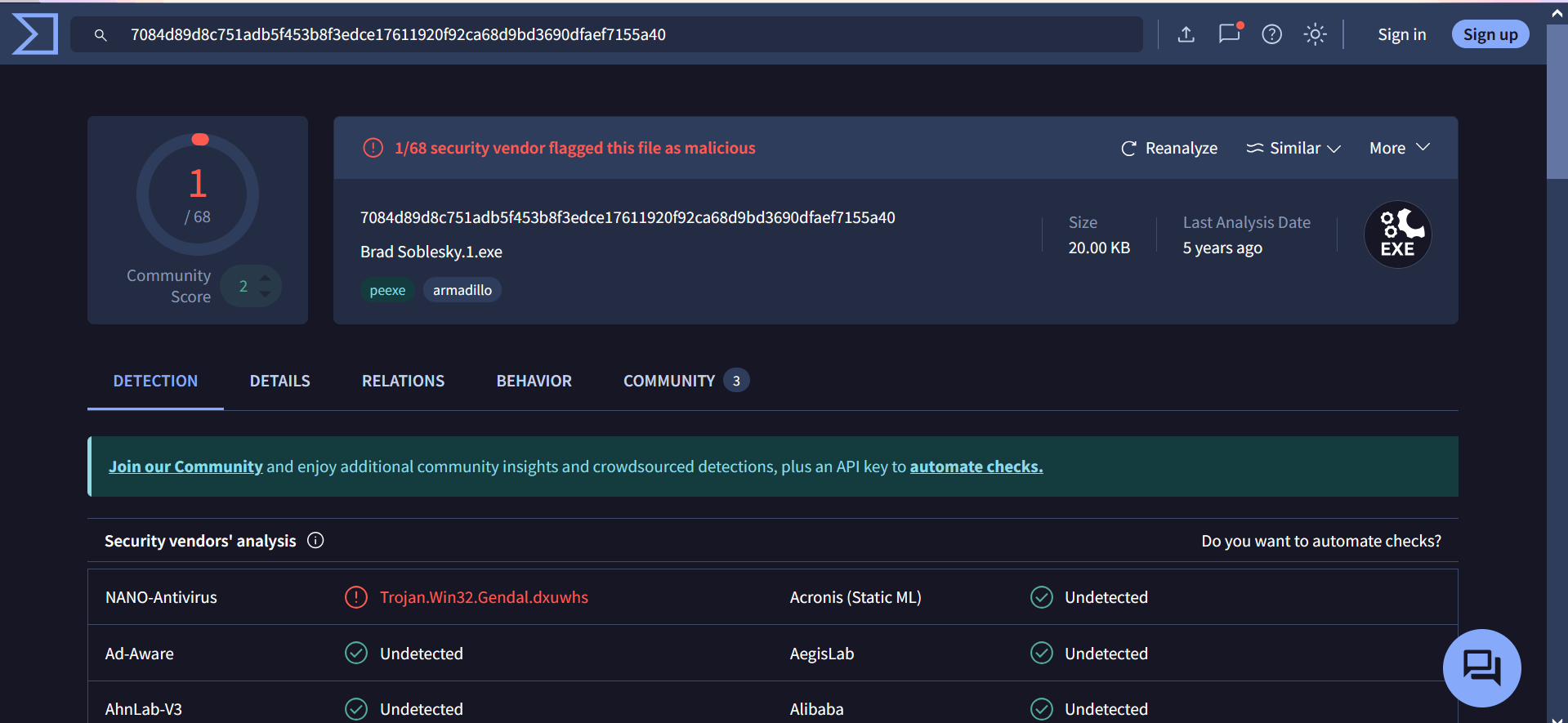
## 时间：2024年12月

选择18号Brad Soblesky.1.exe，一星难度，序列号。

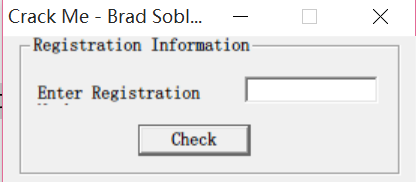
使用Detect-It-Easy检查语言：



使用VirusTotal多引擎在线查毒工具扫描病毒：



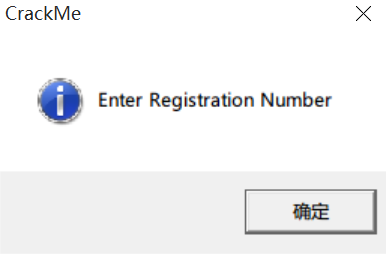
运行程序：



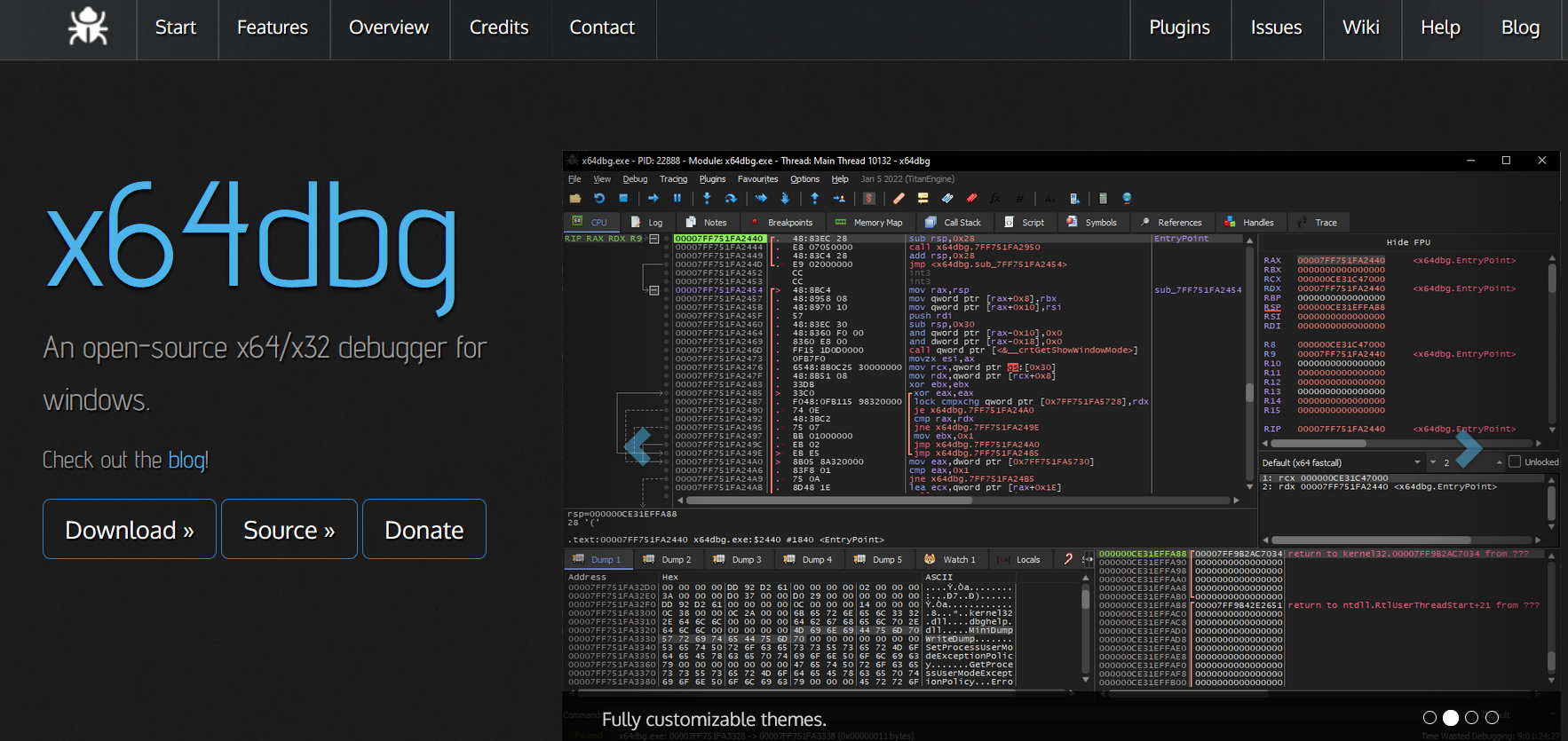
乱输效果:



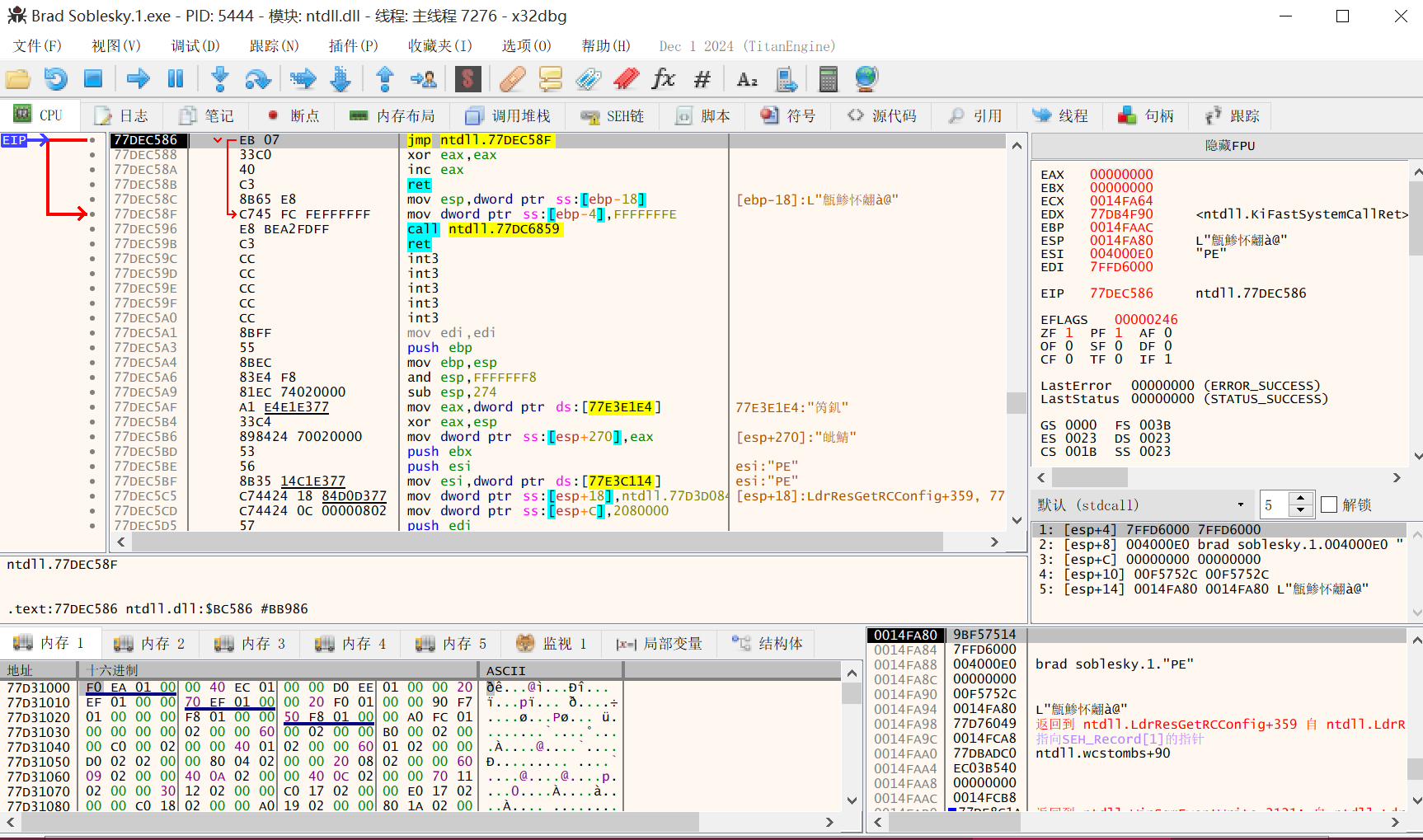
不输留空，直接提交，结果：



下载开源反汇编工具x64dbg：



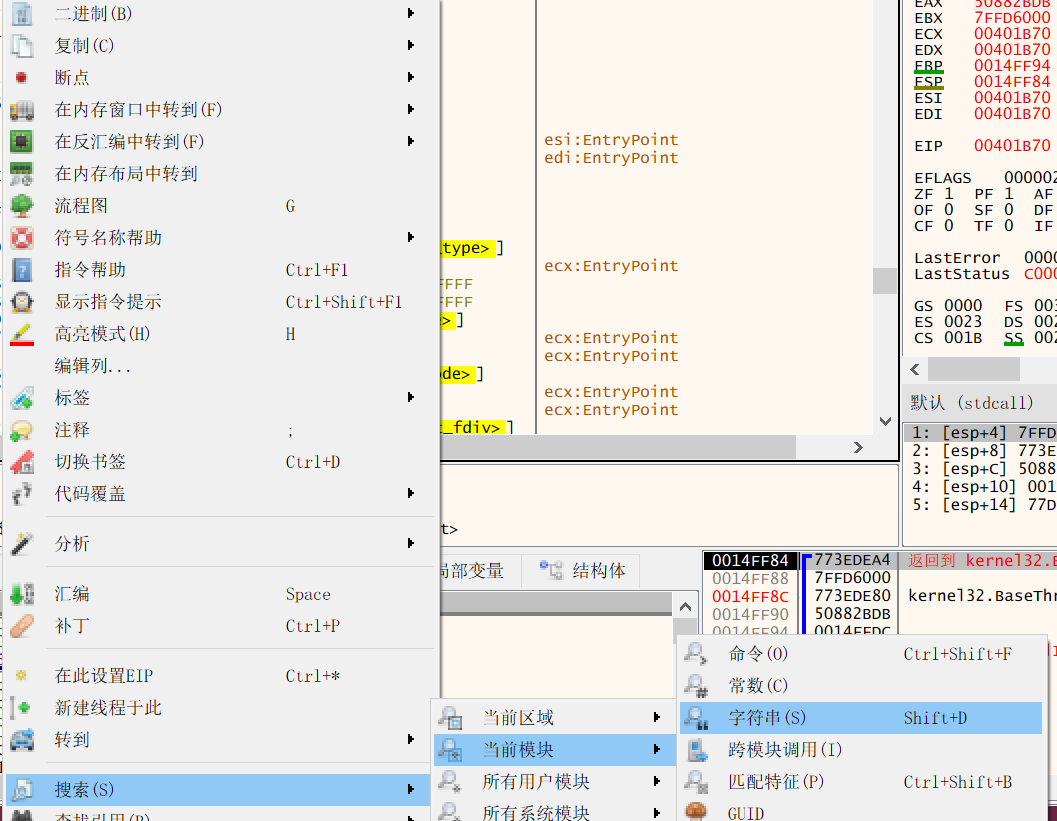
运行并载入程序：



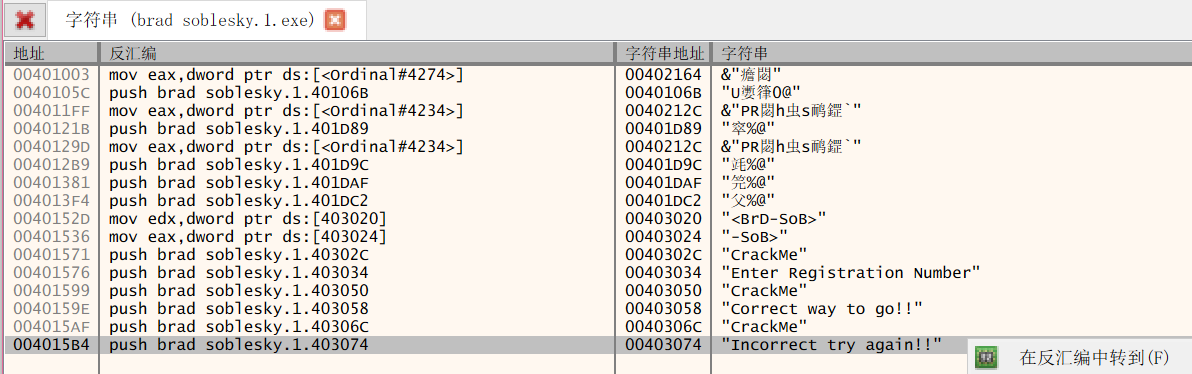
按一下F9运行到用户（即目标）模块：

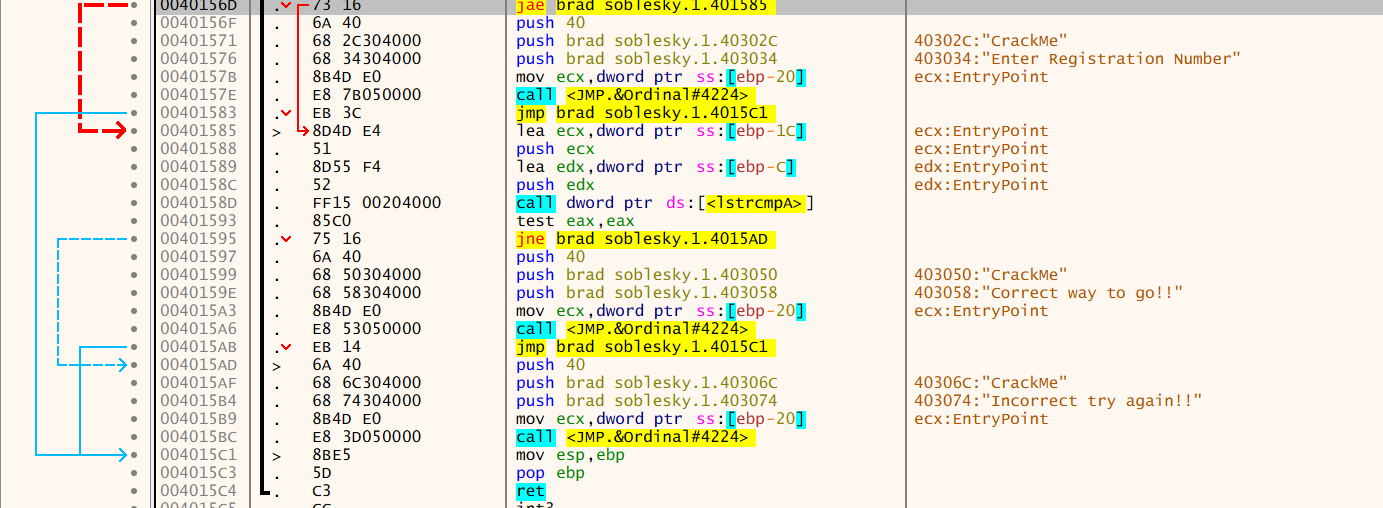


右键 – 搜索 – 当前模块 – 字符串：



找到错误提示时的字符串，再转回对应的反汇编地址：

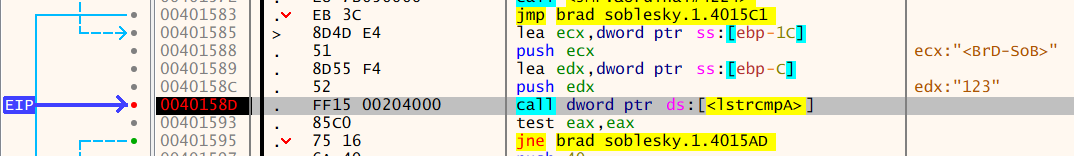




根据右边的文本可以看出第一段判断是密码框为空时输出的内容。

下面两段就是密码正确和错误时的内容，jne的判断条件是由前面的strcmp决定的，比较了ecx和edx的内存地址的内容是否相等。

在call strcmp处打断点，，F9恢复执行，输入错误密码123，命中断点：



可以看到正确密码为<BrD-SoB>。输入正确密码，成功：

