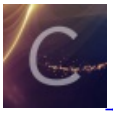
【jarvisoj刷题之旅】逆向题目Classical Crackme的writeup

原创

iqiqiya 于 2018-09-09 20:33:24 发布 833 收藏
分类专栏： 我的逆向之路 我的CTF之路 我的CTF进阶之路 文章标签： Classical Crackme 【jarvisoj刷题之旅】逆向题目 Classical Crackme的writeup reverse



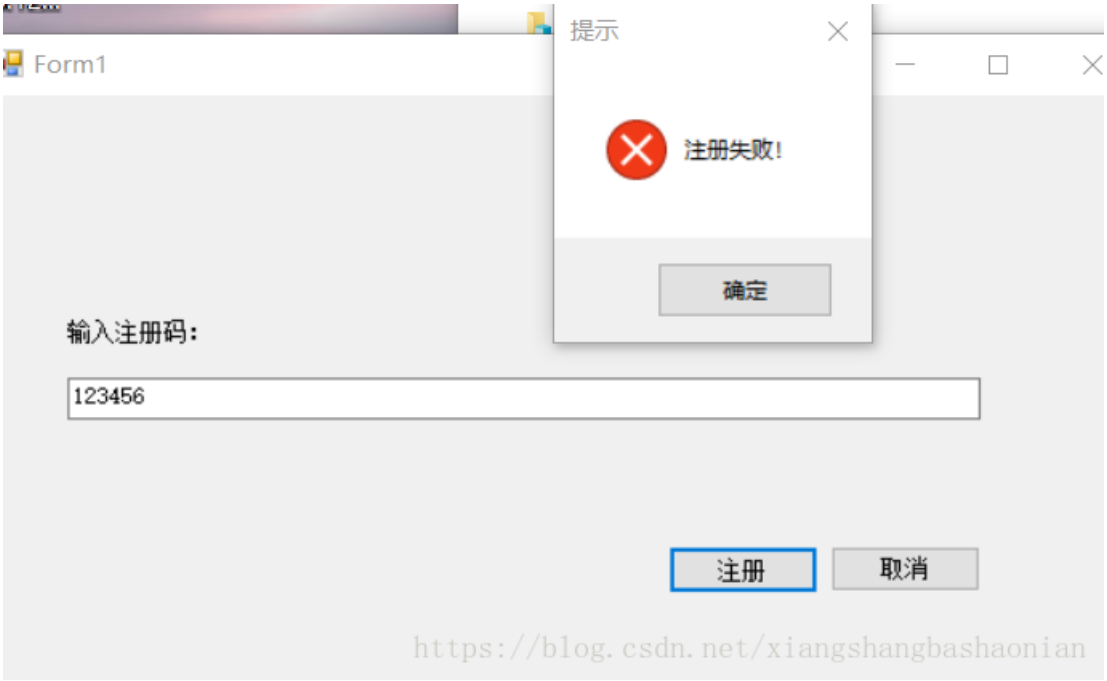
Winhex载入发现是rar压缩包

改后缀为.rar

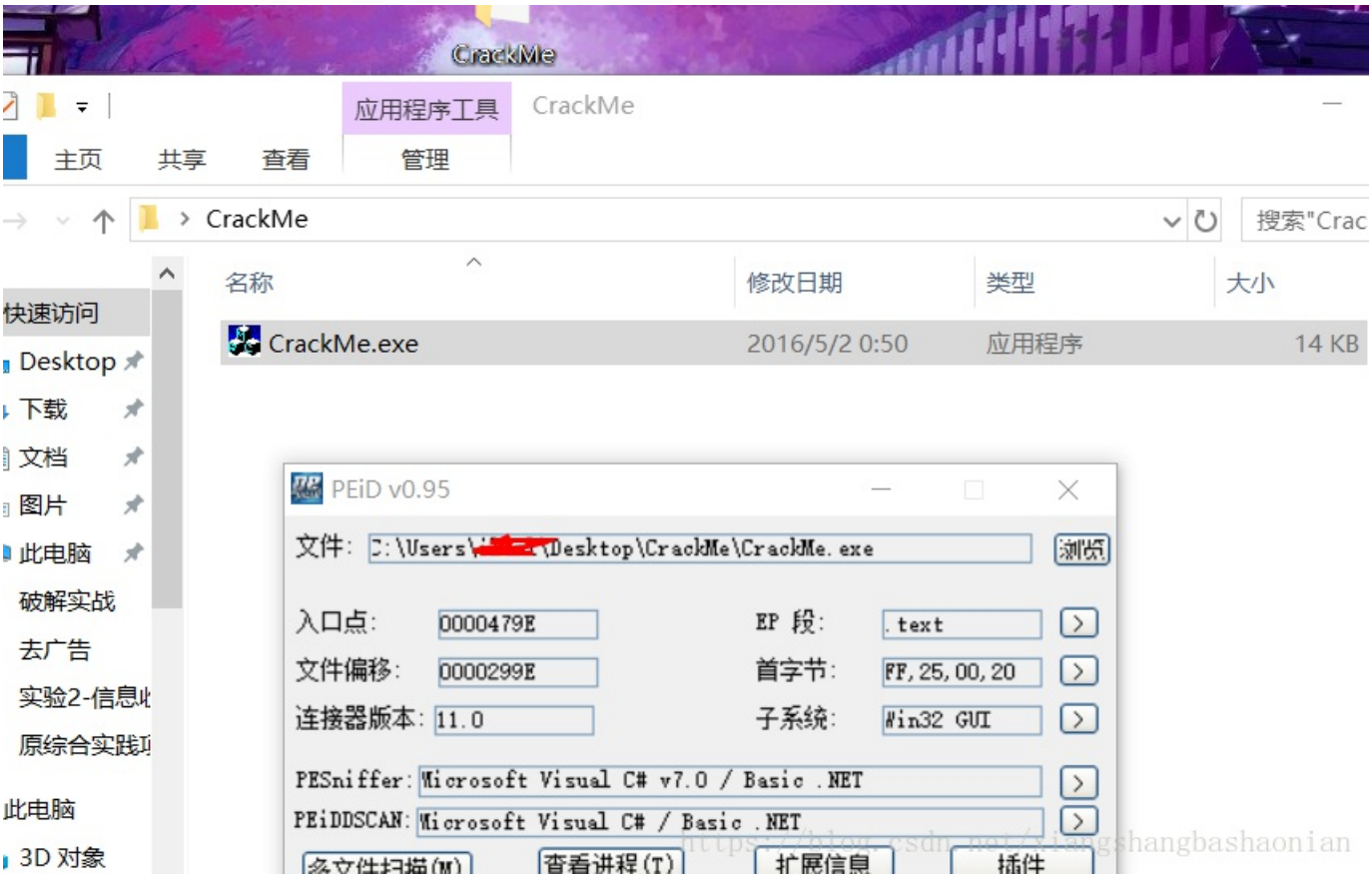
解压得到CrackMe.exe

先运行看看

输入123456 弹窗报错



那么注册失败就是关键词

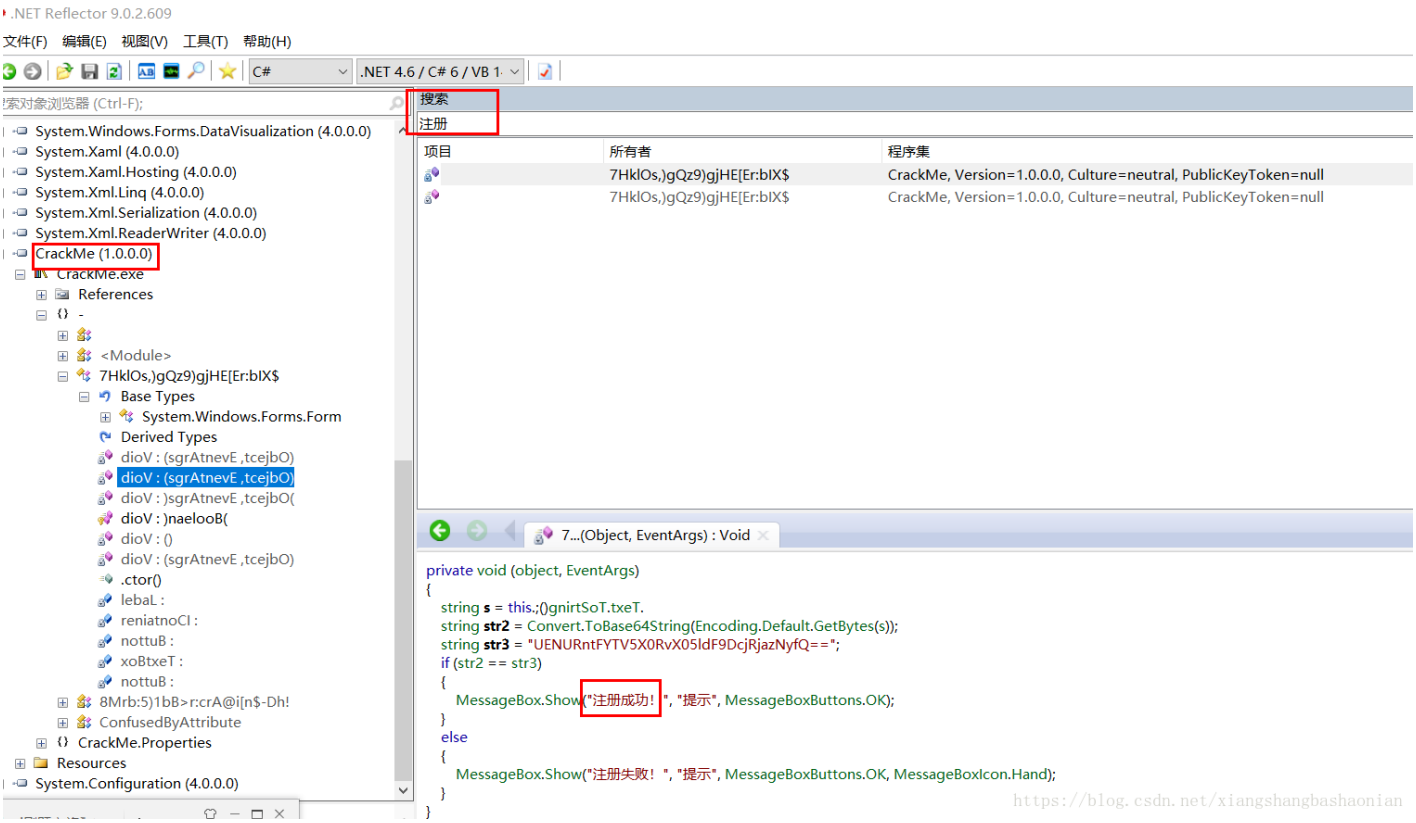


PEiD查壳无壳

可以看到是C#编写的(刚开始没仔细看 直接载入IDA了 结果一脸懵)

那就载入.NET Reflector

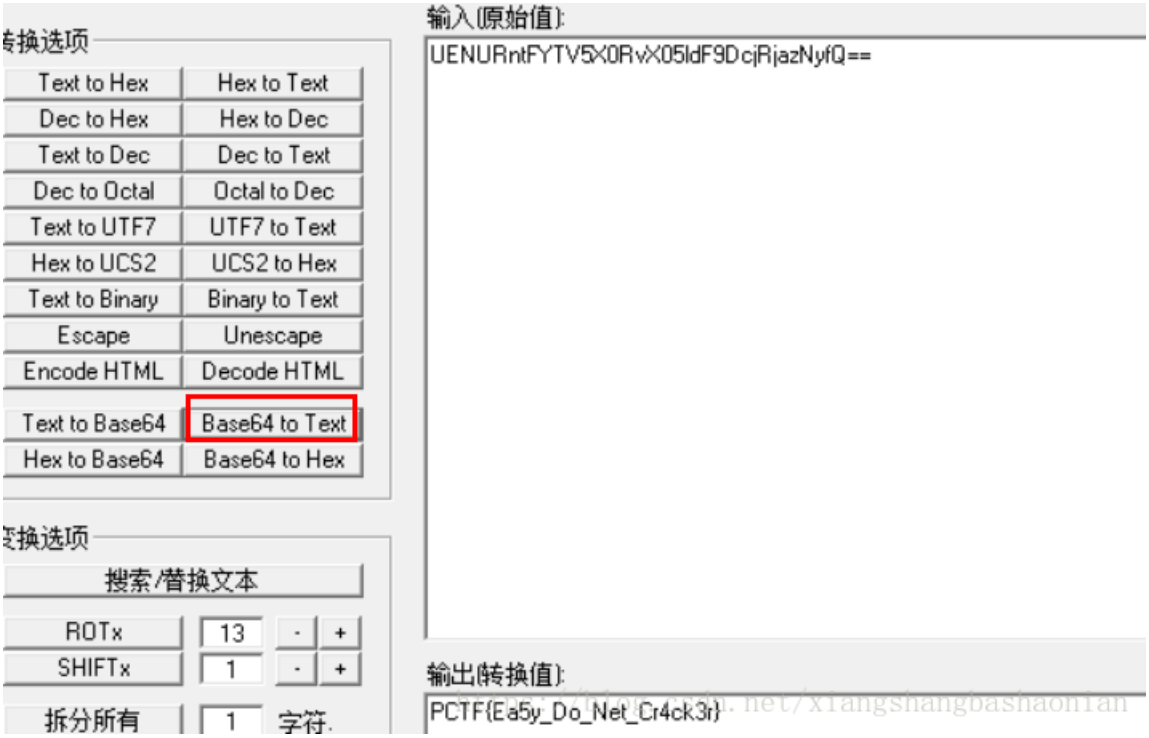
直接搜索“注册”



分析可知 是将我们的输入进行base64编码（即得到str2）

得到后与str3进行比较 如果一致就成功

那么我们只要把str3进行base64解码即可得到flag



提交显示正确