

【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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/xiangshangbashaonian/article/details/82561920>

版权



[我的逆向之路](#) 同时被 3 个专栏收录

108 篇文章 10 订阅

订阅专栏



[我的CTF之路](#)

92 篇文章 5 订阅

订阅专栏

[我的CTF进阶之路](#)

108 篇文章 18 订阅

订阅专栏

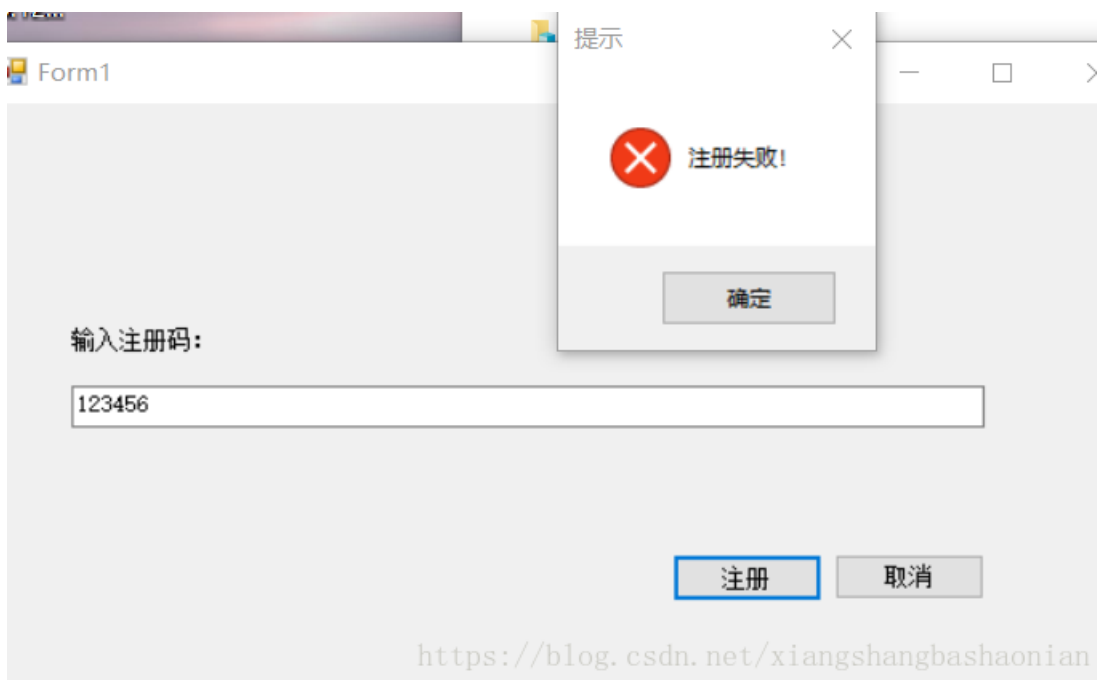
Winhex载入发现是rar压缩包

改后缀为.rar

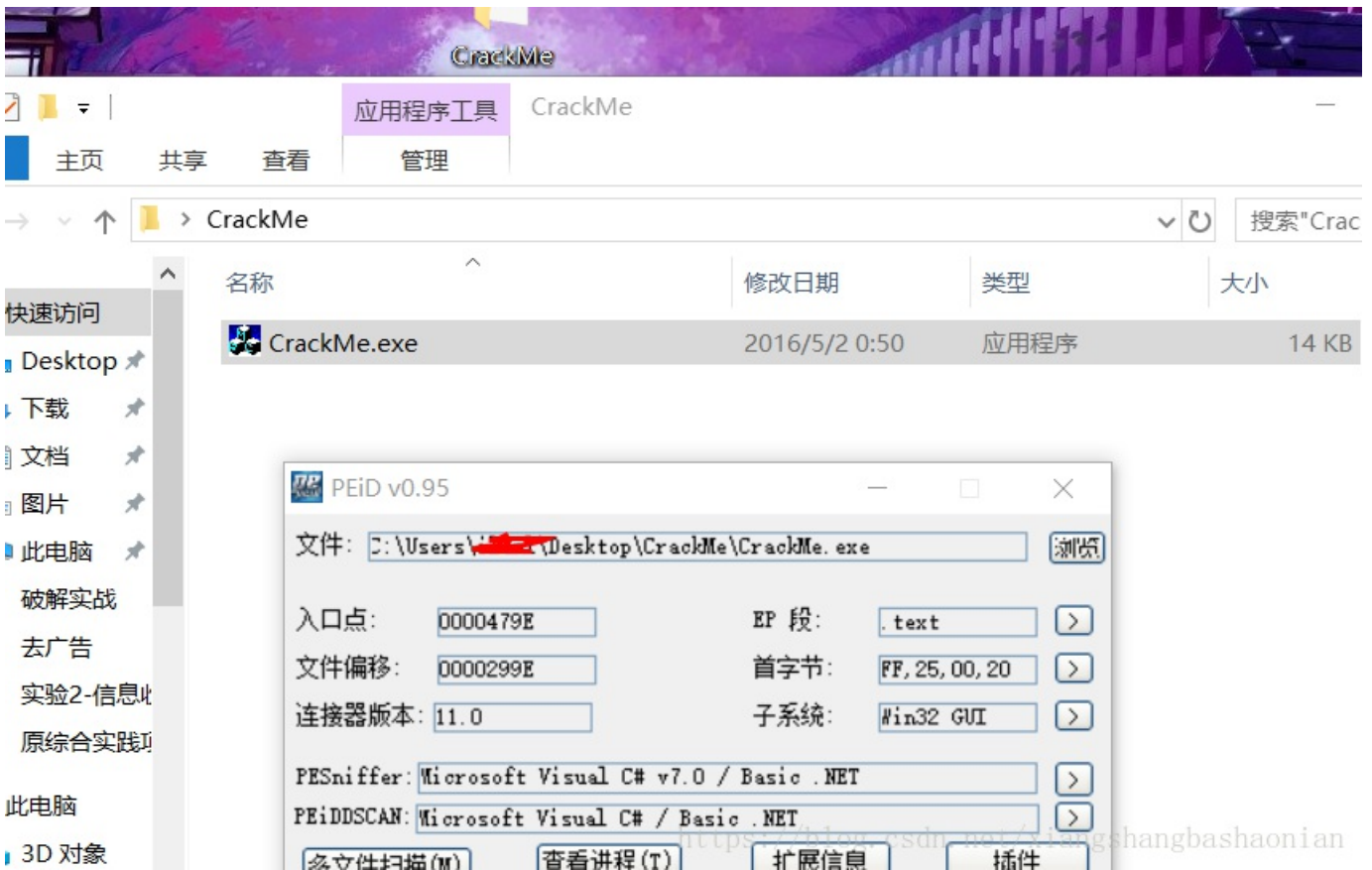
解压得到CrackMe.exe

先运行看看

输入123456 弹窗报错



那么注册失败就是关键词

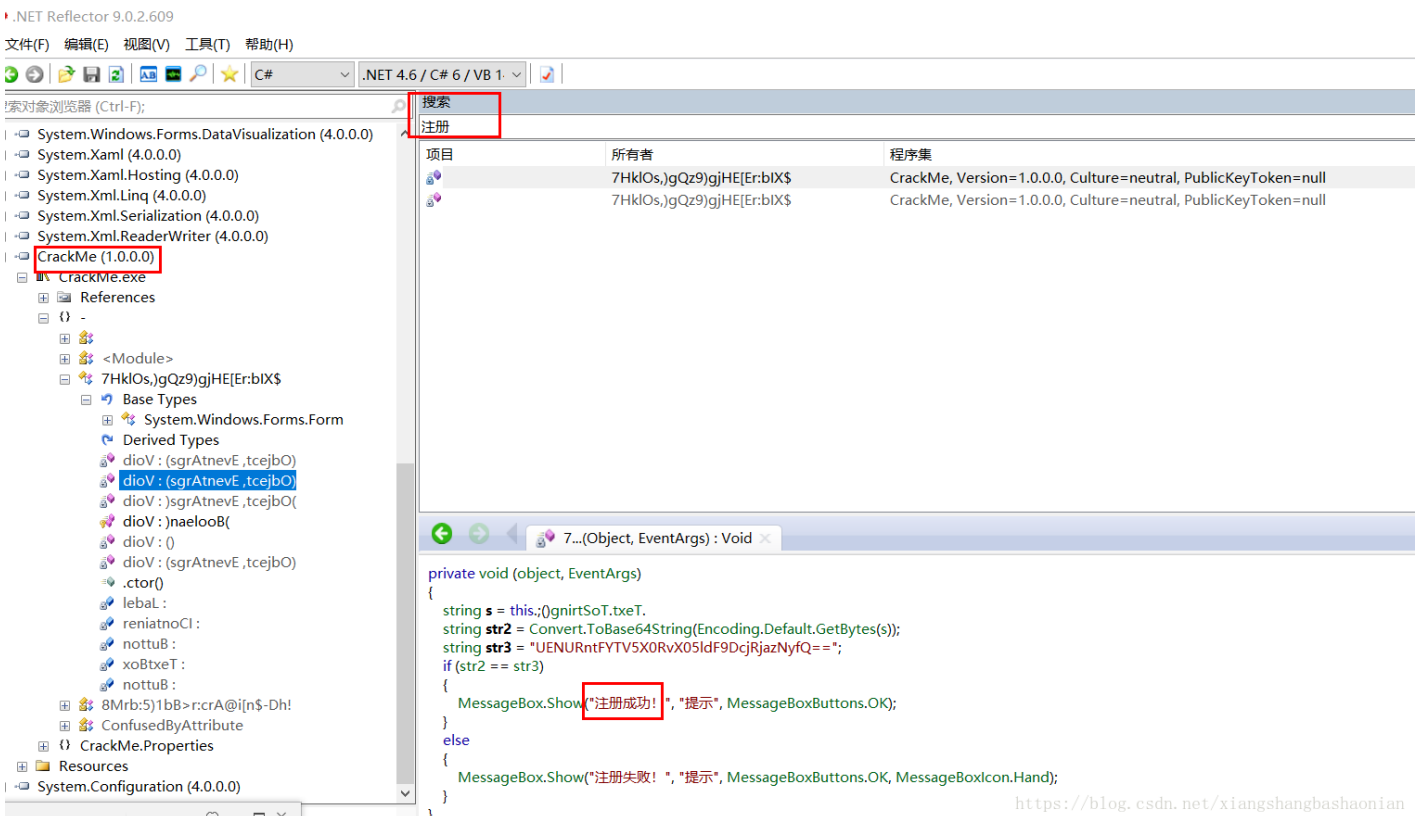


PEiD查壳无壳

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

转换选项

Text to Hex	Hex to Text
Dec to Hex	Hex to Dec
Text to Dec	Dec to Text
Dec to Octal	Octal to Dec
Text to UTF7	UTF7 to Text
Hex to UCS2	UCS2 to Hex
Text to Binary	Binary to Text
Escape	Unescape
Encode HTML	Decode HTML
Text to Base64	Base64 to Text
Hex to Base64	Base64 to Hex

输入(原始值):
UENURntFYTV5XORwX05ldF9DcjRjazNyfQ==

输出(转换值):
PCTF{Ea5y_Do_Net_Cr4ck3r}

转换选项

搜索/替换文本

ROTx | 13 | - | +

SHIFTx | 1 | - | +

拆分所有 | 1 | 字符.

提交显示正确

Classical Crackme 275 SOLVERS 100 REVERSE

经典Crackme题目，FLAG就是注册码。

[CrackMe.rar.4b81595bfc90d446ba30f9c9bb03fb49](#)

PCTF{Ea5y_Do_Net_Cr4ck3r} SUBMIT

Correct Answer!!Congratulations!

<https://blog.csdn.net/xiangshangbashaonian>