CTF小白学习笔记(Reverse)-i春秋 Classical CrackMe

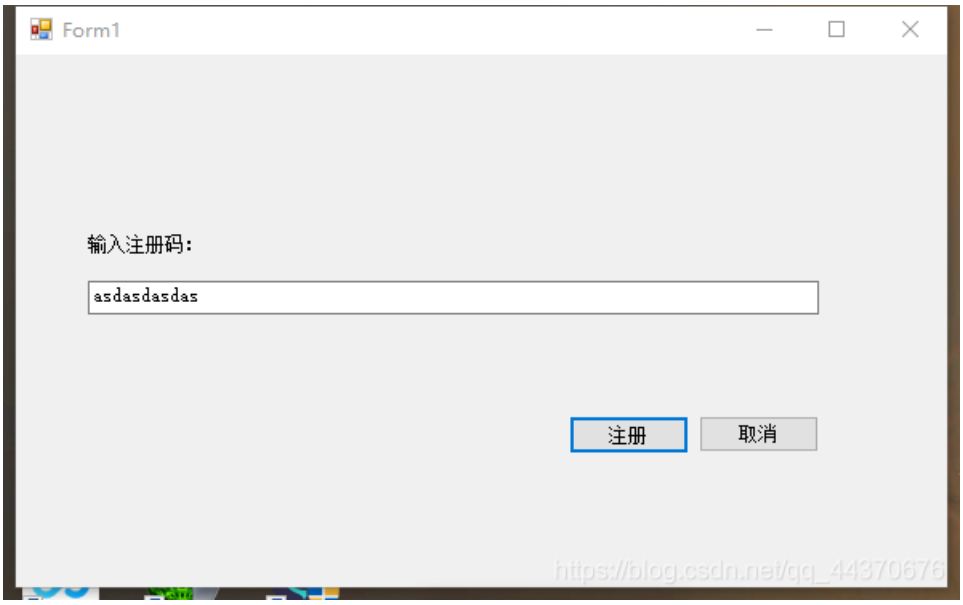
原创

I still … 于 2020-10-30 12:08:48 发布 289 收藏
分类专栏： CTF的writeup 文章标签： 安全

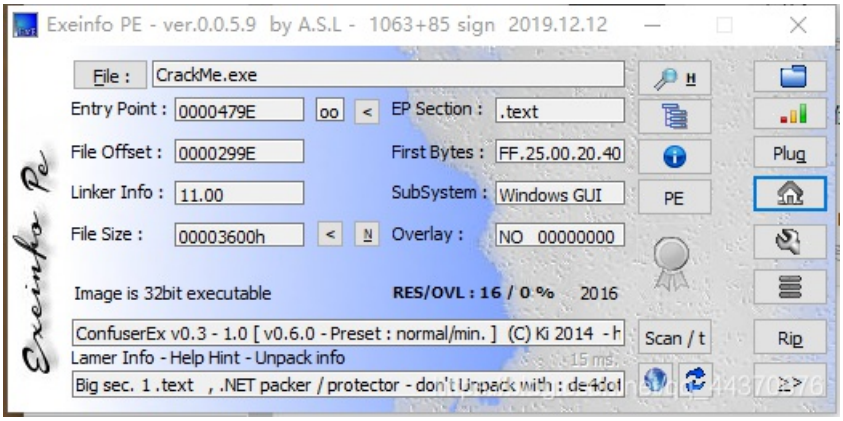
本文链接：https://blog.csdn.net/qq_44370676/article/details/109382710

这道题主要考察.Net程序逆向

运行一下：



用exeinfo查看文件：

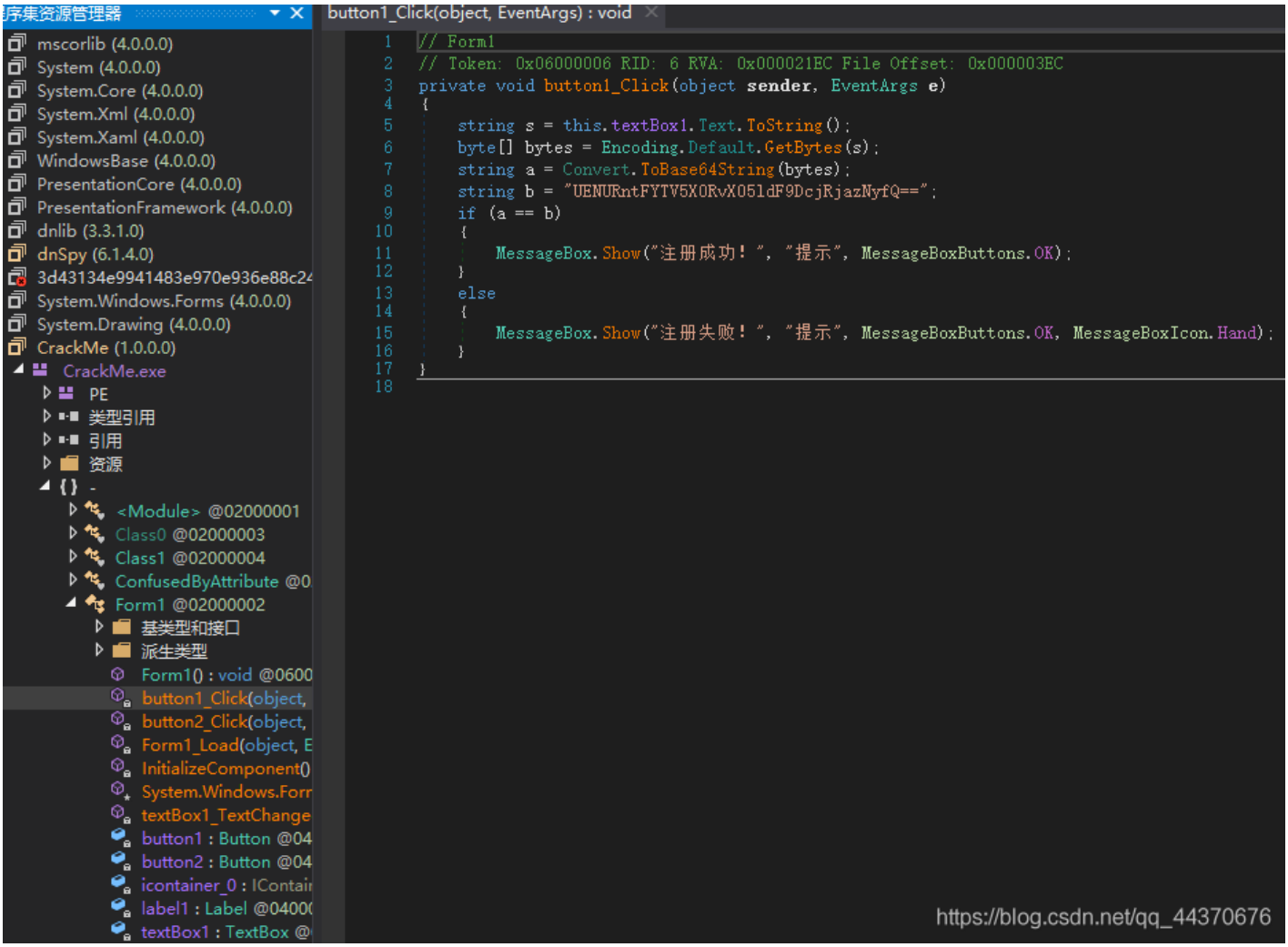


发现是混淆过的.Net程序

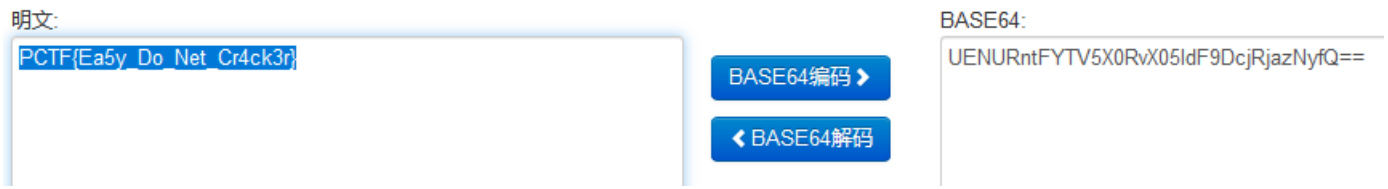
那再用de4dot反混淆，这里给一个de4dot下载链接：https://github.com/de4dot/de4dot/actions/runs/229869631

```
D:\CTFTools\de4dot>de4dot.exe CrackMe.exe

de4dot v3.1.41592.3405

Detected Unknown Obfuscator (D:\CTFTools\de4dot\CrackMe.exe)
Cleaning D:\CTFTools\de4dot\CrackMe.exe
Renaming all obfuscated symbols
Saving D:\CTFTools\de4dot\CrackMe-cleaned.exe

D:\CTFTools\de4dot>
```

反混淆后生成CrackMe-cleaned.exe，用dnsPy打开：



程序大概流程就是把输入字符串base64加密过后与字符串b比对，这里base64解码



得flag:PCTF{Ea5y_Do_Net_Cr4ck3r}