79：i春秋战役-奇怪的安装包

原创

S1lenc3 于 2020-02-28 19:49:39 发布 124 收藏

分类专栏： CTF

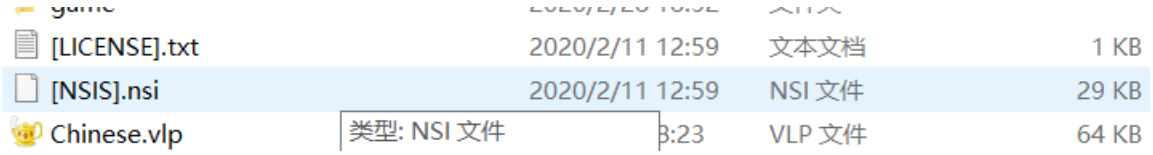
本文链接：https://blog.csdn.net/qq_41858371/article/details/104562533

> 拿到题OD分析了好长时间，根本不知道该怎么做，果断放弃。
> 好菜，找不到工作，唉

后来知道是用nsis做的安装程序，其实exeinfo工具可以查到。直接百度百科就有NSIS的介绍。

> NSIS（Nullsoft Scriptable Install System）是一个开源的 Windows 系统下安装程序制作程序。它提供了安装、卸载、系统设置、文件解压缩等功能。这如其名字所指出的那样，NSIS 是通过它的脚本语言来描述安装程序的行为和逻辑的。NSIS 的脚本语言和通常的编程语言有类似的结构和语法，但它是为安装程序这类应用所设计的。

而且查到了7z15.05版本可以直接提取出nsi脚本。




```
Dialogs::InputBox 1 请输入flag "Input your flag" 确定 取消 4 6
  ; Call Initialize____Plugins
  ; AllowSkipFiles off
  ; File $PLUGINSDIR\Dialogs.dll
  ; SetDetailsPrint lastused
  ; Push 6
  ; Push 4
  ; Push 取消
  ; Push 确定
  ; Push "Input your flag"
  ; Push 请输入flag
  ; Push 1
  ; CallInstDLL $PLUGINSDIR\Dialogs.dll InputBox
IntCmp $4 1 0 label_415 label_415
Push $6
Call func_429
Pop $6
StrCpy $3 gm`fzd787`7bb,g72d,592b,8`g1,cg96813e8d``|
StrCmp $3 $6 0 label_417
MessageBox MB_OK flag正确,可以愉快的玩游戏了
```


找到关键代码进行分析，汇编都能看懂，这看着 就更方便了，最后写脚本跑一下。这题太搞了，难受。

```python
s = 'gm`fzd787`7bb,g72d,592b,8`g1,cg96813e8d``|'
flag = ''
for i in s:
    flag += chr(ord(i) ^ 1)
print(flag)
```