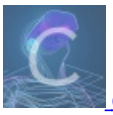
re学习笔记（41）i春秋2020GYCTF-re-奇怪的安装包

原创

Forgo7ten 于 2020-02-23 11:38:19 发布 568 收藏

分类专栏： ctf小白成长ing # reverse 文章标签： nsis ctf i春秋 reverse python

本文链接：https://blog.csdn.net/Palmer9/article/details/104455873


ctf小白成长ing 同时被 2 个专栏收录

112 篇文章 6 订阅

订阅专栏


reverse

113 篇文章 6 订阅

订阅专栏

i春秋2020新春战疫赛-re-奇怪的安装包

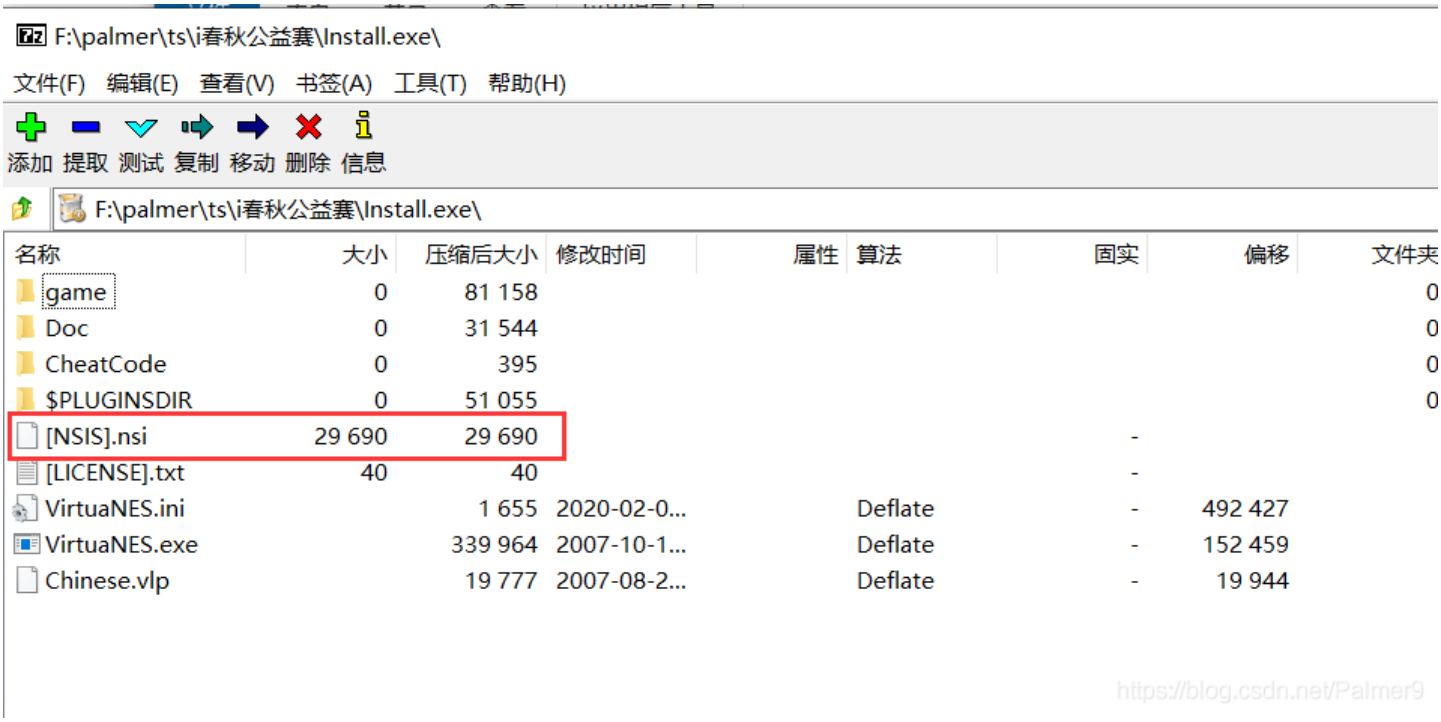
新手一枚，如有错误（不足）请指正，谢谢！！

个人博客：点击进入

题目下载：

> 链接: https://pan.baidu.com/s/1N9NFUPITE9xcFCg7tnOPWw 提取码: 2020

压缩包，想到NSIS制作压缩包（其实没想到
然后使用7-zip打开Install.exe文件，查看[NSIS].nsi文件



找到判断的代码

```
Dialogs::InputBox 1 请输入key "Input your key" 确定 取消 4 6
  ; Call Initialize_____Plugins
  ; SetOverwrite off
  ; File $PLUGINSDIR\Dialogs.dll
  ; SetDetailsPrint lastused
  ; Push 6
  ; Push 4
  ; Push 取消
  ; Push 确定
  ; Push "Input your key"
  ; Push 请输入key
  ; Push 1
  ; CallInstDLL $PLUGINSDIR\Dialogs.dll InputBox
DetailPrint "Checking...: $6"
IntCmp $4 1 0 label_415 label_415
StrCmp $6 NSIISSOEASY 0 label_415
MessageBox MB_OK key正确
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
```

```
  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
  Goto label_419
label_415:
  MessageBox MB_OK 错误的key
  MessageBox MB_OK 想办法找到正确的key把
label_417:
  MessageBox MB_OK flag错误
  MessageBox MB_OK 想办法找到正确的flag把
label_419:
SectionEnd


Section ; Section_1
  WriteUninstaller $INSTDIR\uninst.exe ;  $INSTDIR\$INSTDIR\uninst.exe    ; !!! ERROR: SKIP possible BadCmd
  WriteRegStr HKLM "Software\Microsoft\Windows\CurrentVersion\App Paths\VirtuaNES.exe" "" $INSTDIR\VirtuaNES.exe
  WriteRegStr HKLM Software\Microsoft\Windows\CurrentVersion\Uninstall\VirtuaNES DisplayName $(LSTR_2)    ;  "Vi
rtuaNES 1.0"
  WriteRegStr HKLM Software\Microsoft\Windows\CurrentVersion\Uninstall\VirtuaNES UninstallString $INSTDIR\uninst
.exe
  WriteRegStr HKLM Software\Microsoft\Windows\CurrentVersion\Uninstall\VirtuaNES DisplayIcon $INSTDIR\VirtuaNES.
exe
  WriteRegStr HKLM Software\Microsoft\Windows\CurrentVersion\Uninstall\VirtuaNES DisplayVersion 1.0
  WriteRegStr HKLM Software\Microsoft\Windows\CurrentVersion\Uninstall\VirtuaNES URLInfoAbout http://www.baidu.c
om
  WriteRegStr HKLM Software\Microsoft\Windows\CurrentVersion\Uninstall\VirtuaNES Publisher Ginkgo.
SectionEnd


Function func_429        # 将字符串的每个字符与1异或并返回
  Pop $9                # 输入字符串出栈
  StrCpy $3 ""          # 给$3拷贝空字符串
  StrCpy $0 $9           # 将输入字符串给$0
  StrCpy $1 0         # 将0赋值给$1
label_433:
  StrCpy $2 $0 1 $1
  StrCmp $2 "" label_443 # 如果取到空字符，就退出循环
  Push $2
  Call func_445          # 将取出的一个字符，丢入func_445 call进行处理
  Pop $2
  IntOp $2 $2 ^ 1        # 将字符与1异或后赋值给$2
  IntFmt $2 %c $2        # 将$2解释成字符赋值给$2
  IntOp $1 $1 + 1        # $1自加1，遍历下个字符，直到遍历所有
  StrCpy $3 $3$2         # 将$2拼接到$3后面
  Goto label_433
label_443:
  Push $3
FunctionEnd


Function func_445        # 返回与字符对应的ASCII码
  Exch $0                # 将传入的字符给$0

Exch 交换两个值，如果调用 Exch 没有指定任何参数，将交换堆栈顶部的两个数据。
  如果指定了一个用户变量作为 Exch的参数，变量的值将和堆栈顶部的数据交换。
  如果调用 Exch 并指定了一个栈的索引（从 0 开始，0 代表堆栈顶部的栈），将交换堆栈顶部和指定的栈的数据。
    ; Push $0
```

```
    ; Exch
    ; Pop $0
  Push $1               # 保存$1的值
  Push $2       # 保存$2的值
  StrCpy $2 1           # 给$2赋值1 （进行计数器的初始化）
label_451:
  IntFmt $1 %c $2       # 将$2解释成字符给$1
  StrCmpS $1 $0 0 label_455  # 比较$1和$0  如果相等则退出循环  不相等进行下一次循环
  StrCpy $0 $2          # 将$2这个数值给$0
  Goto label_458
label_455:
  IntOp $2 $2 + 1       # $2自加1
  StrCmp $2 255 0 label_451  # $2如果不等于255就返回label_451（循环255次 $2为计数器）
  StrCpy $0 0           # $0赋值0
label_458:
  Pop $2     # 恢复$2的值
  Pop $1     # 恢复$1的值
  Exch $0               # $0的值为字符对应的ASCII码
    ; Push $0
    ; Exch
    ; Pop $0
FunctionEnd
```

```
711   Dialogs::InputBox 1 请输入key "Input your key" 确定 取消 4 6
712     ; Call Initialize_____Plugins
713     ; SetOverwrite off
714     ; File $PLUGINSDIR\Dialogs.dll
715     ; SetDetailsPrint lastused
716     ; Push 6
717     ; Push 4
718     ; Push 取消
719     ; Push 确定
720     ; Push "Input your key"
721     ; Push 请输入key
722     ; Push 1
723     ; CallInstDLL $PLUGINSDIR\Dialogs.dll InputBox
724   DetailPrint "Checking...: $6"
725   IntCmp $4 1 0 label_415 label_415
726   StrCmp $6 NSIISSOEASY 0 label_415
727   MessageBox MB_OK key正确
728   Dialogs::InputBox 1 请输入flag "Input your flag" 确定 取消 4 6
729     ; Call Initialize_____Plugins
730     ; AllowSkipFiles off
731     ; File $PLUGINSDIR\Dialogs.dll
732     ; SetDetailsPrint lastused
733     ; Push 6
734     ; Push 4
735     ; Push 取消
736     ; Push 确定
737     ; Push "Input your flag"
738     ; Push 请输入flag
739     ; Push 1
740     ; CallInstDLL $PLUGINSDIR\Dialogs.dll InputBox
741   IntCmp $4 1 0 label_415 label_415
742   Push $6
743   Call func_429
744   Pop $6
745   StrCpy $3 gm`fzd787`7bb,g72d,592b,8`g1,cg96813e8d``|
746   StrCmp $3 $6 0 label_417
747   MessageBox MB_OK flag正确,可以愉快的玩游戏了
748   Goto label_419
749 label_415:
750   MessageBox MB_OK 错误的key
751   MessageBox MB_OK 想办法找到正确的key把
752 label_417:
```

```
753     MessageBox MB_OK flag错误
754     MessageBox MB_OK 想办法找到正确的flag把
755   label_419:
756   SectionEnd
```


[NSIS].nsi.txt

```
770
771   Function func_429          # 将字符串的每个字符与1异或并返回
772     Pop $9                   # 输入字符串出栈
773     StrCpy $3 ""             # 给$3拷贝空字符串
774     StrCpy $0 $9             # 将输入字符串给$0
775     StrCpy $1 0              # 将0赋值给$1
776   label_433:
777     StrCpy $2 $0 1 $1
778     StrCmp $2 "" label_443 # 如果取到空字符，就退出循环
779     Push $2
780     Call func_445            # 将取出的一个字符，丢入func_445 call进行处理
781     Pop $2
782     IntOp $2 $2 ^ 1          # 将字符与1异或后赋值给$2
783     IntFmt $2 %c $2          # 将$2解释成字符赋值给$2
784     IntOp $1 $1 + 1          # $1自加1，遍历下个字符，直到遍历所有
785     StrCpy $3 $3$2           # 将$2拼接到$3后面
786     Goto label_433
787   label_443:
788     Push $3
789   FunctionEnd
790
791
792   Function func_445          # 返回与字符对应的ASCII码
793     Exch $0                  # 将传入的字符给$0
794
795   Exch 交换两个值，如果调用 Exch 没有指定任何参数，将交换堆栈顶部的两个数据。
796     如果指定了一个用户变量作为 Exch的参数，变量的值将和堆栈顶部的数据交换。
797     如果调用 Exch 并指定了一个栈的索引（从 0 开始，0 代表堆栈顶部的栈），将交换堆栈顶部和指定的栈的数据。
798       ; Push $0
799       ; Exch
800       ; Pop $0
801     Push $1                  # 保存$1的值
802     Push $2                  # 保存$2的值
803     StrCpy $2 1              # 给$2赋值1 （进行计数器的初始化）
804   label_451:
805     IntFmt $1 %c $2          # 将$2解释成字符给$1
806     StrCmpS $1 $0 0 label_455      # 比较$1和$0  如果相等则退出循环  不相等进行下一次循环
807     StrCpy $0 $2             # 将$2这个数值给$0
808     Goto label_458
809   label_455:
810     IntOp $2 $2 + 1          # $2自加1
811     StrCmp $2 255 0 label_451      # $2如果不等于255就返回label_451（循环255次 $2为计数器）
812     StrCpy $0 0              # $0赋值0
813   label_458:
814     Pop $2                   # 恢复$2的值
815     Pop $1                   # 恢复$1的值
816     Exch $0                  # $0的值为字符对应的ASCII码
817       ; Push $0
818       ; Exch
819       ; Pop $0
820   FunctionEnd
```

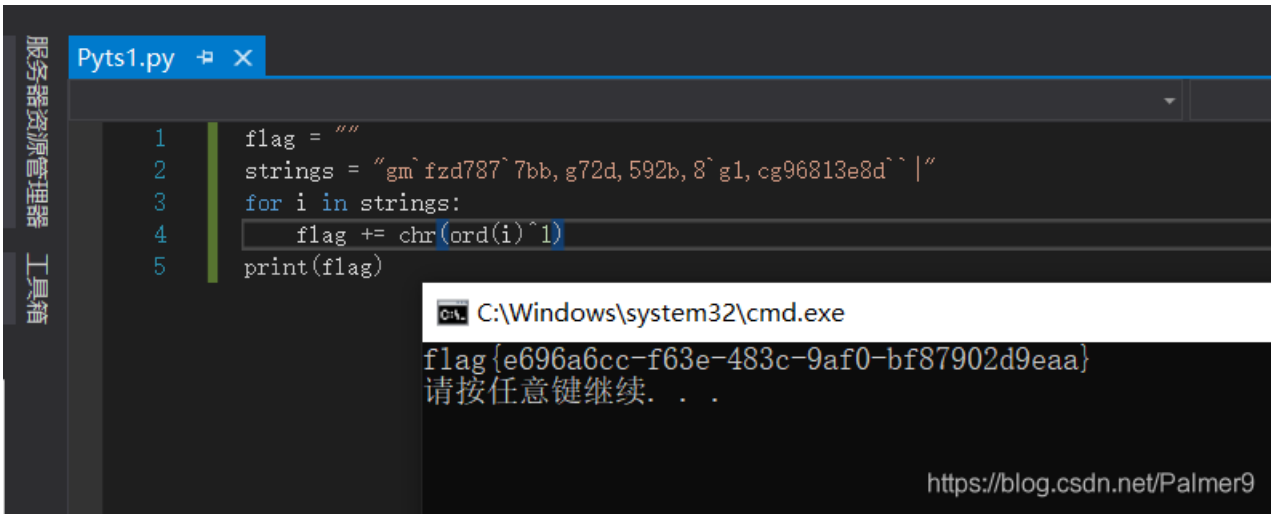

大体流程是将输入的字符串转换为ASCII码然后与1异或，最后与

```
gm`fzd787`7bb,g72d,592b,8`g1,cg96813e8d``|
```

进行比较
所以只要我们将密文与1异或然后就是输入的flag

写脚本得到flag

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



flag为`flag{e696a6cc-f63e-483c-9af0-bf87902d9eaa}`