xctf 逆向crackme题解

原创

buzhifou01 于 2019-12-20 21:50:16 发布 377 收藏

分类专栏： 逆向 Xctf题解 文章标签： 安全

本文链接：https://blog.csdn.net/qq_33526144/article/details/103639091

逆向 同时被 2 个专栏收录

18 篇文章 0 订阅

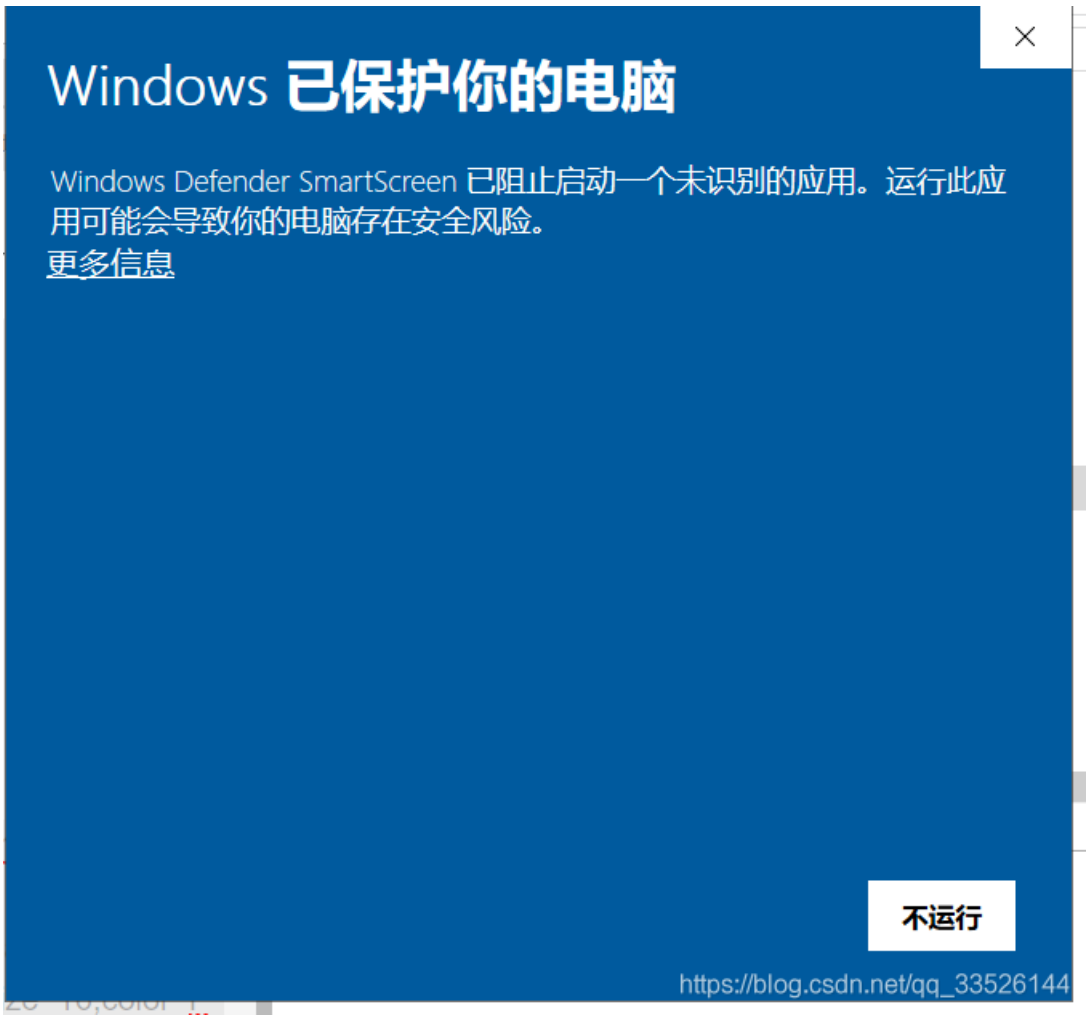
订阅专栏

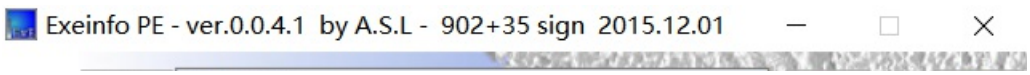
Xctf题解

6 篇文章 0 订阅

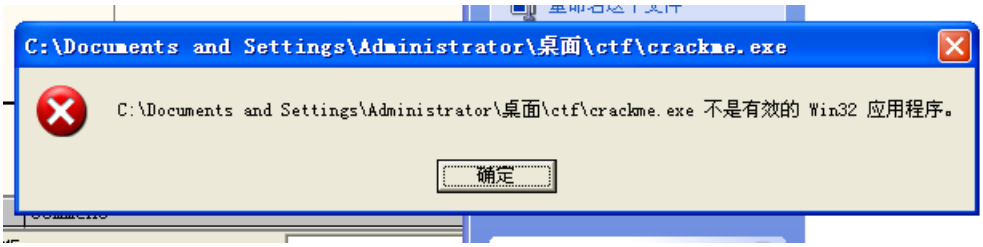
订阅专栏

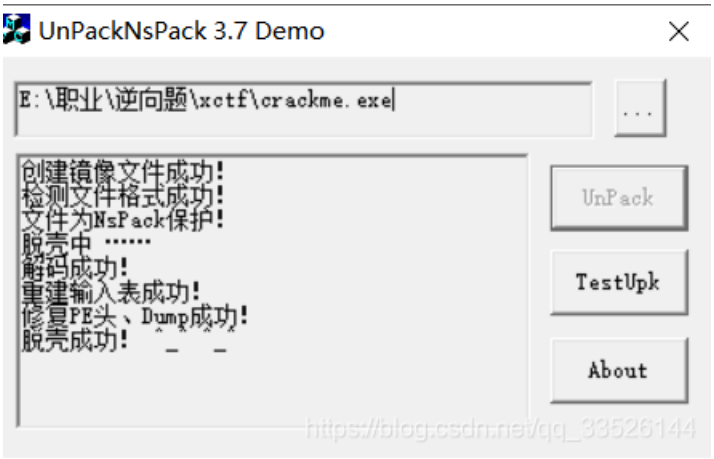
1.运行，运行不了，查壳，发现是nspack壳。

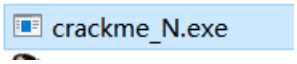




2.在xp系统环境，用od载入，发现失败，用脱壳机脱壳。







3.拖入到ida中，在main函数中看到关键代码

```
if ( strlen(&Buf) == 42 )
  {
    v4 = 0;
    while ( (*(&Buf + v4) ^ byte_402130[v4 % 16]) == dword_402150[v4] )
    {
      if ( ++v4 >= 42 )
      {
        printf("right!\n");
        goto LABEL_8;
      }
    }
```

```
.nsp0:00402130 byte_402130     db 't'                  ; DATA
.nsp0:00402130                                         ; t
.nsp0:00402131 aHisIsNotFlag   db 'his_is_not_flag',0


.nsp0:00402150 dword_402150    dd 12h                  ; DATA XREF: _main+8D↑r
.nsp0:00402154                 dd 4, 8, 14h, 24h, 5Ch, 4Ah, 3Dh, 56h, 0Ah, 10h, 67h, 0
.nsp0:00402184                 dd 41h, 0
.nsp0:0040218C                 dd 1, 46h, 5Ah, 44h, 42h, 6Eh, 0Ch, 44h, 72h, 0Ch, 0Dh
.nsp0:0040218C                 dd 40h, 3Eh, 4Bh, 5Fh, 2, 1, 4Ch, 5Eh, 5Bh, 17h, 6Eh, 0Ch
.nsp0:0040218C                 dd 16h, 68h, 5Bh, 12h, 2 dup(0)
.nsp0:00402200                 dd 48h, 0Eh dup(0)
```

分析算法可知，计算flag的代码如下：

```
s='this_is_not_flag'

a=[
0x12,0x4,0x8,0x14,0x24,0x5C,0x4A,0x3D,0x56,0x0A,0x10,0x67,0x0,0x41,0x0,0x1,0x46,0x5A,0x44,0x42,0x6E,0x0C,0x44,0x
72,0x0C,0x0D,0x40, 0x3E, 0x4B, 0x5F, 0x2, 0x1, 0x4C, 0x5E, 0x5B, 0x17, 0x6E, 0x0C,0x16,0x68,0x5B,0x12,0,0,0x48,0
,0,0,0,0,0,0,0,0,0,0,0,0
]

flag=''

for i in range(0,42):
   flag+=chr(ord(s[i%16])^a[i])

print flag
```

flag为：flag{59b8ed8f-af22-11e7-bb4a-3cf862d1ee75}