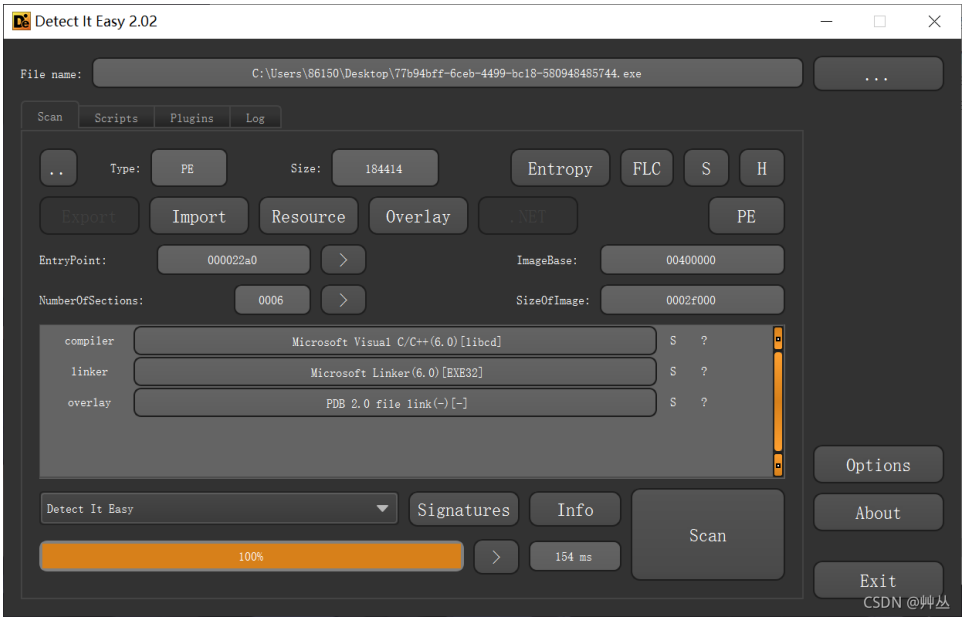
buuctf————findkey

原创

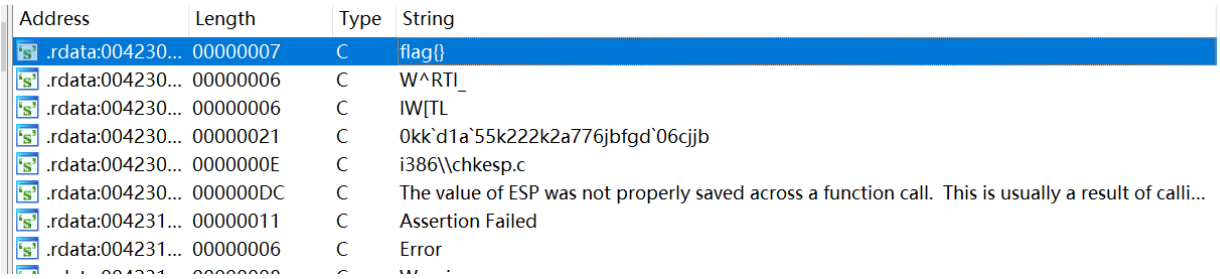
re3sry 于 2021-09-18 18:22:46 发布 145 收藏
文章标签： python

1.查壳。无壳，32位。



2.IDA反编译。

shift+f12查找字符串。发现关键词flag。



跟进。

发现IDA没有反编译成功。手动反编译（p键）。

```
.text:00401A37
.text:00401A37 loc_401A37:                             ; CODE XREF: .text:004019D9↑j
.text:00401A37                 nop
.text:00401A38                 mov     esi, esp
.text:00401A3A                 push    offset aFlag    ; "flag{}"
.text:00401A3F                 mov     edx, [ebp+8]
.text:00401A42                 push    edx
.text:00401A43                 call    ds:SetWindowTextA
.text:00401A49                 cmp     esi, esp
.text:00401A4B                 call    __chkesp
.text:00401A50                 mov     esi, esp
.text:00401A52                 push    0
.text:00401A54                 push    offset asc_423024 ; "^_^"
.text:00401A59                 push    offset aAreYouKiddingM ; "Are you kidding me?"
.text:00401A5E                 mov     eax, [ebp+8]
.text:00401A61                 push    eax
.text:00401A62                 call    ds:MessageBoxA
.text:00401A68                 cmp     esi, esp
.text:00401A6A                 call    __chkesp
.text:00401A6F                 mov     esi, esp
.text:00401A71                 push    0
.text:00401A73                 call    ds:ExitProcess
.text:00401A79 ; ---------------------------------------------------------------------------
.text:00401A79                 cmp     esi, esp
.text:00401A7B                 call    __chkesp
.text:00401A80
```


第一次做的时候按了p就出了。复盘的时候不知道又不行了。

又找了找原因发现是花指令。（这个位置两个一样的push删掉一个就ok）

```
.text:00401918                 push    offset byte_428C54
.text:0040191D
.text:0040191D loc_40191D:                             ; CODE XREF: .text:0040193D↓j
.text:0040191D                 push    offset byte_428C54
.text:00401922                 call    _strlen
```



```
        sub_40101E(String1, v9, (LPSTR)String1);
        strcpy((char *)(a2 - 748), "0kk`d1a`55k222k2a776jbfgd`06cjjb");
        memset((void *)(a2 - 715), 0, 0xDCu);
        v10 = a2 - 715 + 220;
        *(_WORD *)v10 = 0;
        *(_BYTE *)(v10 + 2) = 0;
        strcpy((char *)(a2 - 760), "SS");
        *(_DWORD *)(a2 - 757) = 0;
        *(_WORD *)(a2 - 753) = 0;
        *(_BYTE *)(a2 - 751) = 0;
        v11 = strlen((const char *)(a2 - 748));
        sub_401005((LPCSTR)(a2 - 760), a2 - 748, v11);
        if ( _strcmpi((const char *)String1, (const char *)(a2 - 748)) )
        {
          SetWindowTextA(*(HWND *)(a2 + 8), "flag{}");
          MessageBoxA(*(HWND *)(a2 + 8), "Are you kidding me?", "^_^", 0);
          ExitProcess(0);
        }
        memcpy((void *)(a2 - 1016), &unk_423030, 0x32u);
        v12 = strlen((const char *)(a2 - 1016));
        sub_401005((LPCSTR)(a2 - 492), a2 - 1016, v12);
        MessageBoxA(*(HWND *)(a2 + 8), (LPCSTR)(a2 - 1016), 0, 0x32u);
      }
      ++dword_428D54;
    }
    else
```


3.分析代码。关键函数是sub401005.

根据if条件可得string1（MD5加密后）（看最前面sub40101e函数可知string经过了MD5加密）

（a2-748）是0kk`d1a`55k222k2a776jbfgd`06cjjb经过sub401005计算的结果

查看sub401005函数

只是一个简单的异或。直接上脚本，得到c8837b23ff8aaa8a2dde915473ce0991（MD5加密后）

解密得到string1=123321（一开始以为这就是flag，提交发现是错的）

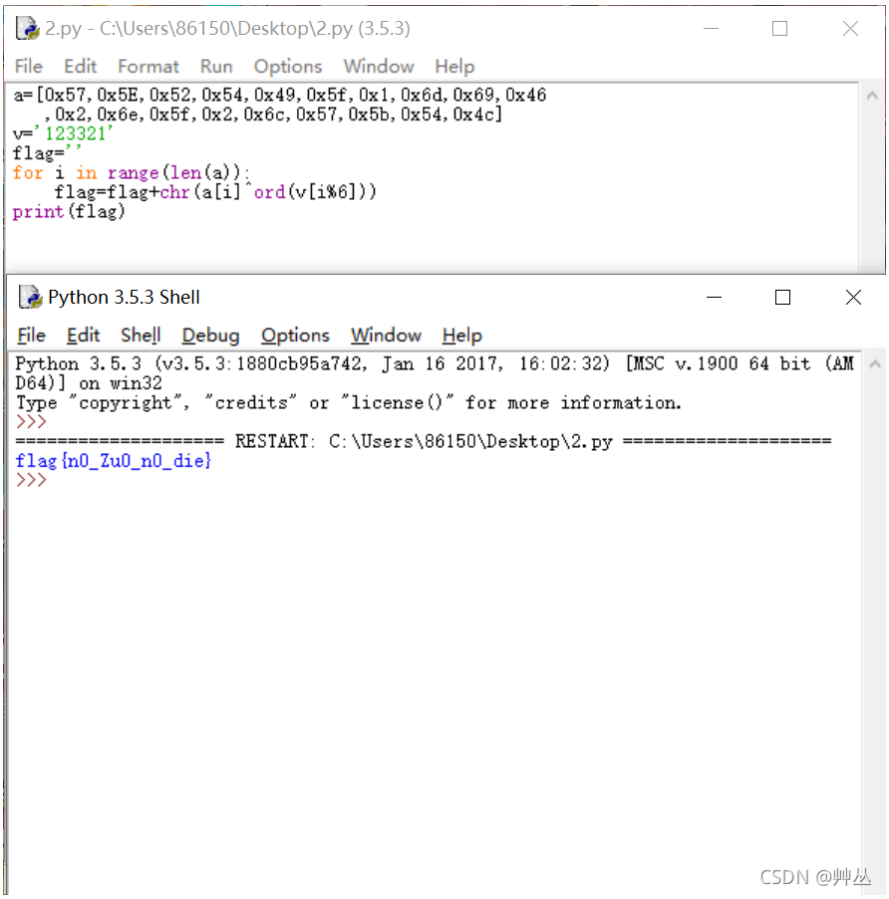
```
File  Edit  Format  Run  Options  Window  Help
a='0kk`d1a`55k222k2a776jbfgd`06cjjb'
v='SS'
flag=''
for i in range(len(a)):
    flag=flag+chr(ord(a[i])^ord(v[i%2]))
print(flag)
```


再次看代码发现后面还有

还是sub_401005函数参数（123321,unk_423030,len(unk_423030)）,再次运行脚本得到flag

```
    {
      SetWindowTextA(*(HWND *)(a2 + 8), "flag{}");
      MessageBoxA(*(HWND *)(a2 + 8), "Are you kidding me?", "^_^", 0);
      ExitProcess(0);
    }
    memcpy((void *)(a2 - 1016), &unk_423030, 0x32u);
    v12 = strlen((const char *)(a2 - 1016));
    sub_401005((LPCSTR)(a2 - 492), a2 - 1016, v12);
    MessageBoxA(*(HWND *)(a2 + 8), (LPCSTR)(a2 - 1016), 0, 0x32u);
}
```


再次运行脚本得到flag



4.get flag

flag{n0_Zu0_n0_die}