step1 writeup —— 输入作为函数参数

原创

R00cky 于 2015-05-02 18:55:17 发布 438 收藏
分类专栏： writeup 文章标签： writeup 逆向 ctf

Hint：

暂无HINT

题目描述：

Do you know SendMessage ?

Writeup：

在IDA字符串窗口中找到字符串“The password is:”，于是根据交叉参考找到了相关函数。

OD同时定位到该函数，单步调试，发现有两个SendMessageA函数，两个函数的参数形式相同，第一个Message为WM_GETTEXT，将获取到的name存入栈中。第二个Message未知，但由于两个SendMessageA函数的参数形式相同，猜测第二个Message同为WM_GETTEXT，且将获取的key存入栈中。

```
push    ecx                             lParam
push    0C                              wParam = C
sub     eax, 200E4
push    eax                             Message
push    esi                             hWnd
call    edi                             SendMessageA
```


可以看到eax-200E4h为Message类型参数，WM_GETTEXT为0Dh，所以eax为200E4h+0Dh=131313D，eax为StrToIntA函数的返回值，因此输入的name应为“131313”。

后面有个GetProcAddress函数，该函数的第二个参数（库函数名称）为输入的key与程序中的一个固定字符串异或而得

```
loc_4010AA:
mov     eax, ecx
cdq
idiv    esi
mov     al, [ebp+edx+String2] ; 固定字符串
xor     [ebp+ecx+ProcName], al ; 与输入的key进行异或
inc     ecx
cmp     ecx, 0Bh
jl      short loc_4010AA
```


返回值存入ebp+arg_8。在后面有个打印password的函数，但是在调用的时候并不是call MessageBoxA，而是call [ebp+arg_8]，因此猜测GetProcAddress函数获取的是MessageBoxA函数的地址，因此GetProcAddress函数的第二个参数为“MessageBoxA”，因而key = MessageBoxA xor 固定字符串。

后面还有最终password的计算方法，但是到这里有了name和key就已经可以让程序自动弹出password了。