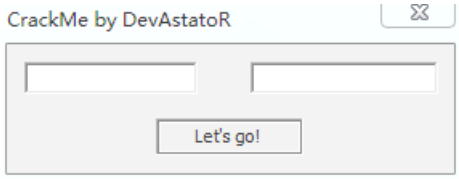
Reverse step1 writeup

原创

zh_explorer 于 2015-04-24 21:54:41 发布 784 收藏

分类专栏： hduisa内部平台writeup 文章标签： ctf reverse writeup

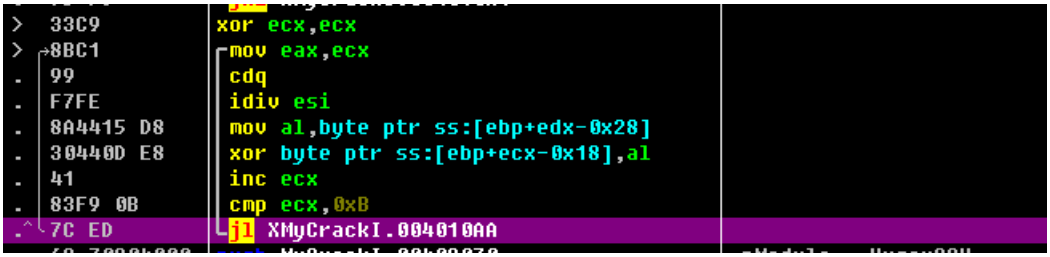
不要吐槽题目的名字，发题目的就是这么取的=,=
某天半夜出现在协会平台里面的Reverse简单题。这几天很忙，就随便随便写写这题的writeup。



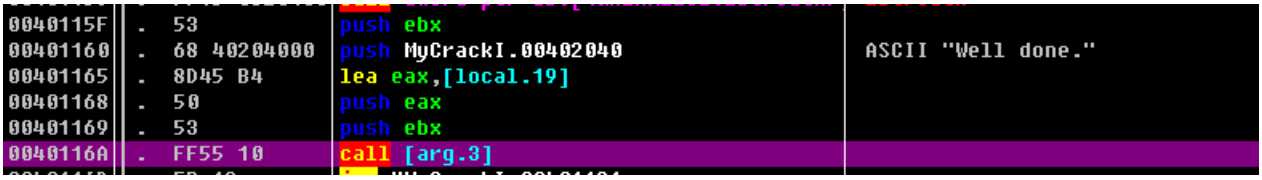
界面很简单，两个edit框和一个按钮。直接丢进od。看这紧凑的代码估计是直接用汇编写的。程序很简单，不像高级语言编译的程序，没有一点多余的代码。结合hint：Do you know SendMessage ?很快就可以发现异常的地方。

把第一个框的输入减去0x200E4作为SendMessage的消息。脑补0xD的WM_GETTEXT消息。算出要输入的参数是”131313”好吧，这随意的参数很有某人的风格=,=。

继续向下，SendMessage消息得到第二个edit框的字符，然后加密。



把输入前11个字符和0018FA24 24 0B 15 1C 13 0A 04 36 06 17 2F亦或。然后作为参数调用GetProcAddress。找找返回的地址在哪使用。



这里，看这4个参数再次脑补MessageBoxA。反向亦或得到输入参数information输入，自动弹出flag

程序会根据两个输入框的输入动态计算出flag，所以强行用od更改流程会弹出错误的flag，只有正确的输入才能得到正确的flag。