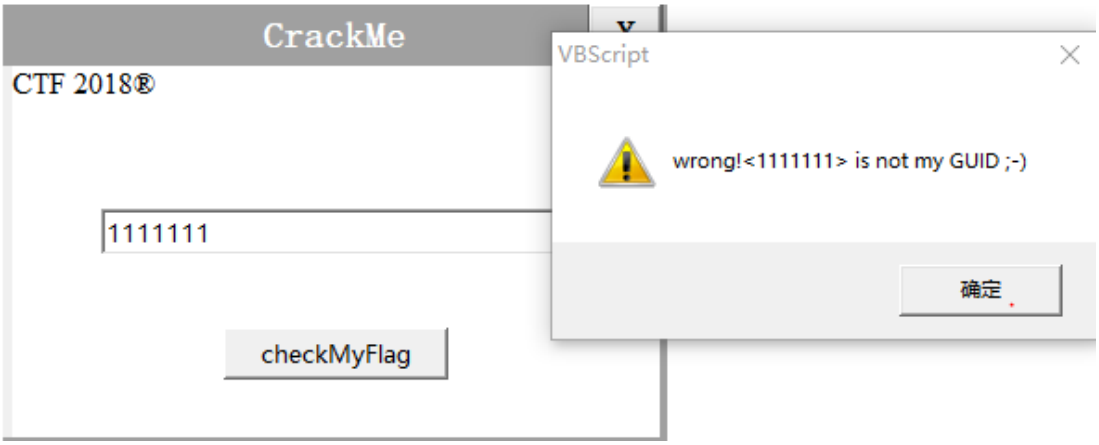
第十题 wp

0x00

本 wp 根据大佬 wp 复现

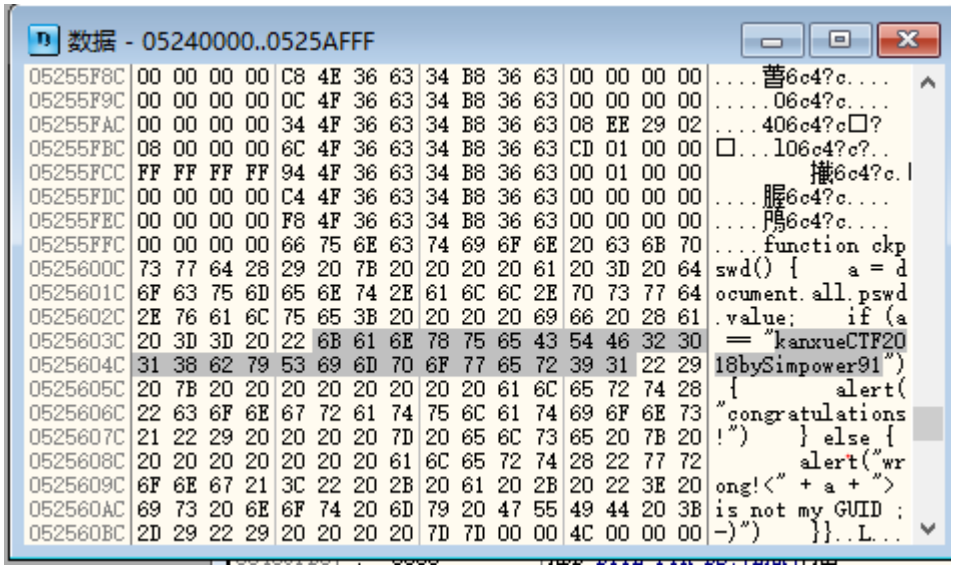
0x01 动态调试法

动态调试主要的优势就是可以实时的观察程序的运行情况
使用 OllyDbg 对程序调试，将程序用 od 打开，然后 F9 运行，弹出对话框。是 VBscript 脚本



思路就是逆向工程的思路，根据结果，往回倒推。就是直接找字符串，弹出的对话框里面的字符串。

在内存中，寻找“is not my GUID”，可以找到如下结果



“is not my GUID”出现之前，有一个简单验证，判断输入的值 a 是否和 flag 相等，直接输入 flag，可以通过