《漏洞利用及渗透测试基础》实验报告

姓名： 许健 学号：2013018 班级：信安班

**实验名称：**

格式化字符串漏洞

**实验要求：**

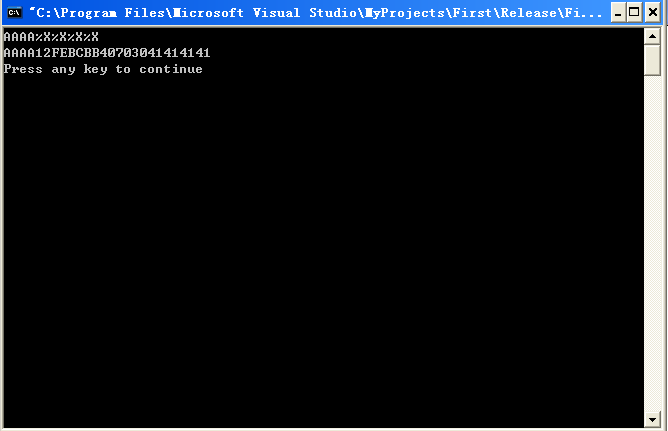
以第四章示例4-7代码，完成任意地址的数据获取，观察Release模式和Debug模式的差异，并进行总结。

**实验过程：**

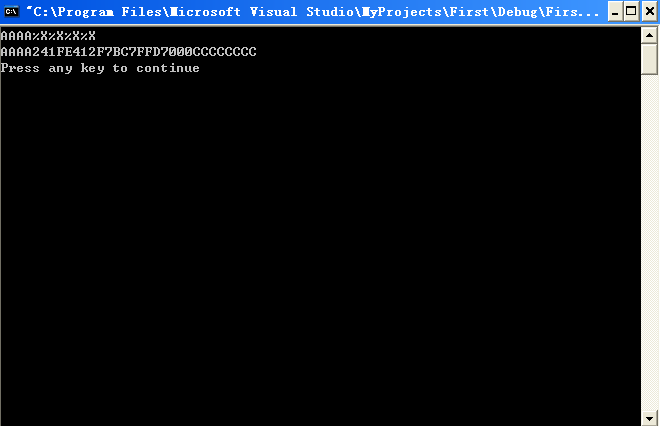
1. **运行结果**

编译后运行，输入AAAA%X%X%X%X

在Release模式下输出结果:（41414141对应的是字符串AAAA）



在Debug模式下输出结果:

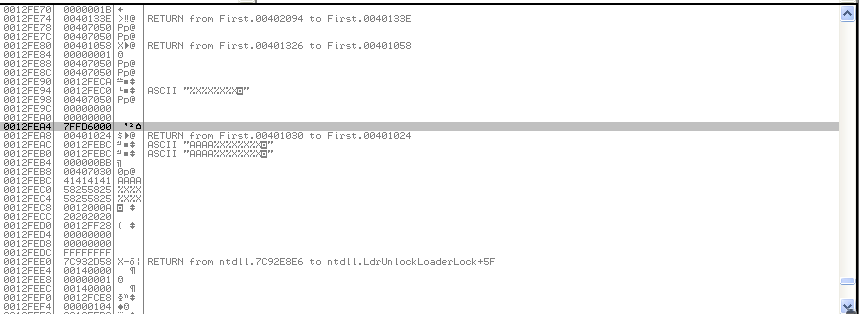


1. **差异原因**

Debug模式和Release模式的栈帧结构：

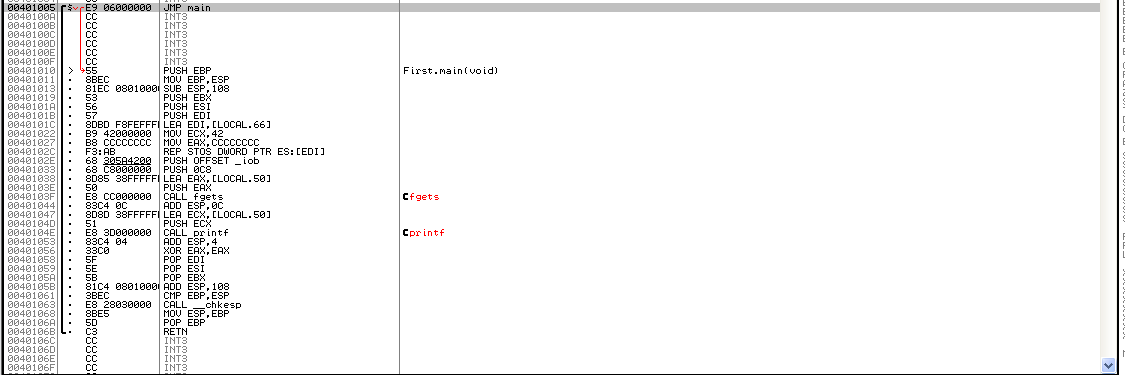
Release模式下，程序会考虑执行的性能，栈帧中并没有将寄存器也压入栈中，仅仅在main函数return语句前有add esp XX恢复栈的结构。

可以使用ollydbg看到Release模式下的堆栈空间：

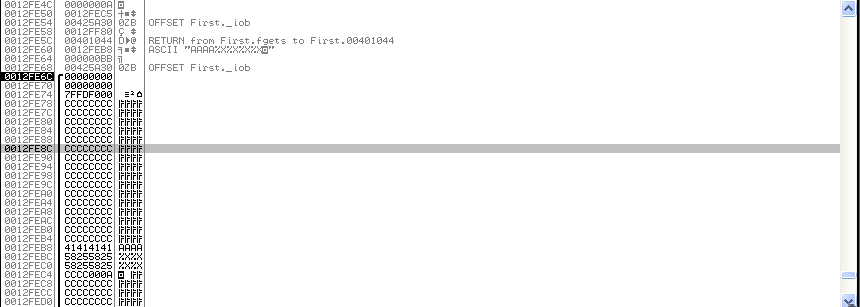


Debug模式会开辟足够大的栈帧空间来初始化，中间用CCCCCCCCh填充，要读到str的地址，需要很多的格式化字符。

Debug模式栈帧分配0x108空间



Debug模式下的堆栈空间（ollydbg调试）：可以看到用CCCCCCCCh填充的部分



1. **读取任意地址**

在Release模式下，如果将AAAA换成地址，第4个%x，换成%s，就可以读取参数指定的地址上的数据了。

比如我们输入：AAAA%x%x%x%s

这样就构造了去获取0x41414141地址上的数据的输入。

**心得体会：**

了解Debug和Release模式程序组织栈帧的不同，以及如何利用格式化字符串漏洞实现任意地址的读取访问