《漏洞利用及渗透测试基础》实验报告

姓名：沙璇 学号：1911562 班级：信息安全

**实验名称：**

格式化字符串漏洞

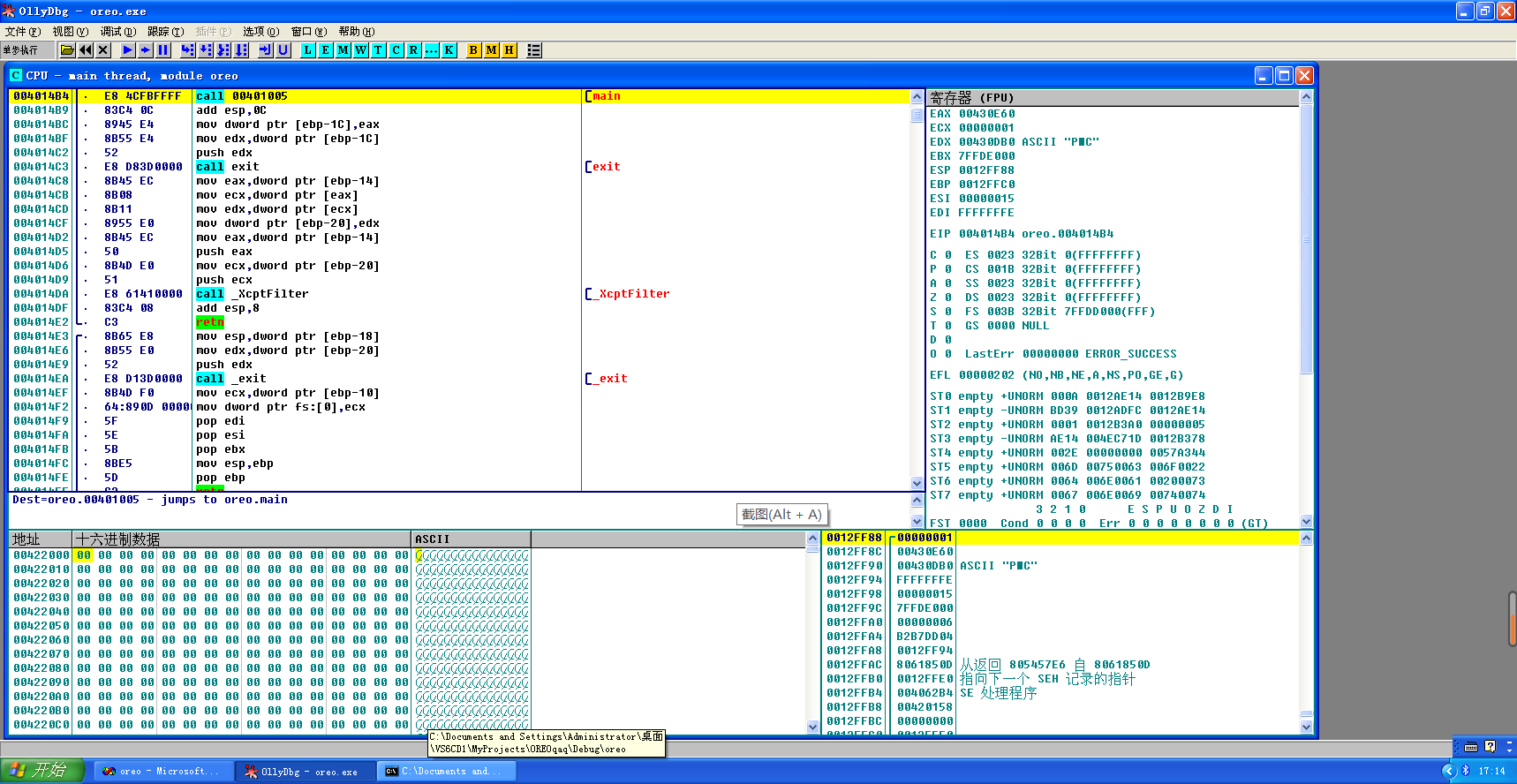
**实验要求：**

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

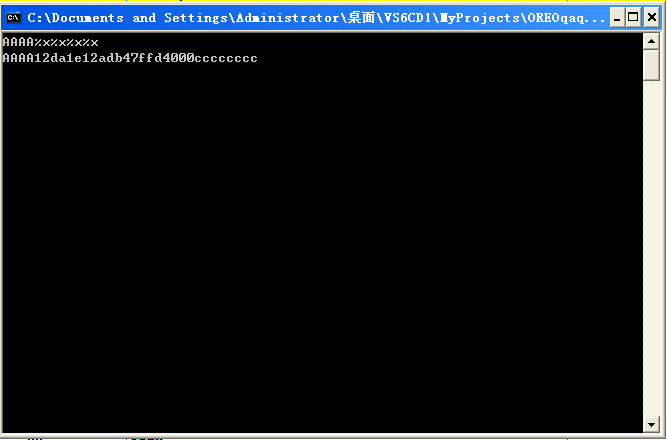
**实验过程：**

Debug模式：

进入ollydbg中程序的main函数

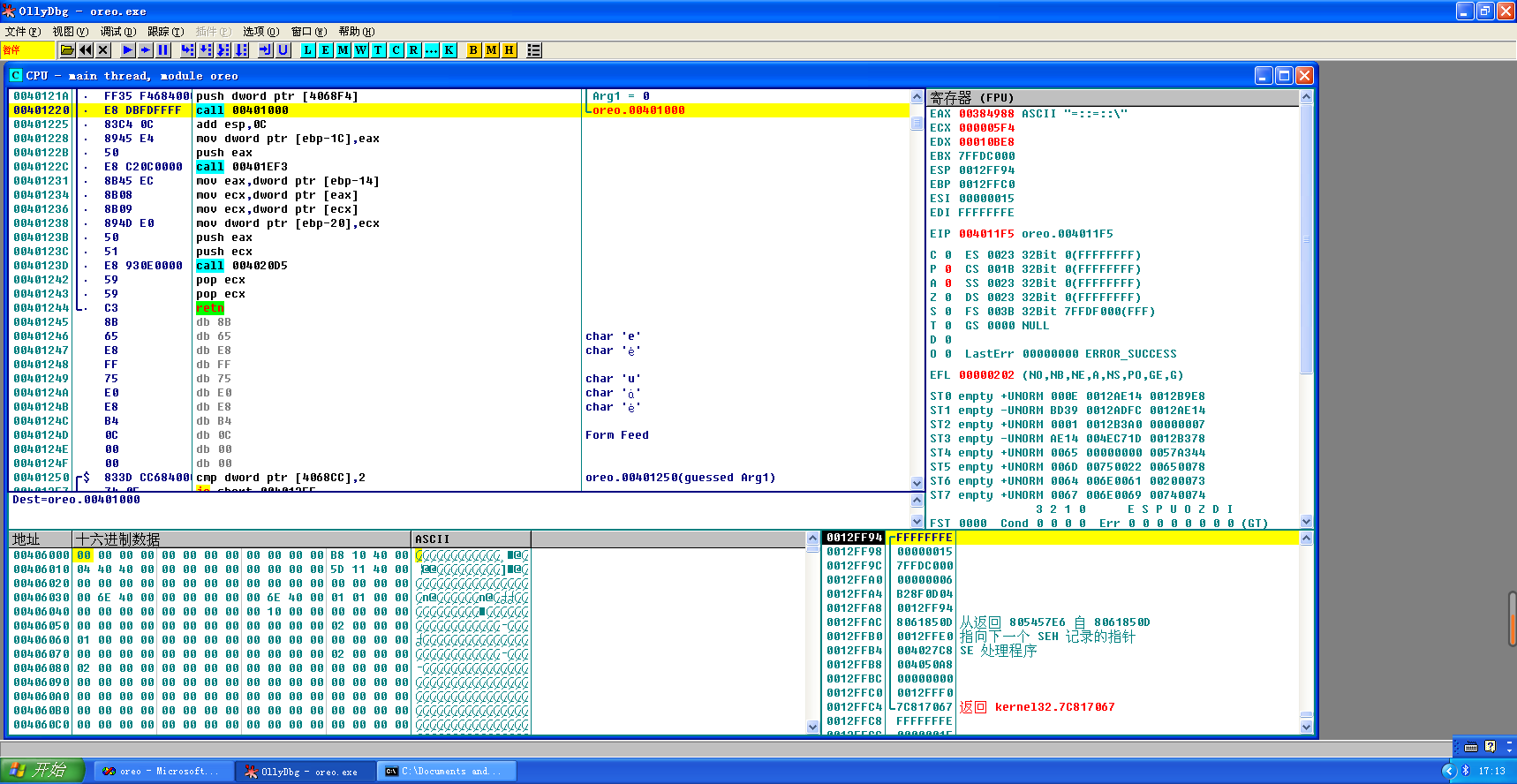


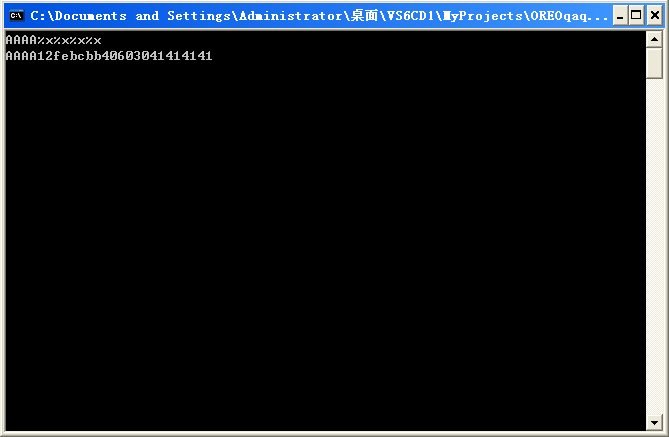
按要求输入“AAAA%x%x%x%x”，得到如下结果：



Relase模式：

进入ollydbg中程序的main函数，

按要求输入“AAAA%x%x%x%x”，得到如下结果：



Relase与Debug模式的区别：

Relase模式中程序代码更加简洁紧凑，不包含调试信息，显然在体积和性能方面都得到了一定优化；Debug模式保存了各种调试信息，更加倾向于为开发人员服务，提供强大的应用程序调试功能。

**心得体会：**

考虑栈帧状态，参数入栈后， 通过%x 依次读参数下面的内存数据时，很快就读到了原来函数的局部变量 str 的数据了。 如果将 AAAA 换成地址，第 4 个%x，换成%s就可以读取任意内存地址的数据。