《格式化字符串漏洞》实验报告

姓名：汤清云 学号：2013536 班级： 1075

**实验名称：**

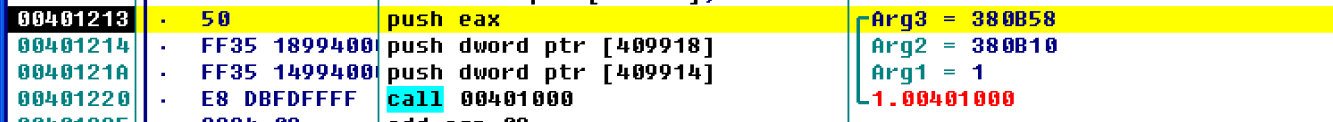
格式化字符串漏洞实验

**实验要求：**

根据第四章示例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. Release模式汇编代码



此处的arg1=1即为源代码中argc。



00401000即主函数入口。



Release模式下没有栈帧的切换，故不将ebp入栈，而直接将esp抬高200字节，只为局部变量声明了空间（即源代码中str声明空间大小），再将此时esp的值（0012FEBC）赋值给eax



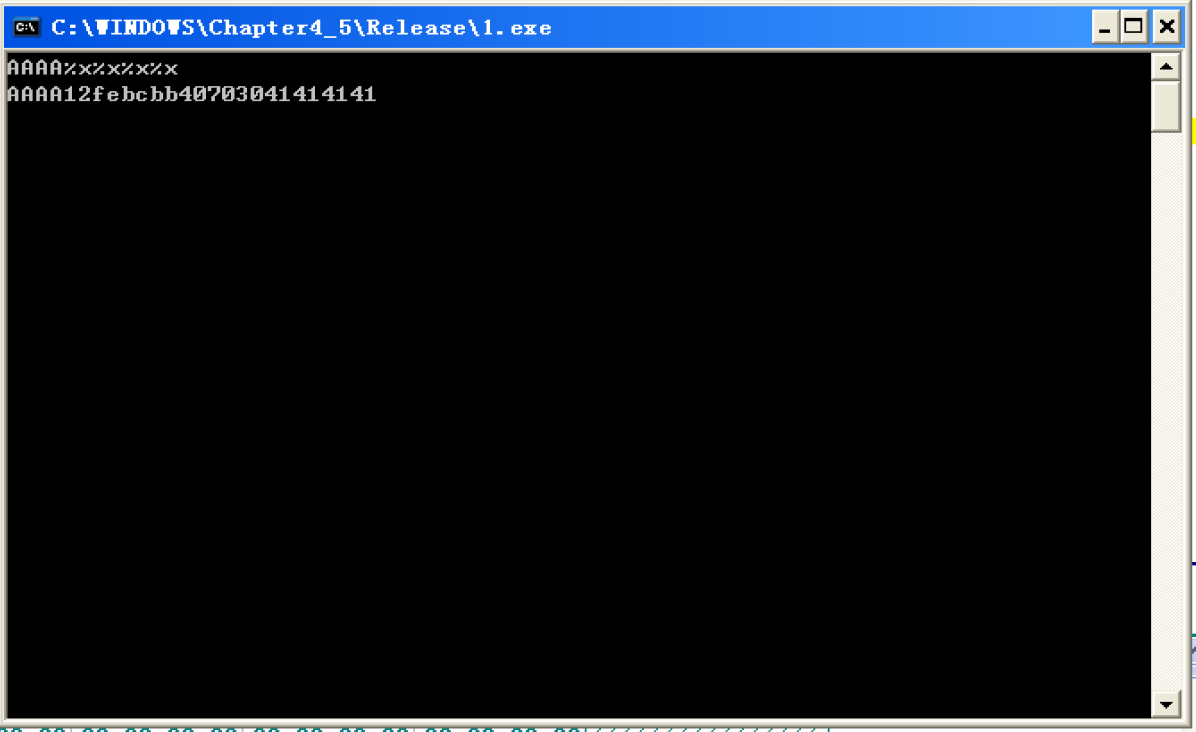
将地址，立即数，eax寄存器入栈，此时栈顶（0012FEB0）存储内容为抬高后的esp地址，也就是要输入的字符串的地址（0012FEBC）



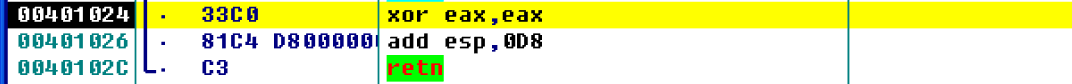
调用fgets函数，输入字符串“AAAA%x%x%x%x”



将字符串地址赋给ecx，此时ecx存储值为0012FEBC，再次将ecx压栈，即此时栈中存储了两个字符串地址。



调用printf结果如上图，可以得知打印出结果依次为AAAA（字符串本身），%x依次打印出栈中接下来的字符串地址，之前压入的变量

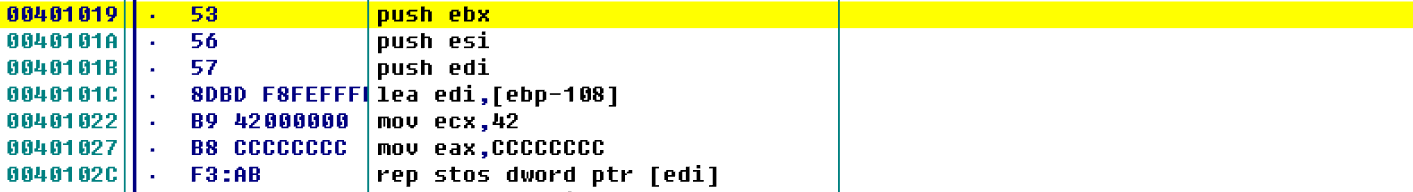


将eax清空，再将esp恢复成原来的地址（即之前所有压入栈中的变量、地址等全部清空）之后return。

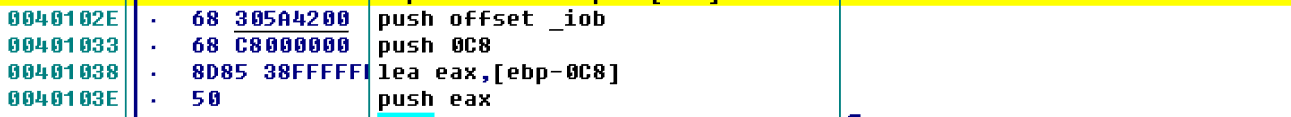
2. Debug模式汇编代码



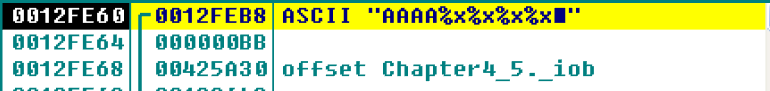
栈帧初始化，将新栈帧设置为264大小。



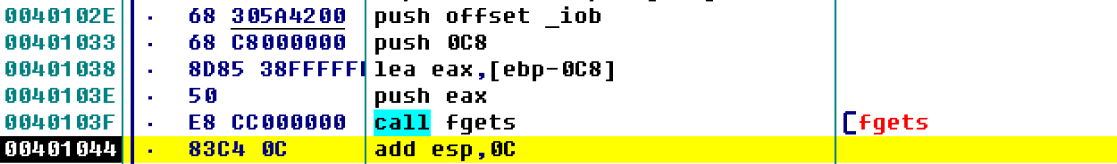
存入原栈帧相关信息，并将栈内空间初始化为CCCC。EBX在栈内地址为0012FE74，ESI在栈内地址为0012FE70，EDI在栈内地址为0012FE6C。



初始化结束，将栈帧存入200位空间后的地址赋值给eax。



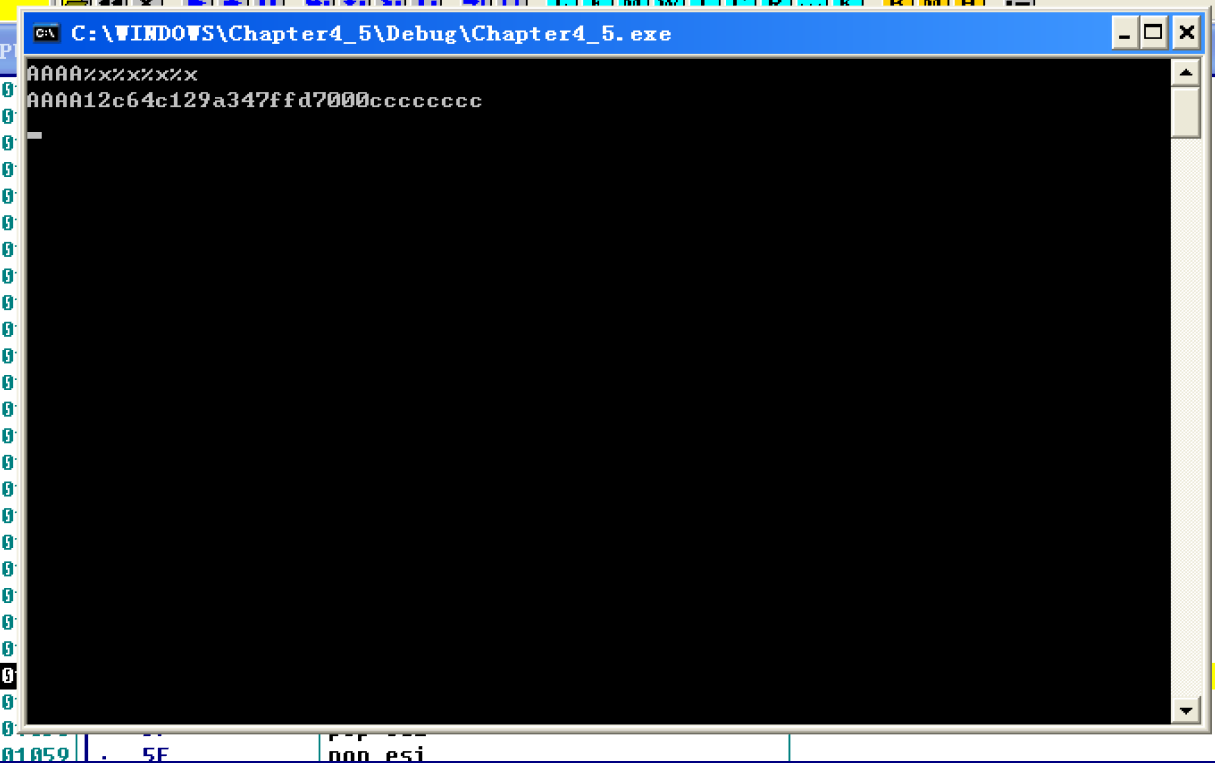
在调用了fgets函数并输入字符串后，在地址为0012FEB8的地址上存放着我们所输入的字符串AAAA%x%x%x%x



调用完fgets后恢复esp指向，将其+12（对应offset\_iob,0C8,eax）



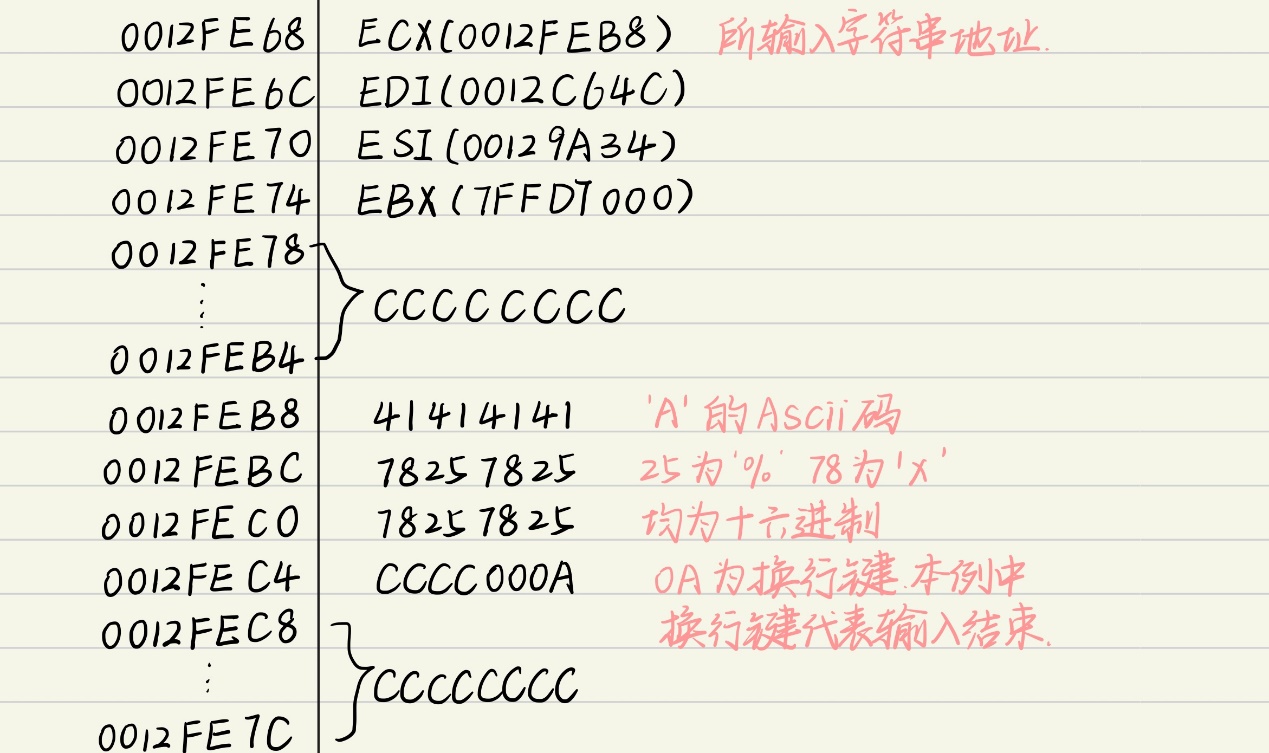
[ebp-0C8]即为我们所输入字符串“AAAA%x%x%x%x”的地址，这两条语句将字符串存储地址压入栈内，位于EDI的上方，地址为0012FE68



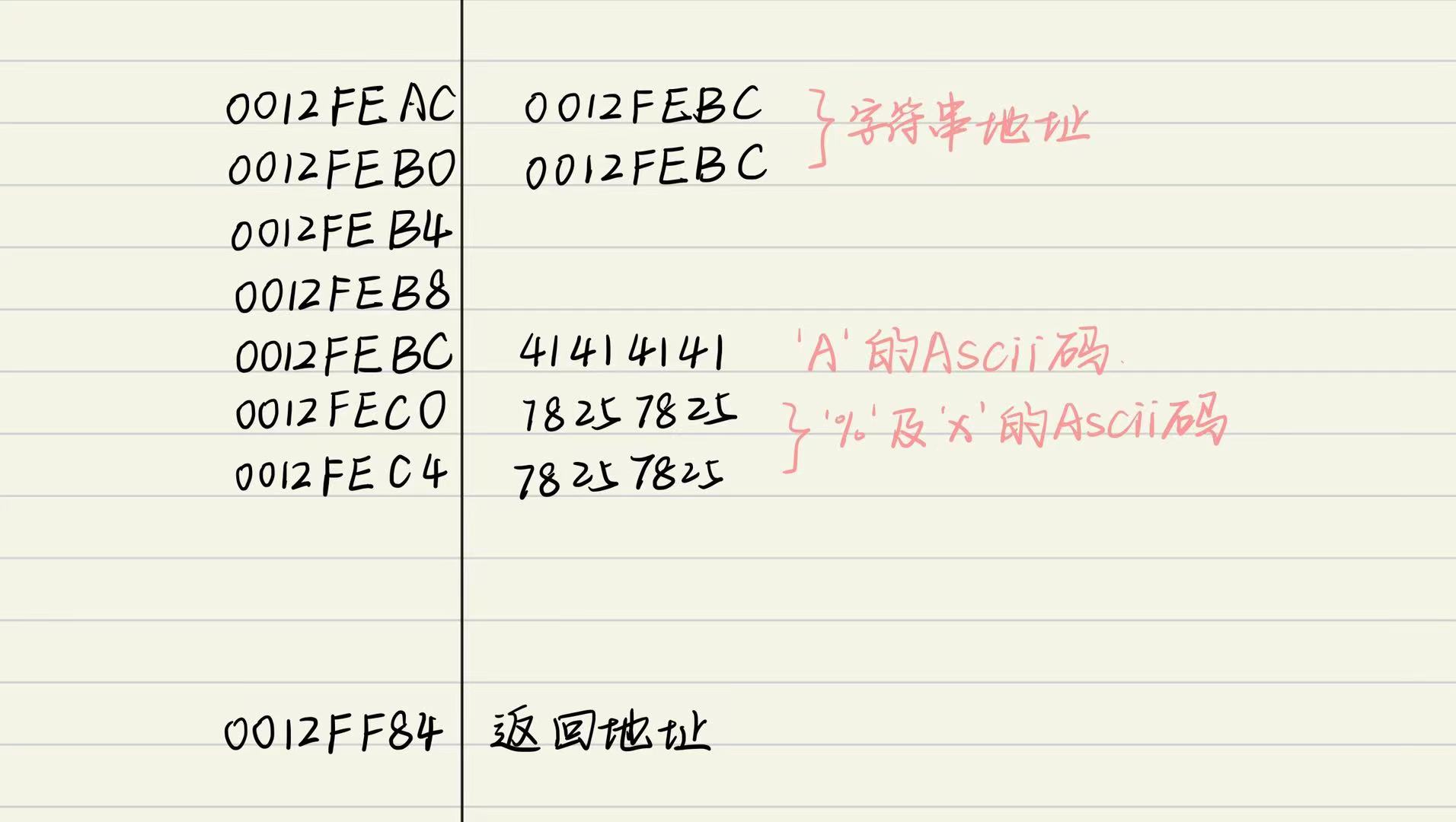
在调用printf函数时，会打印出我们所输入的字符串AAAA，遇到%x时则会自动打印出栈中接下来的地址所存放内容（即依次打印EDI，ESI，EBX的存储内容以及初始化内容CCCCCCCC）

3. 总结

Debug模式下栈内容为：（左为地址，右为存储内容）



Release下地址如下：



**心得体会：**

通过实验更加深入得了解了Release和Debug模式下栈帧的区别。Debug下栈帧会随着调用函数而不断调整，ebp有入栈出栈操作，但在release模式下ebp不会变化。