《漏洞利用及渗透测试基础》实验报告

姓名：王亦辉 学号：2310764 班级：计科1班

**实验名称：**

**堆溢出漏洞下的Dword Shoot攻击**

**实验要求：**

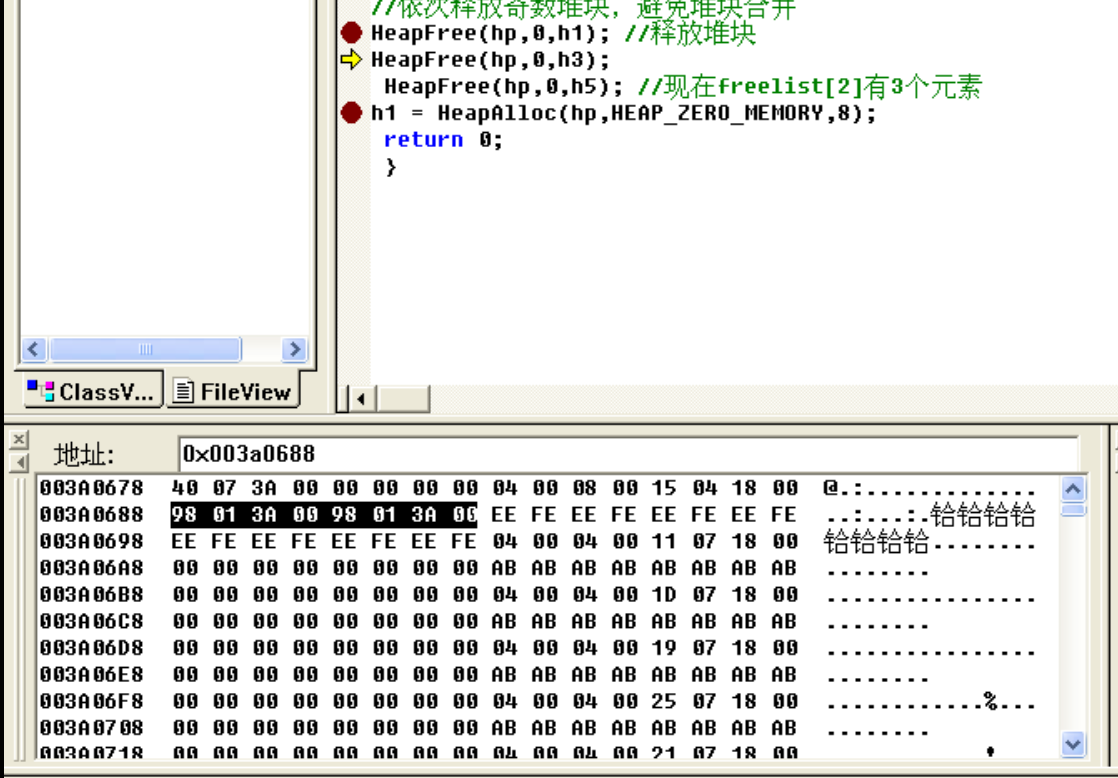
**以第四章示例4-4代码为准，在VC IDE中进行调试，观察堆管理结构，记录Unlink节点时的双向空闲链表的状态变化，了解堆溢出漏洞下的Dword Shoot攻击。**

**实验过程：**

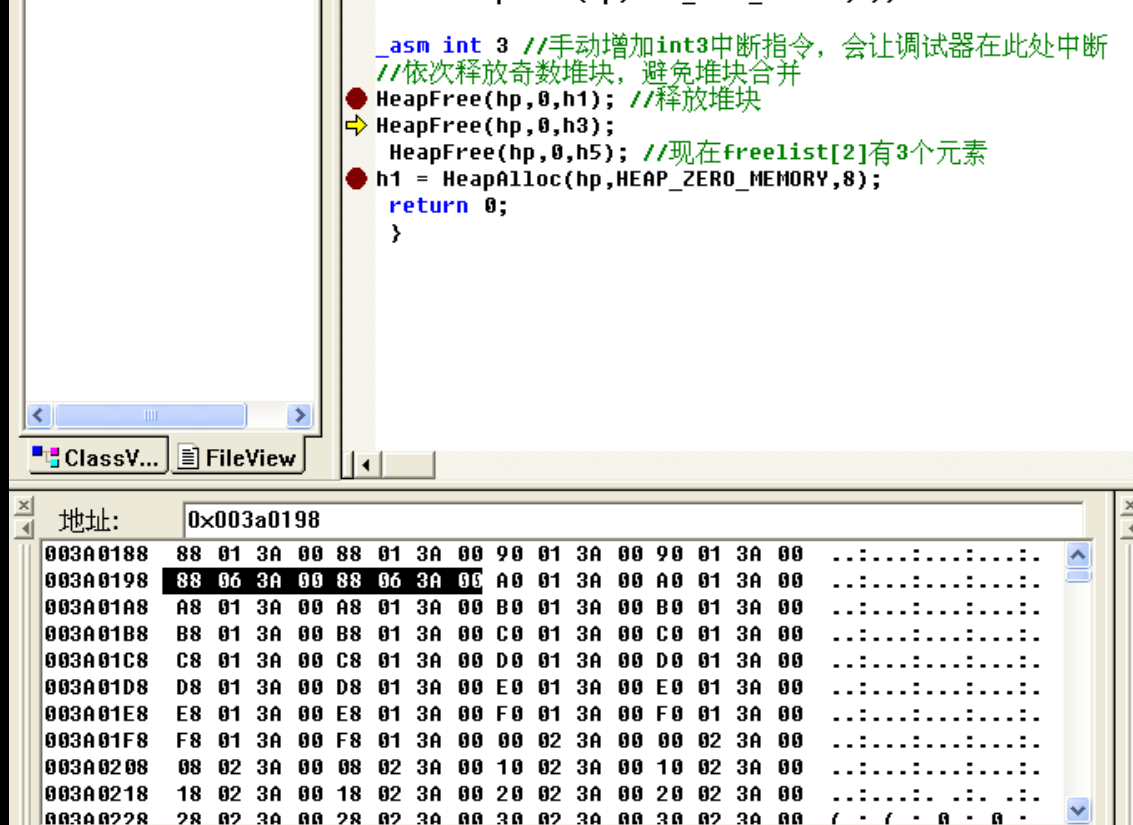
1.观察堆管理结构

1): h1释放

可以看到h1被释放后，他的flink ,blink 都指向 freelist[2]

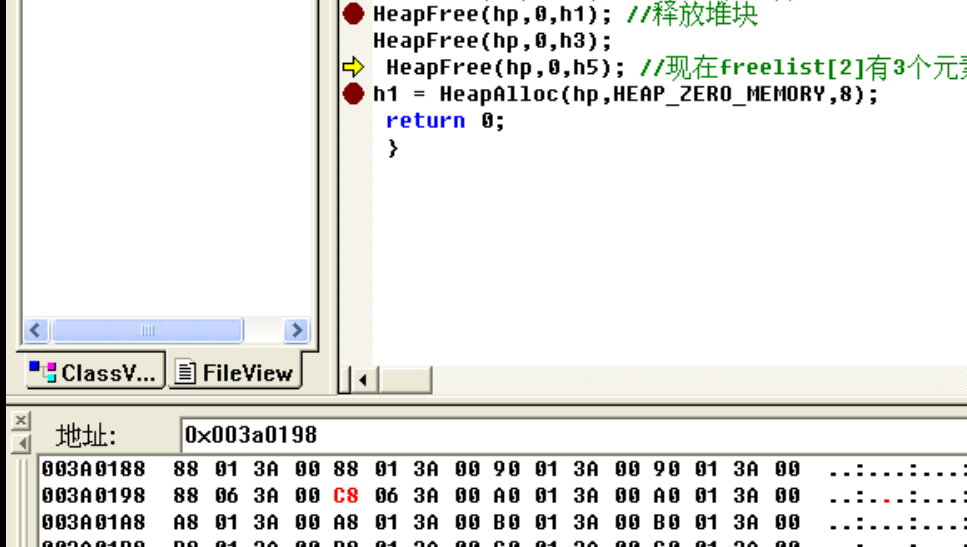


可以看到 freelist[2]的前向后向指针都指向0x003a0688，也就是刚释放的h1 堆块。

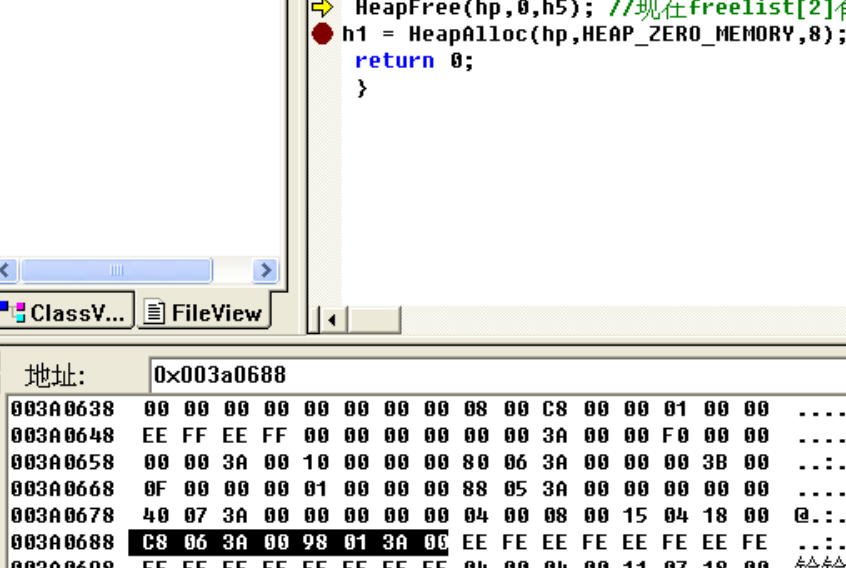


2）：h3释放

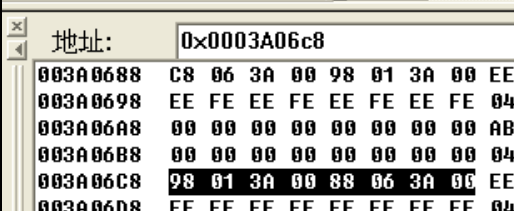
释放h3 之后，freelist[2]里的一个指针指向h3，说明h3 被链入freelist[2] 对应双向链表的尾部



查看h1 的块首，发现有一个指针也改成指向h3了

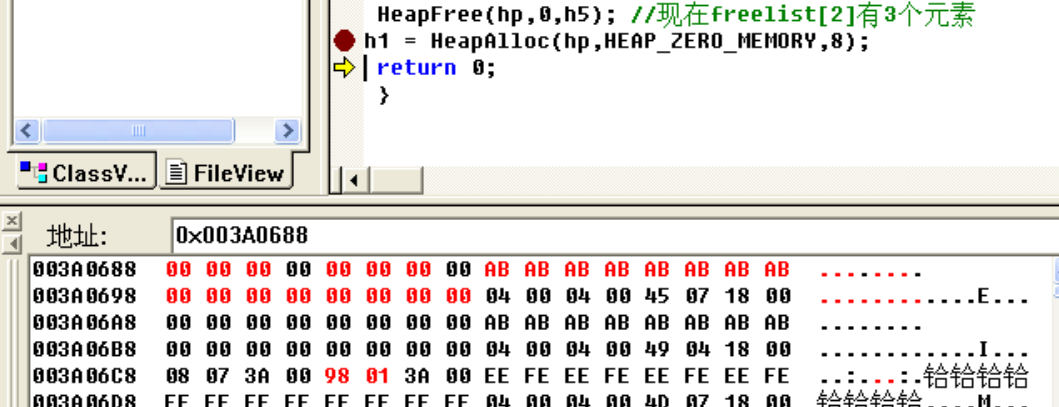


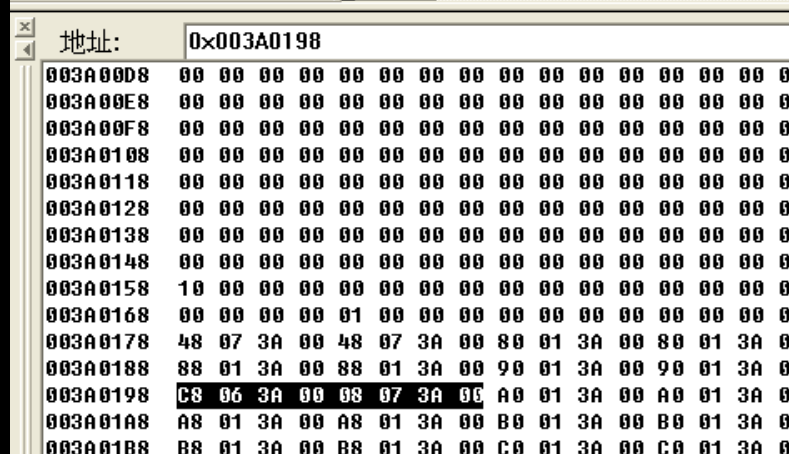
在h3 的块首，则是一个指向h1，一个指向freelist[2].



2. unlink时双向链表的变化

可以看到，将原来分配给h1对应的空闲堆块从freelist[2] 里释放出来之后，它的后一个空闲堆块h3的前向指针改成指向freelist[2]了，而freelist[2]的后向指针改为指向h3。也就是说如果通过堆溢出，修改了h1 中的blink和flink，在unlink的时候，由于指针的更改，就会把 blink指向的位置写入 flink 的值， 把flink 所指往后4字节的位置（原本是要更新flink所指的堆块的blink，而blink指针是在flink指针之后的）写入blink的值。





**心得体会：**

一些很简单的指针操作也能被利用，作为攻击方法。