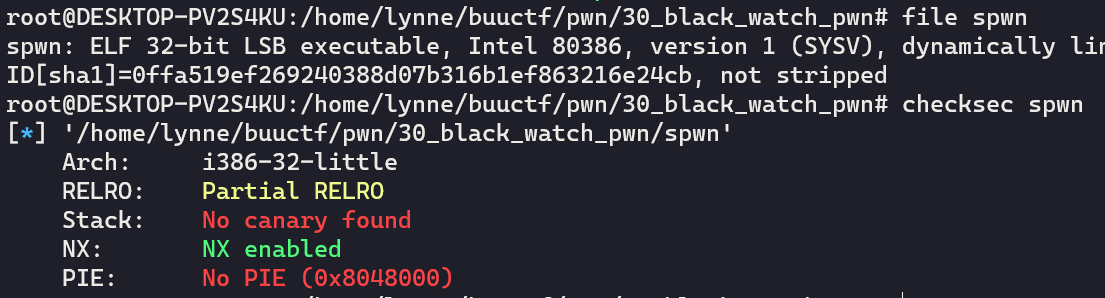
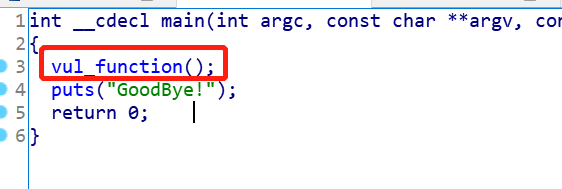
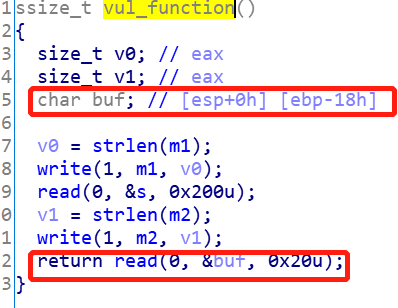
首先看文件：

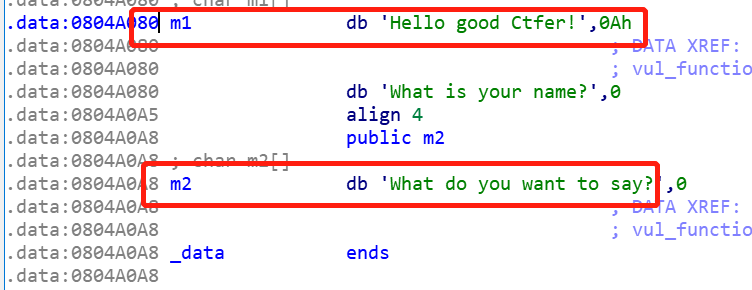


Main函数：





发现char只能多溢出8个字节，然后m1和m2分别是：



溢出的字节有限，所以考虑使用栈转移攻击。

每个函数结束调用的时候，会leave;ret。这其实代表了三条指令：mov esp ebp; pop ebp; pop eip。

因此，可以给一个假的ebp，使其指向bss段或data段。

然后，再执行一次leave;ret之后，栈就会被迁移到bss段或data段上。

这个时候，可以构造rop链。

本题的思路是：

首先迁移一次栈到s的地址，通过write函数，泄露libc的基地址；然后回到main函数，再迁移一次栈，执行system sh。即可获取shell。

需要注意的是：read不要用sendline。用send！！！

