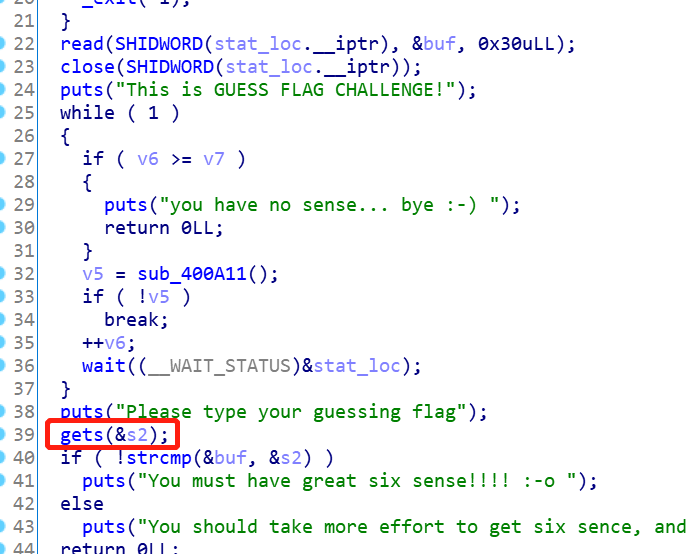


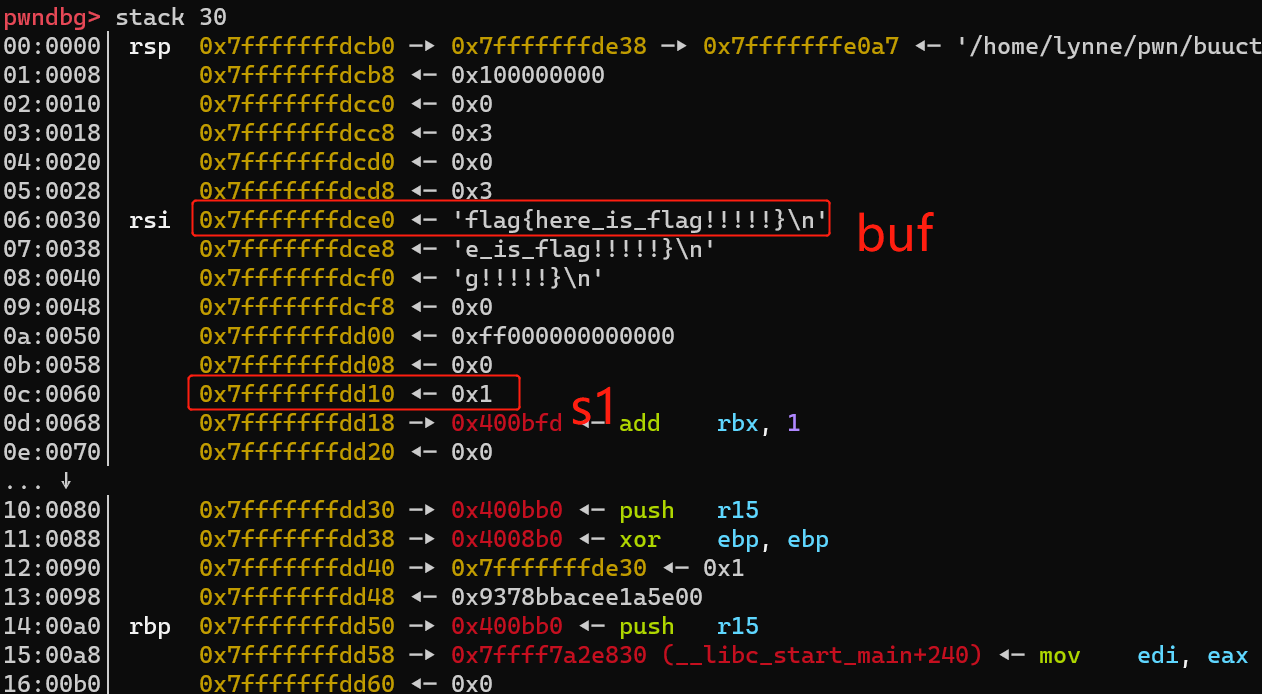
利用stack smashing

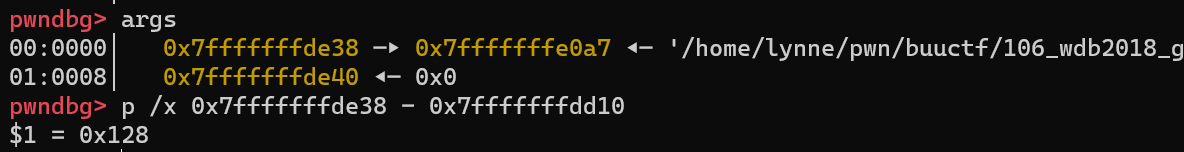
首先泄露got表中某函数的地址，得到libc的地址

然后通过libc中的\_\_envrion得到栈地址

然后计算得到buf的地址，读取flag

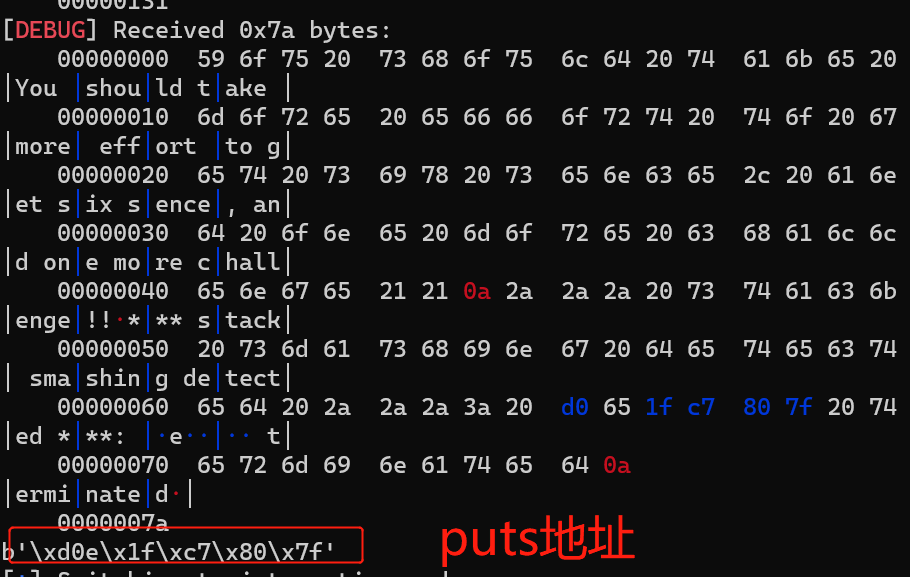


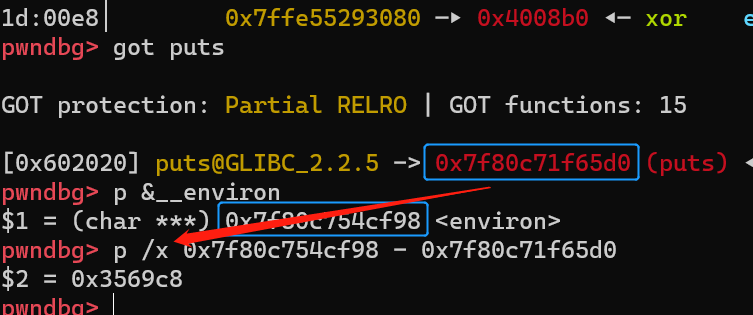




和args[0]之间的偏移为0x128

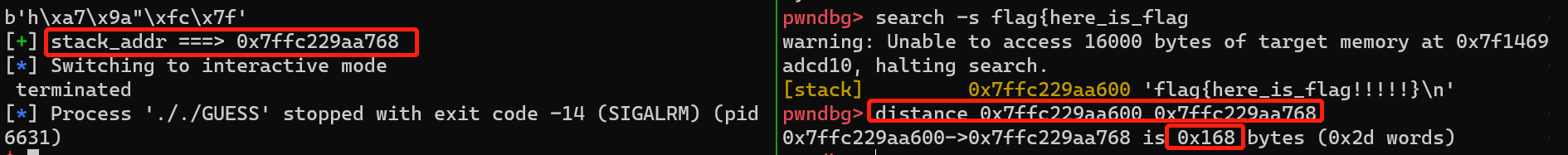
第一次stack smashing





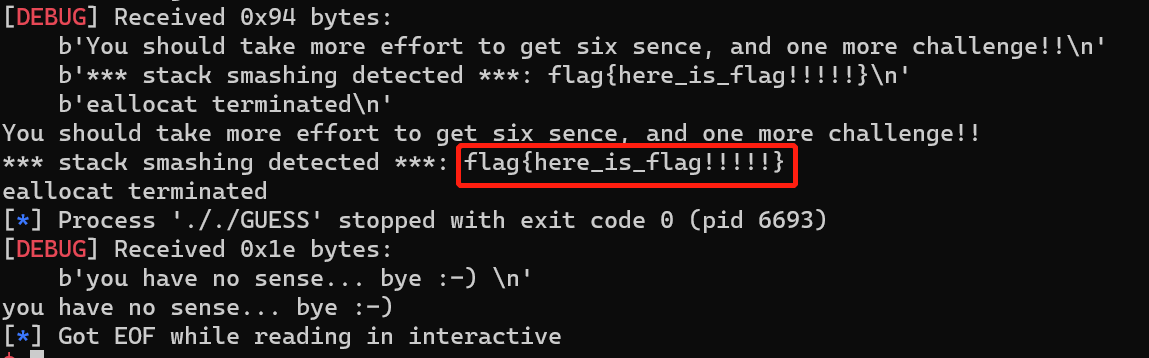
与\_\_environ之间的偏移为0x3569c8

第二次泄露libc的地址



计算得到buf的地址

第三次泄露处buf处的内容



然后打远程：

