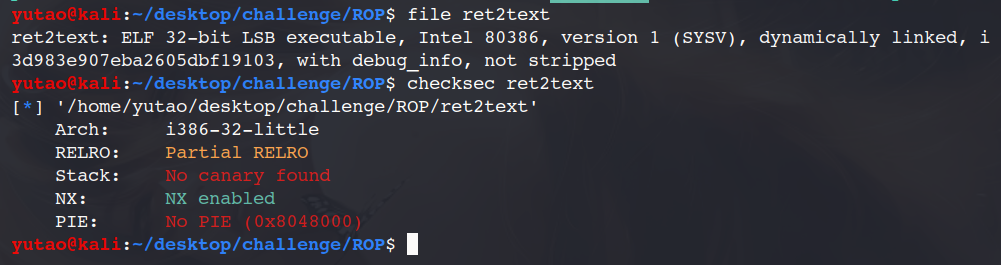
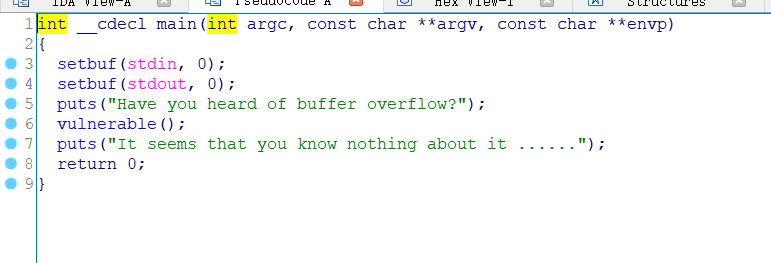
# Ret2text

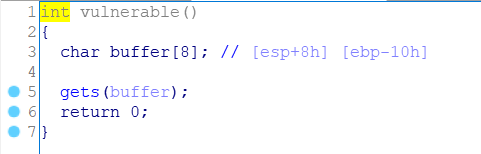
首先file和checksec一下：



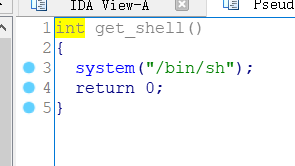
ida打开：



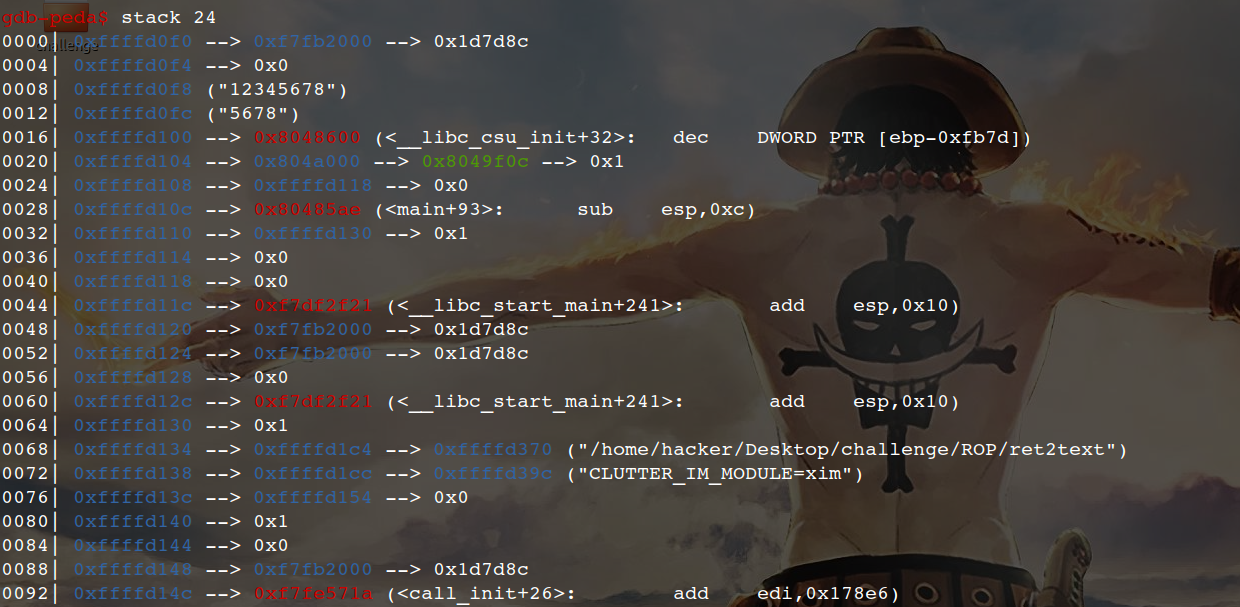
观察到有个vulnerable()函数：



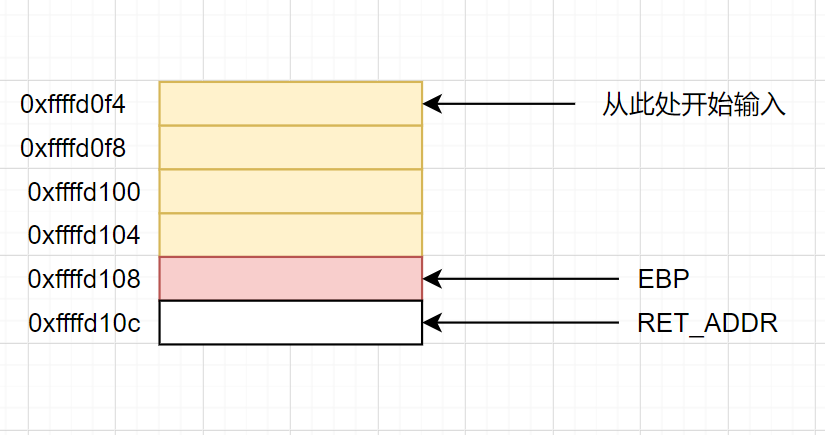
还有个后门函数：get\_shell()



gdb打开，main处下断点后跟进，输入12345678后查看stack：

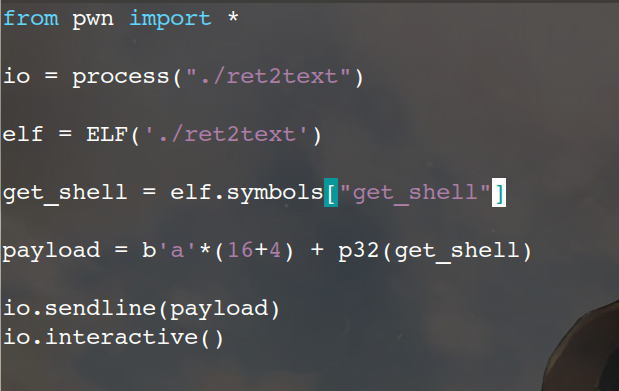


此时ebp= 0xffffd108,



将黄色与红色部分全部覆盖后填入get\_shell()的地址。

exp如下：



getshell：

