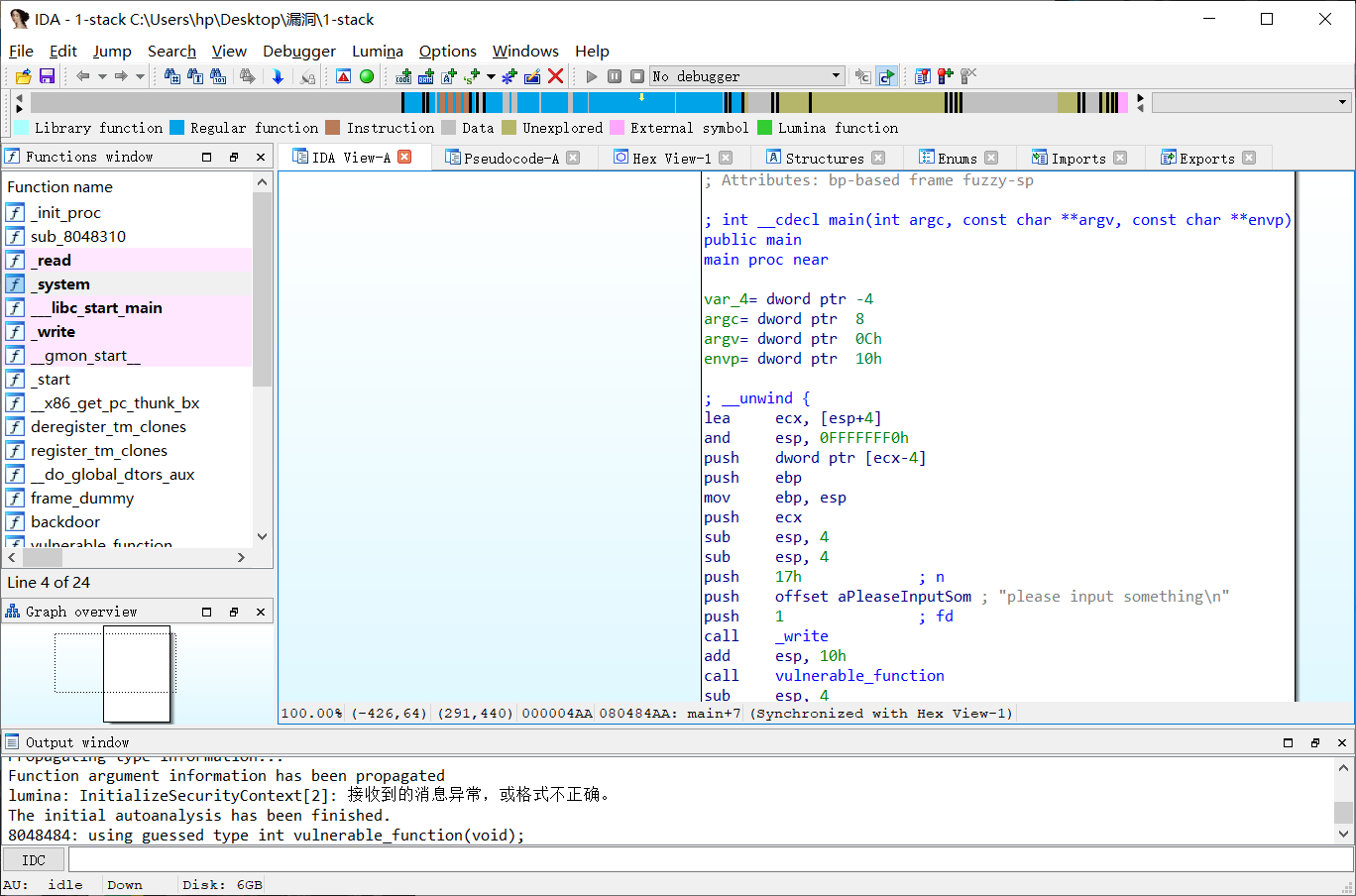
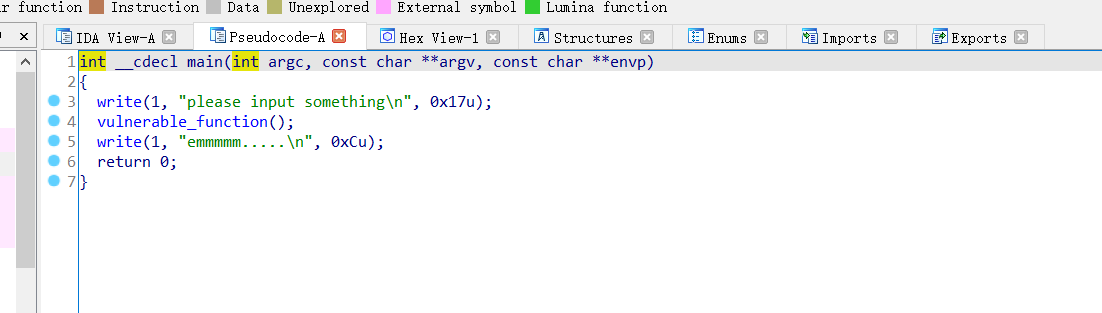
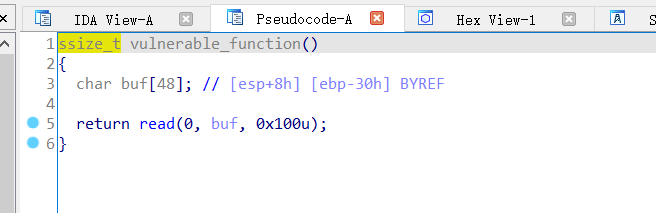
Ida静态查看



按F5

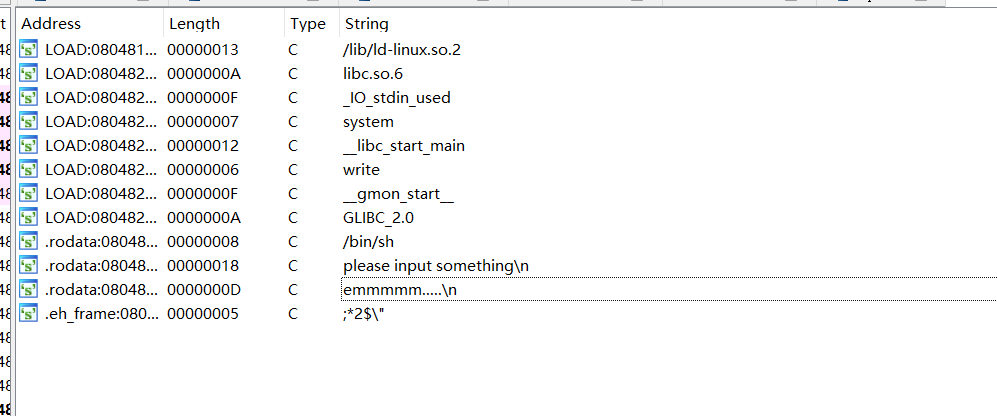


双击关键函数

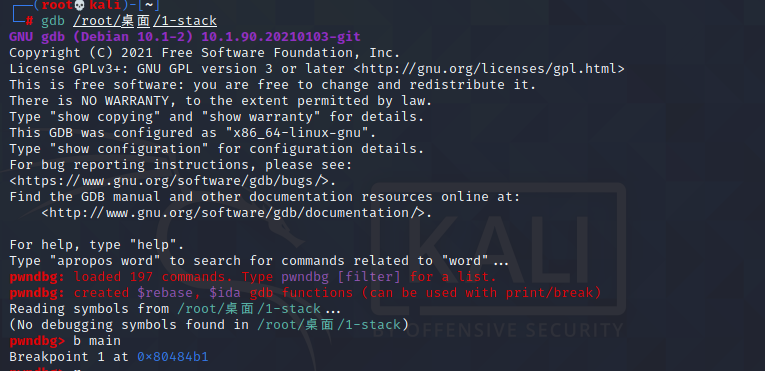


按Alt+7

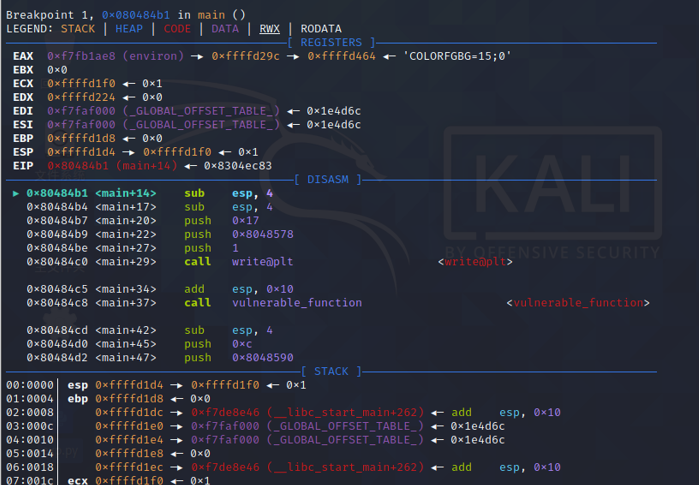
找到system，双击打开

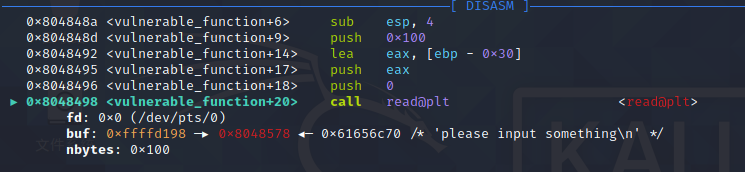


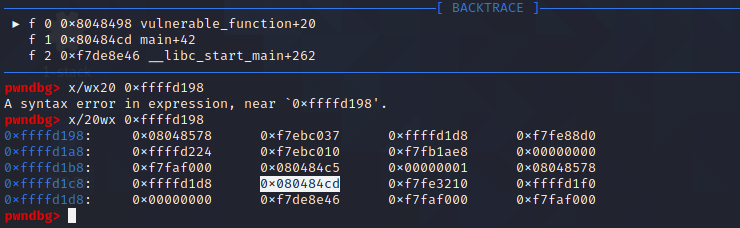
动态分析Gdb打开动态调试，在main函数下断点



单步运行，来到function函数，找到buf参数的地址（0xffffd198）







计算偏移地址，0xc8-0x98+0x4=0x34，编写exp，再覆盖上shell地址即可：

