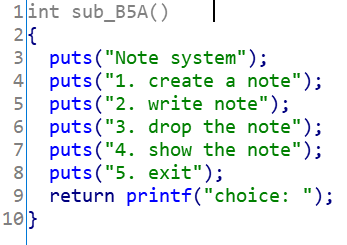
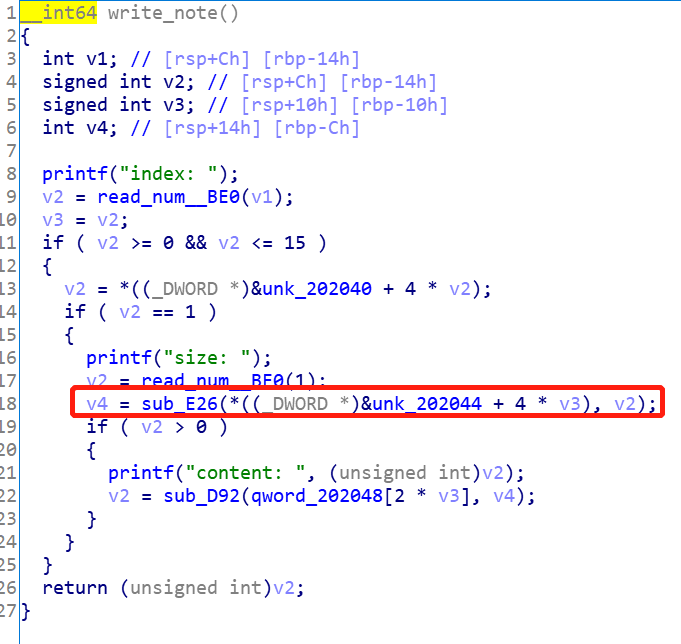


保护全开呢。。。

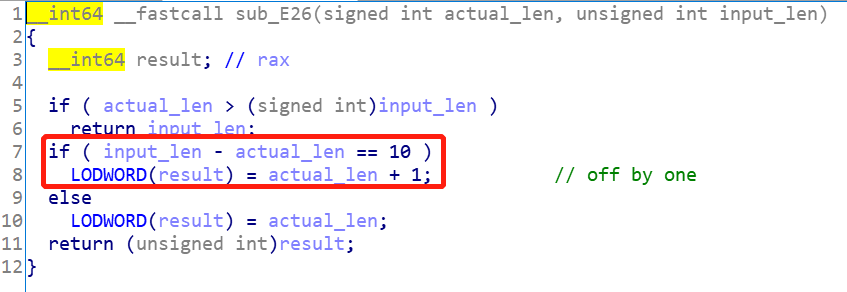
菜单题



漏洞点在write\_note函数：



这里会对输入的size做一个校验，但是存在一个off by one的漏洞。



只要输入的size等于原来size+10，就可以多输入一个字节。控制chunk后向合并。

然后泄露libc的基地址，然后覆盖malloc\_hook。

这里还是要覆盖realloc\_hook，通过relloc来调整栈帧，出发one\_gadget!

