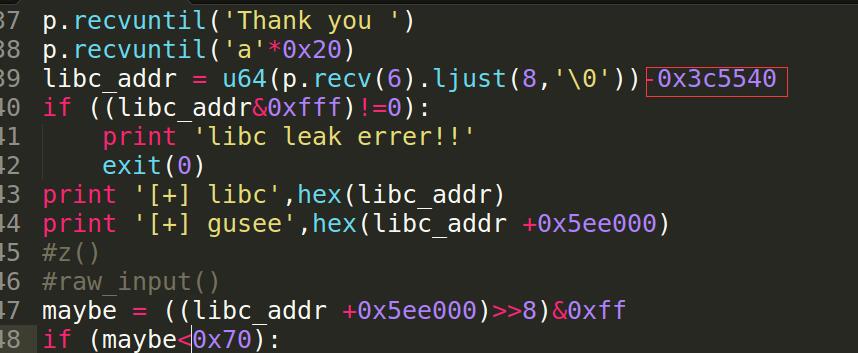
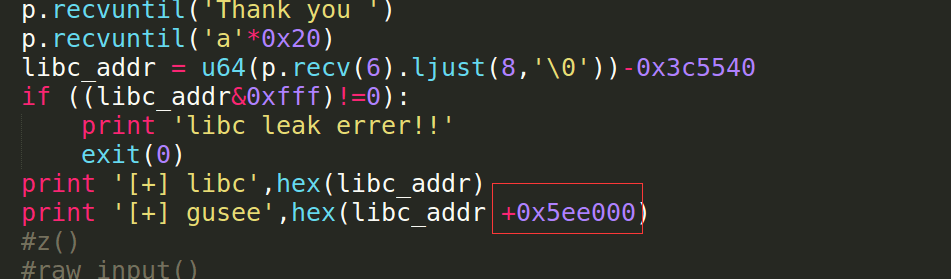
1. 泄露libc的是std\_err的地址，有时候泄露不对不知道为啥



1. 这个偏移是由libc基址 预测mmap 远程不一定一样



1. 思路是：将one\_gadget写入start那个vmmap块的0x20位置，伪造congratulation函数，改start那个地方为自己，利用congratulation函数触发system
2. maybe这个值只是一个字节 实在实在不行爆破多打几次 1/16左右的概率, 0x\*0这样的数, 比如0xb0 0x80