WP

白给

签到一下，打开文件夹发现给的.c，芜湖ida都不用，起飞!

```
if(num == "paSswOrd"){ //Do you know strcmp?
    printf("you are right!\n");
    system("/bin/sh");
} else {
    printf("sorry,you are wrong.\n");
}
```

如果`if(num == "paSswOrd")`不够明显的话，`//Do you know strcmp?`一定足够明显了。

num需要的是paSswOrd字符串的地址，好吧还是要ida，打开一看，好嘞，科学计算器换算成数字，直接nc，输入，不需要Python真好。

其实once我写了的，只是没交.jpg

once这题很明显的read溢出，覆盖返回值，但是发现程序崩溃，于是考虑开了pie，覆盖返回地址后两位。
返回地址在ida中的后三位是0x1bf，所以能覆盖的位置只有0x100到0x1ff，尝试覆盖为0x169从main开始执行，但是程序崩溃，盲猜setbuf可能不能重复执行，所以从0x1a9开始，会重新输出“only once”，vuln函数return的时候会输出buf的内容，碰到到'\x00'结束，我们的输入最后是'\xa9'，后面会跟上该处的真实地址，把它recv过来，可以得到程序的偏移。
然后考虑libc库的偏移，用printf函数泄露内存的内容，尝试发现第6个参数处，内存存储正好是我们的输入的字符串的内容，于是我们输入的前八个字节构造输出格式，然后后面跟上got表中printf的地址，来输出它的真实地址。
这里需要注意的是，“题目turn: ”的末尾是有空格的。
然后开始ROP了，ida发现源程序里面有`_libc_csu_init()`,第一反应是通用gadget。构造完成，发现不行但是gdb单步时候发现return跳转的第一个地址是对的。开始疑惑，然后发现是我的payload太长了。贼心不死的我，试着多次构造栈的数据，然后返回。但是读写权限出了点问题。然后听说可以onegadget？百度，我靠还有这个好东西，于是开整。
第一次因为turn：后面的空格导致偏移算错，卡了两个小时，之后条件不满足，卡了半个多小时，换了一个。时间只剩四十分钟。最后我发现程序没了反应，但是我随便输入不会结束，我怀疑是我条件没搞好，于是各种修改，在八点十五时候我想起来，我输入还不结束，但是没反应，是因为我是process，天崩地裂，试着撤回操作，拿到flag和大家哭诉。
这里提醒大家，做题一定要带脑子，做人也一定要长脑子，希望大家都能有脑子。