本题是一道非常规的格式化字符串，因为字符串在堆里面所以不能直接利用栈里面的格式化字符串进行任意写攻击，而是利用ROP链进行低位覆写

Printf打印之前的栈空间



* 首先修改0xffffceb8地址处的内容为0xffffce9c，这里需要修改最低的一个字节，偏移为1
* 然后修改0xffffce9c地址处的内容为0x80485ab，这里只需要修改最低的两个字节，偏移为1

具体payload查看exp

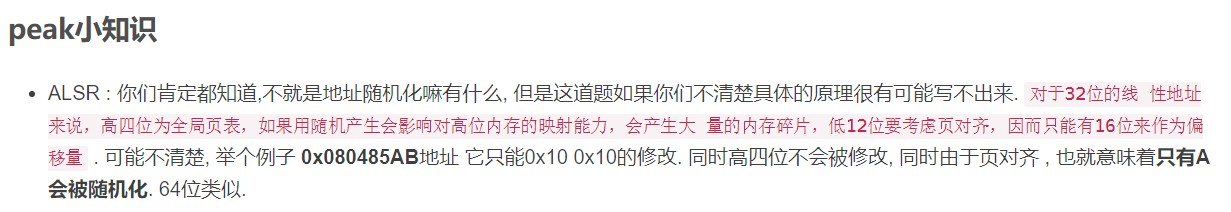
具体参考：

<https://www.cnblogs.com/LynneHuan/p/14535038.html#sub_80485c4>

ASLR地址不变位问题--未解决

这里面存在一个我不理解的问题，我看另外一个师傅博客里面

<https://blog.csdn.net/Y_peak/article/details/115327826>

写

首先按照此知识点在例子中0x80485ab高4位应该是0，低12位是5ab，不是中间的8048每次会被随机化吗?而不是a？

另外在自己动调时发现确实只有最低4位不变

0xffe0e95c  
0xffa309bc  
0xfff9a85c  
0xffaad80c  
0xfff9c5ec  
但我看动调的结果是高8位和低4位不变，其他位置发生改变