详细wp

<https://blog.csdn.net/mcmuyanga/article/details/113242453>

这里仅仅记录下我遇到的疑惑（已解决和未解决）

1. 一开始我按照32位程序的方法来做结果泄露libc就失败了，经过动态调试后发现是got表有\x00截断了输入payload，必须采用got表放后面的方法（已解决）
2. 后按照第一种方法还是泄露不了libc，但仅仅限于printf和sprintf（printf是我自己试出来的（本地可以，远程失败），sprintf是我看其他师傅博客了解到的），猜测是远程环境问题，必须用puts或strlen的got表，同理后面的任意地址写同样不能覆写sprintf和printf只能覆写strlen的got表（未解决）
3. 覆写got表时只能覆写低三字节，覆写低四字节失败，看师傅博客的意思应该是printf一次性无法输出太多字符导致失败（未解决）