先看题目：

We all make mistakes, let's move on.
(don't take this too seriously, no fancy hacking skill is required at all)

This task is based on real event
Thanks to dhmonkey

hint : operator priority

ssh mistake@pwnable.kr -p2222 (pw:guest)

连上去看一下：

```c
#include <stdio.h>
#include <fcntl.h>

#define PW_LEN 10
#define XORKEY 1

void xor(char* s, int len){
        int i;
        for(i=0; i<len; i++){
                s[i] ^= XORKEY;
        }
}

int main(int argc, char* argv[]){

        int fd;
        if(fd=open("/home/mistake/password",O_RDONLY,0400) < 0){
                printf("can't open password %d\n", fd);
                return 0;
        }

        printf("do not bruteforce...\n");
        sleep(time(0)%20);

        char pw_buf[PW_LEN+1];
        int len;
        if(!(len=read(fd,pw_buf,PW_LEN) > 0)){
                printf("read error\n");
                close(fd);
                return 0;
        }

        char pw_buf2[PW_LEN+1];
        printf("input password : ");
        scanf("%10s", pw_buf2);

        // xor your input
        xor(pw_buf2, 10);

        if(!strncmp(pw_buf, pw_buf2, PW_LEN)){
                printf("Password OK\n");
                system("/bin/cat flag\n");
        }
        else{
                printf("Wrong Password\n");
        }

        close(fd);
        return 0;
}
```

简单分析一下逻辑，就是先读取 password 里的内容放入 pw_buf 里，然后让用户输入

Pw_buf2，让其与 **1** 异或后再和 pw_buf 比较，成功则得到 flag

但是这个程序存在漏洞：

```
    int fd;
    if(fd=open("/home/mistake/password",O_RDONLY,0400) < 0){
            printf("can't open password %d\n", fd);
            return 0;
    }
```

=和<的优先级不同

<的优先级大于=

同时，open 打开文件无论如何都不会返回小于 0 的数

则先进行比较 故 open（）<0 这句为 0

然后进行赋值 fd=0

而我们知道 fd=0 为标准输入，

```
  if(!(len=read(fd,pw_buf,PW_LEN) > 0)){
          printf("read error\n");
          close(fd);
          return 0;
```

此处 read 函数为输入

那么我们运行程序后是有输入内容的 可以输入 0*10

而后 password 因为要通过异或校验，那么就需要输入 1*10

测试一下：

```
mistake@prowl:~$ ./mistake
do not bruteforce...
0000000000
input password : 1111111111
Password OK
Mommy, the operator priority always confuses me :(
mistake@prowl:~$
```

成功得到 flag