二次排序注入也成为存储型的注入，就是将可能导致sql注入的字符先存入到数据库中，当再次调用这个恶意构造的字符时，就可以触发sql注入

注册界面没有对用户名和密码做限制，直接写进了mysql数据库
登陆界面也没有对读取的用户名和密码做处理，因此就有漏洞。登陆语句为
SELECT * FROM users WHERE username='$username' and password='$password'

登录admin'#该，修改该帐号的密码，此时修改的就是admin的密码，我修改为123456。

Sql语句变为UPDATE users SET passwd="New_Pass" WHERE username =' admin' # ' AND password='

也就是执行了UPDATE users SET passwd="New_Pass" WHERE username =' admin'

但是这个题的下载貌似有问题，login.php有问题，无论如何没办法实现登录