**Sql注入验证绕过**

## **Sql 注入实例二.验证绕过** 使用事先编写好的页面，只要输入正确的用户名和密码就能登录成功。



先尝试随意输入用户名 123 和密码 123 登录：

22

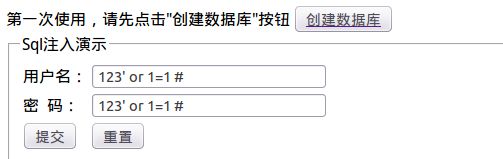
查看后台代码验证：

IMG_258

实际执行的操作时：

select \* from users where username='123' and password='123'

当查询到数据表中存在同时满足 username 和 password 字段时，会返回登录成功，在用户名中输入 123' or 1=1 #, 密码同样输入 123' or 1=1 # ：





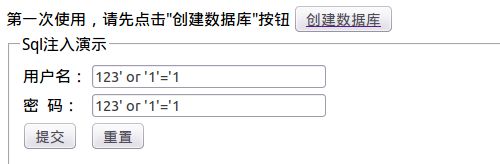
实际执行的语句是：

select \* from users where username='123' or 1=1 #' and password='123' or 1=1 #'

按照 Mysql 语法，# 后面的内容会被忽略，所以以上语句等同于（实际上密码框里不输入任何东西也一样）：

select \* from users where username='123' or 1=1

由于判断语句 or 1=1 恒成立，所以结果当然返回真，成功登录。  
尝试不使用 # 屏蔽单引号，采用手动闭合的方式：  
在用户名中输入 123' or '1'='1, 密码同样输入 123' or '1'='1 （不能少了单引号，否则会有语法错误）：





实际执行的 Sql 语句是：

select \* from users where username='123' or '1'='1' and password='123' or '1'='1

两个 or 语句使 and 前后两个判断永远恒等于真，所以能够成功登录。