**1. sql注入问题**

1.1 问题来源：sql语句采用拼接字符串

|  |
| --- |
| String sql = "select \* from users where username='"  +username+"' and password='"+password+"'"; |

1.2 界面输入用户名和密码后，通过字符串拼接后进行字符串查询



1.3 如果输入的是这样的

用户名： asdfasfasd //随便写

密码： asdfas' or '1'='1 //密码部分随便写

组合后的sql语句就成了

|  |
| --- |
| select \* from users  where username='asdfas' and password='asdfas' or '1'='1' |

主要是拼接了 or '1'='1' ，任何的用户名和密码都无所谓了，这就是登录之sql注入

**2. 解决方案**

针对于sql注入，jdbc提供了参数化执行对象PreparedStatement——？

在DBUtils重载get方法

|  |
| --- |
| /\*\*  \* 参数化查询获得单个对象  \* **@param** sql  \* **@param** clazz  \* **@param** params  \* **@return**  \*/  **public** Object get(String sql, Class clazz,Object[] params) {  Object obj = **null**;  Connection conn = **null**;  **try** {  conn = getConnection();  QueryRunner qRunner = **new** QueryRunner();  obj = qRunner.query(conn, sql, **new** BeanHandler(clazz), params);  } **catch** (SQLException e) {  e.printStackTrace();  } **finally** {  DbUtils.*closeQuietly*(conn);  }  **return** obj;  } |