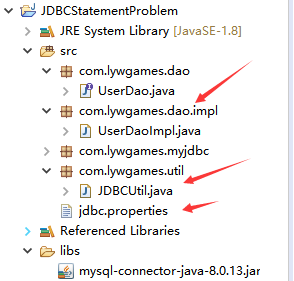
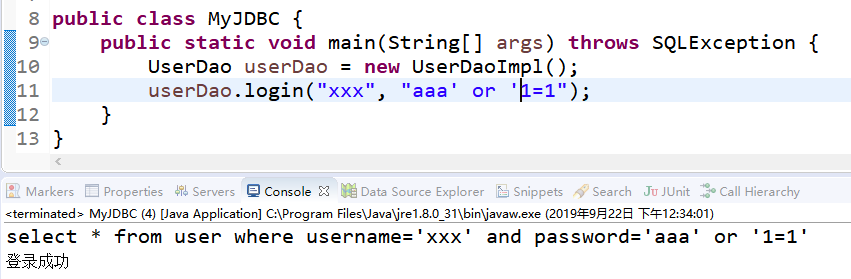
1.新建一个JDBCStatementProblem工程, 使用我们之前的JDBCUtil.java和jdbc.properties属性文件, 以及UserDao



2.输入任意用户名和密码, 在密码处拼接1=1, 运行程序, 居然登录成功了。



3.Statement执行, 其实是拼接sql语句的。 先拼接sql语句, 然后在一起执行。如果变量里面带有了数据库的关键字, 那么一并认为是关键字, 不认为是普通的字符串。 这里拼接 or 1=1, 永远为真, 返回登录成功。