sql注入问题：

preparedStatement：预编译对象

是statement对象的子类

在执行插入操作的时候，建议将插入的列名全部写出来，尽量不要使用*，这样的执行效率会变得更高

特点：

性能要高

会把sql语句预先进行编译

安全

效率高

使用问号表达式：

```
Connection connection = null;
        PreparedStatement statement = null;
        ResultSet rSet = null;
        try {
                connection = test.getConnection();
                String sql = "insert into emp2 values(?,?,?,?,?,?,?,?)";
                statement = connection.prepareStatement(sql);
                statement.setInt(1, 7905);
                statement.setString(2, "anqili");
                statement.setString(3, "clerk");
                statement.setInt(4,7963);
                statement.setString(5, "2018-9-20");
                statement.setDouble(6, 10000.00);
                statement.setDouble(7, 500.00);
                statement.setInt(8, 30);

                int i  = statement.executeUpdate();
```

statement接口：

resultset executeQuery（sql）执行select语句

int executeUpdate（sql）执行insert ，update，delete

Boolean execute（）仅仅当执行的是select语句，且有结果返回的时候才返回true，其他情况都返回false

resultset：

boolean next（）把游标向下移动一行

getInt（int columnindex）根据列的索引查找，索引从1开始

getInt（string columnname）根据列名进行查找

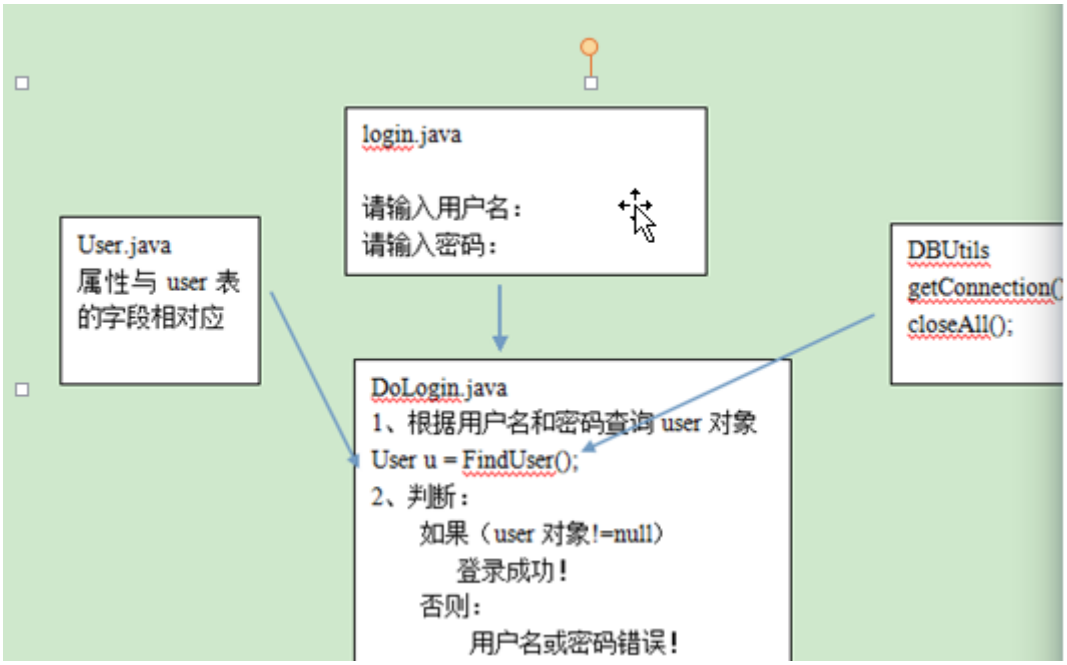
getDouble（）

getFloat（）

getDate（）

getString（）（方法；类型都与getInt类似）

java实现登录，并使用数据库：



preparedstatement：

性能要高

会把sql语句预先编译

sql语句中的参数会发生变化，过滤掉用户输入的关键字