1. 使用Statement的弊端：
2. 需要拼串，
3. SQL注入，WHERE USER = '1' or ' AND PASSWORD = '='1' or '1' = '1';
4. 使用PreparedStatement预编译的Statement简介：
5. PreparedStatement 对象所代表的 SQL 语句中的参数用问号(?)来表示
6. 调用 PreparedStatement 对象的 setXxx() 方法来设置这些参数.
7. setXxx() 方法有两个参数，第一个参数是要设置的 SQL 语句中的参数的索引(从 1 开始)，第二个是设置的 SQL 语句中的参数的值
8. int excuteUpdate(String sql)：执行更新操作INSERT、UPDATE、DELETE ResultSet executeQuery(String sql)：执行查询操作SELECT
9. 创建通用的增删改方法，使用不定长参数，填充占位符
10. 创建针对表的通用查询方法，使用不定长参数，填充占位符，使用ResultSetMetaDate获取结果集的元数据
11. 创建通用的查询方法，使用不定长参数，填充占位符，使用ResultSetMetaDate获取结果集的元数据，使用反射创建对象，使用反射对应数据，使用泛型作为返回值