Atitit mysql sql 特殊字符

‘单偏号 字符串定界符号

\反斜杠要替换为俩个反斜杠

；分号 多语句分隔符 问题不大，因为单引号闭合问题。。

-- 双岗 注释符号 双模杠：--

# ＃号，注释符号

波浪号 表名分割符号

16进制字符的问题不怕，因为有俩个单引号保卫了起来

SELECT 0x5061756c t

都有单引号闭合起来，特殊字符就失去了作用。。不怕 不怕了。。

数字可以转换为数字，字符串有单引号闭合替换即可。。

态 SQL 语句的方式。为了防止他人使用特殊 SQL 字符破坏 SQL 的语句结构或植入恶意操作，必须在变量拼接到 SQL 语句之前对其中的特殊字符进行转义处理。Spring 并没有提供相应的工具类，您可以通过 jakarta commons lang 通用类包中（spring/lib/jakarta-commons/commons-lang.jar）的 StringEscapeUtils 完成这一工作：

**清单 4. SqlEscapeExample**

|  |
| --- |
| package com.baobaotao.escape; import org.apache.commons.lang.StringEscapeUtils; public class SqlEscapeExample {  public static void main(String[] args) {  String userName = "1' or '1'='1";  String password = "123456";  userName = StringEscapeUtils.escapeSql(userName);  password = StringEscapeUtils.escapeSql(password);  String sql = "SELECT COUNT(userId) FROM t\_user WHERE userName='"  + userName + "' AND password ='" + password + "'";  System.out.println(sql);  } } |

事实上， StringEscapeUtils 不但提供了 SQL 特殊字符转义处理的功能，还提供了 HTML、XML、JavaScript、Java 特殊字符的转义和还原的方法。如果您不介意引入 jakarta commons lang 类包，我们更推荐您使用 StringEscapeUtils 工具类完成特殊字符转义处理的工作。