😊21、#{}和${}的区别

微信公众号java-mindmap

- #{}
  - 解读
    - 使用#{}格式的语法在mybatis中使用Preparement语句来安全的设置值
    - PreparedStatement ps = conn.prepareStatement(sql);
ps.setInt(1,id);
  - 例子
    - 执行SQL：Select * from emp where name = #{employeeName}
    - 参数：employeeName=>Smith
    - 解析后执行的SQL：Select * from emp where name = ?
  - #方式能够很大程度防止sql注入
- ${}
  - 解读
    - 有时你只是想直接在 SQL 语句中插入一个不改变的字符串。比如，像 ORDER BY
    - $将传入的数据直接显示生成在sql中
    - Statement st = conn.createStatement();
ResultSet rs = st.executeQuery(sql);
  - 例子
    - 执行SQL：Select * from emp where name = ${employeeName}
    - 参数：employeeName传入值为：Smith
    - 解析后执行的SQL：Select * from emp where name =Smith
- ★总结
  - #方式能够很大程度防止sql注入，$方式无法防止Sql注入
  - $方式一般用于传入数据库对象
  - 使用$要么不允许用户输入这些字段，要么自行转义并检验。
  - 一般能用#的就别用$