**[mybatis中"#"和"$"的区别](http://www.cnblogs.com/kangyun/p/5881531.html)**

　　动态 sql 是 mybatis 的主要特性之一，在 mapper 中定义的参数传到 xml 中之后，在查询之前 mybatis 会对其进行动态解析。mybatis 为我们提供了两种支持动态 sql 的语法：#{} 以及 ${}。

　　在下面的语句中，如果 username 的值为 zhangsan，则两种方式无任何区别：

select \* from user where name = #{name};

select \* from user where name = ${name};

　　其解析之后的结果均为

select \* from user where name = 'zhangsan';

　　但是 #{} 和 ${} 在预编译中的处理是不一样的。#{} 在预处理时，会把参数部分用一个占位符 ? 代替，变成如下的 sql 语句：

select \* from user where name = ?;

　　而 ${} 则只是简单的字符串替换，在动态解析阶段，该 sql 语句会被解析成

select \* from user where name = 'zhangsan';

　　以上，#{} 的参数替换是发生在 DBMS 中，而 ${} 则发生在动态解析过程中。

　　那么，在使用过程中我们应该使用哪种方式呢？

　　答案是，优先使用 #{}。因为 ${} 会导致 sql 注入的问题。看下面的例子：

select \* from ${tableName} where name = #{name}

　　在这个例子中，如果表名为

　　 user; delete user; --

　　则动态解析之后 sql 如下：

select \* from user; delete user; -- where name = ?;

　　--之后的语句被注释掉，而原本查询用户的语句变成了查询所有用户信息+删除用户表的语句，会对数据库造成重大损伤，极大可能导致服务器宕机。

　　但是表名用参数传递进来的时候，只能使用 ${} ，具体原因可以自己做个猜测，去验证。这也提醒我们在这种用法中要小心sql注入的问题。