**1、$ 和 #**

**区别**

#{ }是预编译处理，MyBatis在处理#{ }时，它会将sql中的#{ }替换为？，然后调用PreparedStatement的set方法来赋值，传入字符串后，会在值两边加上单引号，如值 “4,44,514”就会变成“ '4,44,514' ”；

${ }是字符串替换， MyBatis在处理${ }时,它会将sql中的${ }替换为变量的值，传入的数据不会加两边加上单引号。

注意：使用${ }会导致sql注入，不利于系统的安全性！

**应用**

#{ }：主要用户获取DAO中的参数数据,在映射文件的SQL语句中出现#{}表达式,底层会创建预编译的SQL；

${ } : 主要用于获取配置文件数据,DAO接口中的参数信息,当$出现在映射文件的SQL语句中时创建的不是预编译的SQL,而是字符串的拼接,有可能会导致SQL注入问题.所以一般使用$接收dao参数时,这些参数一般是字段名,表名等,例如order by {column}。

注：${}获取DAO参数数据时,参数必须使用@param注解进行修饰或者使用下标或者参数#{param1}形式；

#{}获取DAO参数数据时,假如参数个数多于一个可有选择的使用@param。