动态SQL,Mybatis在动态sql中有分别有两个占位符#{}和${},一般如果输入的是数据的表明或者字段名使用${},#{}作为条件中的字段值.能用#{}的地方尽量不适用#{}区别如下:

#{}将传入的参数当成一个字符串，会给传入的参数加一个双引号

${}将传入的参数直接显示生成在sql中，不会添加引号

#{}能够很大程度上防止sql注入，${}无法防止sql注入

　　${}在预编译之前已经被变量替换了，这会存在sql注入的风险。