1.数据库访问用预定义会话PreparedStatement而不是用Statement， 传参使用#{}而不是使用${}

2.是采用正则表达式将包含有 单引号('), 分号(;) 和 注释符号(--)的语句给替换掉来防止SQL注入

3.前台过滤，对于必要的input输入信息进行格式和长度验证