在几番尝试后我采用了StringEscapeUtils作为防范sql注入和xss注入的safeguard。

首先想到的方法是在每一个输入框加上解析判断，但是这样会做大量重复工作，而且每一次加上一个输入都需要再解析太麻烦。

于是找到使用filter过滤，但是和struts一起配置在web.xml似乎会出问题。

最后采用在struts.xml里配置interceptor。开始时使用自己解析字符串对每个字符进行判断是否是敏感字符，之后发现了StringEscapeUtils这个工具，在commons-lang中有commons-lang3去除了的escapeSql，且有escapeHtml，利用两个函数可以直接进行sql注入和xss注入的过滤，非常方便。

最后在ie浏览器下，bookstore网站的book search界面测试通过。