# web安全

## SQL注入

web安全一大原则：永远不要相信用户的任何输入

* 对输入参数做好检查（类型和范围）：过滤和转移特殊字符
* 不要直接拼接sql，使用ORM可以大大降低sql诸如风险
* 数据库层：做好权限管理配置，不要铭文存储敏感信息

## XSS(cross site scripting)，跨站脚本攻击

* 恶意用户将代码植入到提供给其他用户使用的页面中，未经转义的恶意代码输出到其他用户的浏览器被执行
* 用户浏览页面的时候嵌入页面中的脚本（js）会被执行，攻击用户
* 主要分为两类：反射性（非持久型），存储型（持久型）

## CSRF