web安全：1 sql注入，2 xss(跨站脚本攻击)，3 csrf(跨站请求伪造)

1. 避免sql动态拼接，过滤转义字符，使用orm框架，敏感信息加密
2. 过滤敏感标签，如<a><script>,转义"<" ">" "&"

- 令牌同步(Synchronizer token pattern，简称STP)：在用户请求的表单中嵌入一个隐藏的csrf_token，服务端验证其是否与 cookie 中的一致（基于同源策略其他网站是无法获取cookie中的csrf_token)
- 如果是 js 提交需要先从cookie获取csrf_token作为 X-CSRFToken 请求头提交提交
- 其他：检测来源HTTP Referer(容易被伪造)；验证码方式(安全但是繁琐)