# Web应用安全

参考链接

<https://segmentfault.com/a/1190000004585199>

<https://blog.csdn.net/tiankai30/article/details/54892108>

## 入门知识

### 安全分类

#### 认证与授权

认证：访问网站时需要登录，用户名和密码的提交校验就是认证的过程。   
授权：登录网站后，每个人所能访问的页面不尽相同，就是授权的作用。

如何测试：得到需要登录才能访问的页面（可通过页面属性、抓包等工具），直接拷贝在浏览器地址栏中访问，如果加了安全机制，直接访问会提示错误；否则，不安全。

#### XSS攻击

XSS指攻击者在网页中嵌入客户端脚本(例如JavaScript), 用户浏览网页就会触发恶意脚本执行