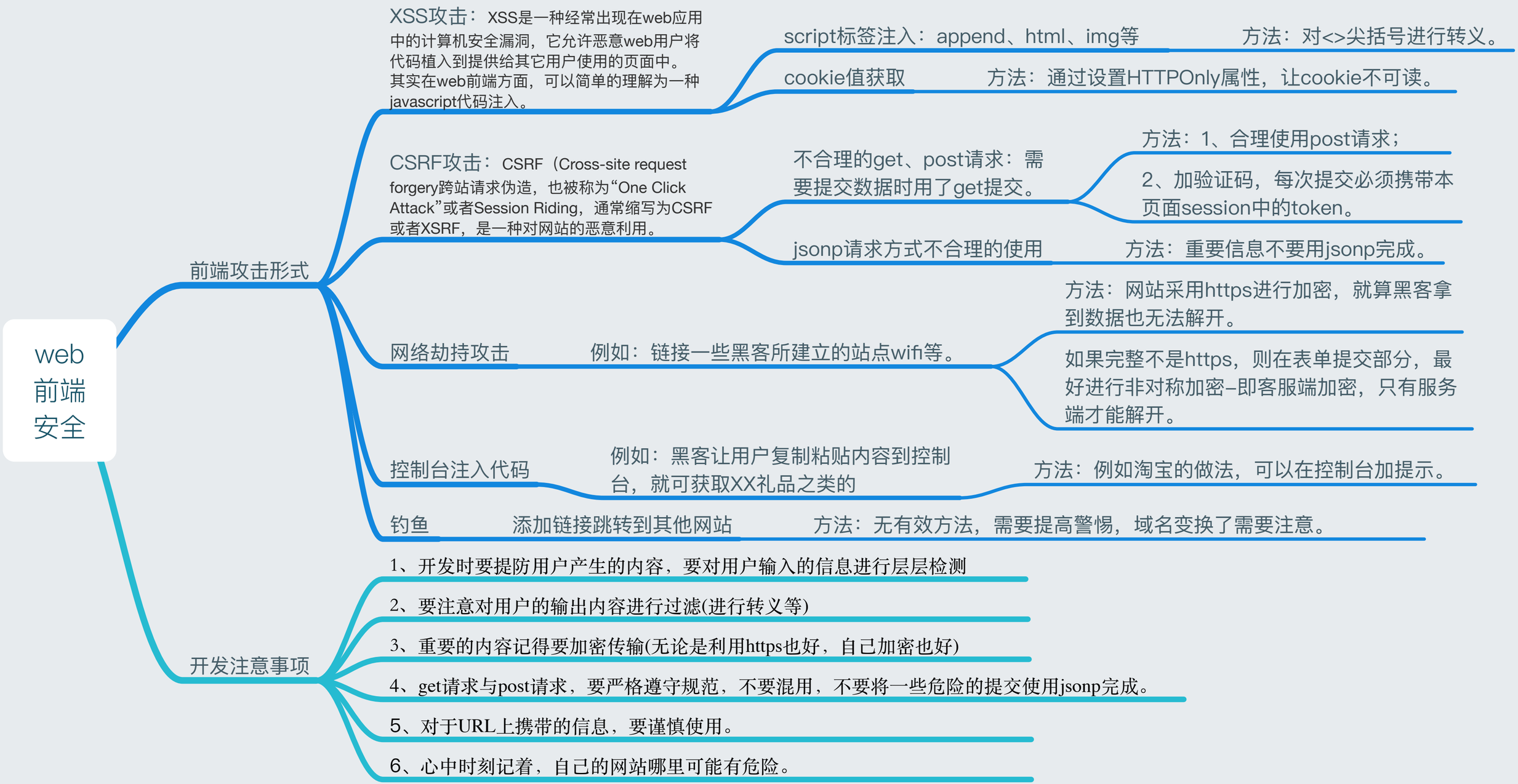
web
前端
安全
前端攻击形式
XSS攻击：XSS是一种经常出现在web应用中的计算机安全漏洞，它允许恶意web用户将代码植入到提供给其它用户使用的页面中。其实在web前端方面，可以简单的理解为一种javascript代码注入。
script标签注入：append、html、img等
方法：对<>尖括号进行转义。
cookie值获取
方法：通过设置HTTPOnly属性，让cookie不可读。
CSRF攻击：CSRF（Cross-site request forgery跨站请求伪造，也被称为“One Click Attack”或者Session Riding，通常缩写为CSRF或者XSRF，是一种对网站的恶意利用。
不合理的get、post请求：需要提交数据时用了get提交。
方法：1、合理使用post请求；
2、加验证码，每次提交必须携带本页面session中的token。
jsonp请求方式不合理的使用
方法：重要信息不要用jsonp完成。
网络劫持攻击
例如：链接一些黑客所建立的站点wifi等。
方法：网站采用https进行加密，就算黑客拿到数据也无法解开。
如果完整不是https，则在表单提交部分，最好进行非对称加密–即客服端加密，只有服务端才能解开。
控制台注入代码
例如：黑客让用户复制粘贴内容到控制台，就可获取XX礼品之类的
方法：例如淘宝的做法，可以在控制台加提示。
钓鱼
添加链接跳转到其他网站
方法：无有效方法，需要提高警惕，域名变换了需要注意。
开发注意事项
1、开发时要提防用户产生的内容，要对用户输入的信息进行层层检测
2、要注意对用户的输出内容进行过滤(进行转义等)
3、重要的内容记得要加密传输(无论是利用https也好，自己加密也好)
4、get请求与post请求，要严格遵守规范，不要混用，不要将一些危险的提交使用jsonp完成。
5、对于URL上携带的信息，要谨慎使用。
6、心中时刻记着，自己的网站哪里可能有危险。