安全-如何预防网络攻击

XSS 攻击

Cross Site Script 跨站脚本攻击。

- 表现：黑客将 JS 代码插入到网页内容中，渲染时执行 JS 代码。
- 处理：特殊字符处理，将 > 替换为 > 将 < 符号替换为 <

CSRF 攻击

Cross Site Request Forgery 跨站请求伪造。

- 手段：黑客诱导用户去访问另一个网站的接口，伪造请求。
- 预防：严格的跨域限制，加验证码机制。

2.1. CSRF 详细过程

- 用户登录了 A 网站，有了 cookie。
- 黑客诱导用户进入了 B 网站，并发起了 A 网站的请求。
- A 网站的用户发现 API 有 cookie，认为是用户自己操作的。

2.2. 预防手段

- 严格的跨域请求限制，如 referrer （请求来源，推荐人，这个单词拼写错误，标准定了之后就没法修改了）。
- 为 cookie 设置 SameSite, 禁止跨域传递 cookie。
- 关键接口加上短信验证码。