# Web安全

1. **XSS概念、攻击手段和如何防范**

**概念：**

中文名为跨站脚本, 是发生在目标用户的浏览器层面上的，简单理解就是：攻击者想 尽一切办法将可以执行的代码注入到网页中。重点在脚本

**两种类型：**

1. 持久类型：攻击的代码被服务端写入进数据库中。 比如在一些论坛的评论中，写script标签加alert语句，如果前后端没有做好防御的话，这段评论就 会被存储到数据库中，这样每个打开该页面的用户都会被攻击到
2. 非持久型一般通过修改 URL 参数的方式加入攻击代码，诱导用户访问链接从而进行攻击

**防范：**

1. 转义字符：转义输入输出的内容，对于引号、尖括号、斜杠进行转义
2. CSP白名单：明确告诉浏览器哪些外部资源可以加载和执行
   1. 设置 HTTP Header 中的 Content-Security-Policy
   2. 设置meta标签的方式meta http-equiv="Content-Security-Policy”
3. **CSRF**

**概念：**

CSRF 中文名为跨站请求伪造。 CSRF攻击的本质在于利用用户的身份，执行非本意的操作。重点在于：CSRF的请求是跨域且伪造的。 跨站请求伪造的攻击是攻击者通过一些技术手段欺骗用户的浏览器去访问用户曾经认证过的网站并执行 一些操作（如发送邮件、发消息、甚至财产操作如转账和购买商品等）。由于浏览器曾经认证过，所以 被访问的网站会认为是真正的用户操作而去执行。这利用了web登录身份认证的一个漏洞：简单的身份 认证只能保证请求来自用户的浏览器，但不能识别请求是用户自愿发出的

**防范规则：**

1. Get 请求不对数据进行修改
2. 不让第三方网站访问到用户 Cookie
3. 阻止第三方网站请求接口
4. 请求时附带验证信息，比如验证码或者 Token

**实用方法：**

1. 对Cookie设置SameSite属性：该属性表示 Cookie 不随着跨域请求发送，可以很大程度减少 CSRF 的攻击，但是该属性目前并不是所 有浏览器都兼容
2. 验证Referer：可以通过验证 Referer 来判断该请求是否为第三方网站发起的
3. 使用Token：服务器下发一个随机 Token，每次发起请求时将 Token 携带上，服务器验证 Token 是否有效
4. **点击劫持**

**概念：**

点击劫持是一种视觉欺骗的攻击手段。攻击者将需要攻击的网站通过 iframe 嵌套的方式嵌入自己的网 页中，并将 iframe 设置为透明，在页面中透出一个按钮诱导用户点击

**防范措施：**

a) **设置HTTP头：X-FRAME-OPTIONS：**这个 HTTP 响应头 就是为了防御用iframe 嵌套的点击劫持攻击。 该响应头有三个值可选，分别是

1. DENY ，表示页面不允许通过 iframe 的方式展示
2. SAMEORIGIN ，表示页面可以在相同域名下通过 iframe 的方式展示
3. ALLOW-FROM ，表示页面可以在指定来源的 iframe 中展示
4. **JS 防御：**对于某些远古浏览器来说，并不能支持上面的这种方式，那我们只有通过 JS 的方式来防御点击劫持 了。 当通过 iframe 的方式加载页面时，攻击者的网页直接不显示所有内容了
5. **中间人攻击**

**概念：**

中间人攻击是攻击方同时与服务端和客户端建立起了连接，并让对方认为连接是安全的，但是实际上整 个通信过程都被攻击者控制了。攻击者不仅能获得双方的通信信息，还能修改通信信息

**如何防范：**

防御中间人攻击其实并不难，只需要增加一个安全通道来传输信息。HTTPS 就可以用来防御中间人攻 击，但是并不是说使用了 HTTPS 就可以高枕无忧了，因为如果你没有完全关闭 HTTP 访问的话，攻击 方可以通过某些方式将 HTTPS 降级为 HTTP 从而实现中间人攻击