链滴

什么是跨站点脚本攻击（XSS）？应如何阻止他?

作者：Vanessa

原文链接：https://ld246.com/article/1553313536893

来源网站：链滴

2019-03-22

回答

XSS 是指客户端代码注入，攻击者将带有恶意脚本的代码注入到合法的网站或 web 应用程序中。这常发生在应用程序对用户的输入不进行验证时，这样恶意代码就会轻松的注入到动态的 HTML 内容。

例如，一个评论系统如果没有对用户的输入进行验证或转义，那么该评论系统将面临风险。如果评论容中包含未转义的 HTML，那么评论时就可以将 <script> 标签注入到网站中，当其他用户访问这个论页面时就会执行该脚本以发起攻击。

- 恶意的脚本有权限访问到通常用于存储会话令牌的 cookie。如果攻击者可以获取用户的会话 cooki，那么攻击者就可以冒充该用户。
- 当页面中注入的恶意脚本执行时，就可以对该页面中的 DOM 进行任意操作。这样一来，攻击者不可以插入与网站相似的内容或操作，也可以窜改网站上原有的实际内容。
- 该脚本还可以使用 AJAX 发送带有任意内容的 HTTP 请求到任意一台服务器上。

加分回答

- 在客户端，可以使用 textContent 来代替 innerHTML 以阻止浏览器运行通过 HTML 解析器执内部脚本得到的字符串。
- 在服务器端，转义 HTML 标签可以阻止浏览器将用户的输入解析为真实的 HTML，这样也不会执脚本。但如果你想真实的展现用户的输入，那就只能对会被注入的标签、标签属性进行过滤。

返回总目录

30 秒面试系列一