

# XSS学习笔记

From <https://www.hackthebox.com/>, Thanks for working

## 介绍

随着 Web 应用程序变得越来越高级和普遍，Web 应用程序漏洞也越来越多。最常见的 Web 应用程序漏洞类型是跨站点脚本 (XSS) 漏洞。XSS 漏洞利用用户输入中的缺陷将 JavaScript 代码“写入”页面并在客户端执行，从而导致多种类型的攻击。

## 什么是 XSS

典型的 Web 应用程序通过从后端服务器接收 HTML 代码并将其呈现在客户端互联网浏览器上来工作。当易受攻击的 Web 应用程序未正确清理用户输入时，恶意用户可以在输入字段（例如，评论/回复）中注入额外的 JavaScript 代码，因此一旦其他用户查看同一页面，他们就会在不知不觉中执行恶意 JavaScript 代码。

XSS 漏洞仅在客户端执行，因此不会直接影响后端服务器。它们只能影响执行漏洞的用户。XSS 漏洞对后端服务器的直接影响可能相对较小，但它们在 Web 应用程序中非常常见，因此这相当于中等风险（），我们应该始终通过 `low impact + high probability = medium risk` 检测 `reduce`、修复和修复来尝试冒险。主动防止这些类型的漏洞。



## XSS 攻击

XSS 漏洞可以促进范围广泛的攻击，可以是任何可以通过浏览器 JavaScript 代码执行的攻击。XSS 攻击的一个基本示例是让目标用户无意中将他们的会话 cookie 发送到攻击者的 Web 服务器。另一个例子是让目标的浏览器执行导致恶意操作的 API 调用，例如将用户密码更改为攻击者选择的密码。还有许多其他类型的 XSS 攻击，从比特币挖掘到显示广告。

由于 XSS 攻击在浏览器内执行 JavaScript 代码，因此它们仅限于浏览器的 JS 引擎（即 Chrome 中的 V8）。他们无法执行系统范围的 JavaScript 代码来执行系统级代码执行之类的事情。在现代浏览器中，它们也仅限于易受攻击网站的同一域。尽管如此，如上所述，能够在用户的浏览器中执行 JavaScript 仍可能导致各种各样的攻击。除此之外，如果熟练的研究人员发现网络浏览器中的二进制漏洞（例如，Chrome 中的堆溢出），他们可以利用 XSS 漏洞在目标浏览器上执行 JavaScript 漏洞利用，最终突破浏览器的沙箱并在用户的机器上执行代码。

XSS 漏洞可能存在于几乎所有现代 Web 应用程序中，并且在过去二十年中一直被积极利用。一个著名的 XSS 示例是 Samy 蠕虫，这是一种基于浏览器的蠕虫，它在 2005 年利

用了社交网站 MySpace 中存储的 XSS 漏洞。它在查看受感染的网页时执行，方法是在受害者的 MySpace 页面上发布一条消息，内容为“Samy is my hero”。消息本身也包含相同的 JavaScript 负载，以便在其他人的查看时重新发布相同的消息。一天之内，超过一百万的 MySpace 用户在他们的页面上发布了这条消息。尽管这个特定的有效负载没有造成任何实际伤害，但该漏洞可能被用于更邪恶的目的，比如窃取用户的信用卡信息、在他们的浏览器上安装键盘记录器，甚至利用用户网络浏览器中的二进制漏洞（这在当时的网络浏览器中更为常见）。

2014 年，一名安全研究人员意外发现了 Twitter 的 TweetDeck 仪表板中的 XSS 漏洞。此漏洞被利用在 Twitter 中创建一条 自我转发的推文，导致该推文在不到两分钟的时间内被转发超过 38,000 次。最终，它迫使 Twitter 在修补漏洞时 暂时关闭 TweetDeck。

时至今日，即使是最著名的 Web 应用程序也存在可被利用的 XSS 漏洞。甚至谷歌的搜索引擎页面在其搜索栏中也存在多个 XSS 漏洞，最近一次是在 2019 年，当时在 XML 库中发现了一个 XSS 漏洞。此外，互联网上最常用的 Web 服务器 Apache Server 曾报告过一个 XSS 漏洞，该漏洞被积极利用来窃取某些公司的用户密码。所有这些都告诉我们应该认真对待 XSS 漏洞，并且应该付出大量努力来检测和预防它们。