

## <<XSS跨站脚本攻击剖析与防御>>

### 图书基本信息

书名：<<XSS跨站脚本攻击剖析与防御>>

13位ISBN编号：9787115311047

10位ISBN编号：7115311048

出版时间：2013-9-1

作者：邱永华

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## <<XSS跨站脚本攻击剖析与防御>>

### 内容概要

《XSS跨站脚本攻击剖析与防御》是一本专门剖析XSS安全的专业书，总共8章，主要包括的内容如下。

第1章 XSS初探，主要阐述了XSS的基础知识，包括XSS的攻击原理和危害。

第2章 XSS利用方式，就当前比较流行的XSS利用方式做了深入的剖析，这些攻击往往基于客户端，从挂马、窃取Cookies、会话劫持到钓鱼欺骗，各种攻击都不容忽视。

第3章 XSS测试和利用工具，介绍了一些常见的XSS测试工具。

第4章 发掘XSS漏洞，着重以黑盒和白盒的角度介绍如何发掘XSS漏洞，以便帮助读者树立安全意识。

第5章 XSS Worm，讲解了Web 2.0的最大威胁——跨站脚本蠕虫，剖析了Web 2.0相关概念和其核心技术，这些知识对于理解和预防XSS Worm十分重要。

第6章 Flash应用安全，就当前的Flash应用安全做出了深入阐述。

第7章 深入XSS原理，讨论一些比较深入的XSS理论。

第8章 防御XSS攻击，介绍了一些防范XSS攻击的方法，例如，运用XSS Filter进行输入过滤和输出编码，使用Firefox浏览器的Noscript插件抵御XSS攻击，使用HTTP-only的Cookies同样能起到保护敏感数据的作用。

《XSS跨站脚本攻击剖析与防御》适合网站管理人员、信息/网络安全或相关工作从业者、软件开发工程师，以及任何对Web安全技术感兴趣的读者。

# <<XSS跨站脚本攻击剖析与防御>>

作者简介

邱永华

## &lt;&lt;XSS跨站脚本攻击剖析与防御&gt;&gt;

## 书籍目录

## 目 录

- 第1章 XSS初探 1
  - 1.1 跨站脚本介绍 1
    - 1.1.1 什么是XSS跨站脚本 2
    - 1.1.2 XSS跨站脚本实例 4
    - 1.1.3 XSS漏洞的危害 6
  - 1.2 XSS的分类 8
    - 1.2.1 反射型XSS 8
    - 1.2.2 持久型XSS 10
  - 1.3 XSS的简单发掘 12
    - 1.3.1 搭建测试环境 12
    - 1.3.2 发掘反射型的XSS 12
    - 1.3.3 发掘持久型的XSS 15
  - 1.4 XSS Cheat Sheet 18
  - 1.5 XSS构造剖析 21
    - 1.5.1 绕过XSS-Filter 22
    - 1.5.2 利用字符编码 33
    - 1.5.3 拆分跨站法 37
  - 1.6 Shellcode的调用 39
    - 1.6.1 动态调用远程JavaScript 40
    - 1.6.2 使用window.location.hash 41
    - 1.6.3 XSS Downloader 41
    - 1.6.4 备选存储技术 43
- 第2章 XSS利用方式剖析 45
  - 2.1 Cookie窃取攻击剖析 45
    - 2.1.1 Cookie基础介绍 46
    - 2.1.2 Cookie会话攻击原理剖析 48
    - 2.1.3 Cookie欺骗实例剖析 49
  - 2.2 会话劫持剖析 51
    - 2.2.1 了解Session机制 51
    - 2.2.2 XSS实现权限提升 52
    - 2.2.3 获取网站Webshell 55
  - 2.3 网络钓鱼 57
    - 2.3.1 XSS Phishing 57
    - 2.3.2 XSS钓鱼的方式 59
    - 2.3.3 高级钓鱼技术 60
  - 2.4 XSS History Hack 63
    - 2.4.1 链接样式和getComputedStyle() 64
    - 2.4.2 JavaScript/CSS history hack 64
    - 2.4.3 窃取搜索查询 65
  - 2.5 客户端信息刺探 67
    - 2.5.1 JavaScript实现端口扫描 67
    - 2.5.2 截获剪贴板内容 68
    - 2.5.3 获取客户端IP地址 70
  - 2.6 其他恶意攻击剖析 71

## &lt;&lt;XSS跨站脚本攻击剖析与防御&gt;&gt;

- 2.6.1 网页挂马 71
- 2.6.2 DOS和DDOS 72
- 2.6.3 XSS Virus/Worm 73
- 第3章 XSS测试和工具剖析 75
  - 3.1 Firebug 75
  - 3.2 Tamper Data 80
  - 3.3 Live HTTP Headers 82
  - 3.4 Fiddler 84
  - 3.5 XSS-Proxy 86
  - 3.6 XSS Shell 90
  - 3.7 AttackAPI 94
  - 3.8 Anehta 98
- 第4章 发掘XSS漏洞 104
  - 4.1 黑盒工具测试 104
  - 4.2 黑盒手动测试 107
  - 4.3 源代码安全审计 110
  - 4.4 JavaScript代码分析 118
    - 4.4.1 DOM简介 118
    - 4.4.2 第三种XSS——DOM XSS 120
    - 4.4.3 发掘基于DOM的XSS 123
  - 4.5 发掘Flash XSS 126
  - 4.6 巧用语言特性 129
    - 4.6.1 PHP 4 phpinfo() XSS 130
    - 4.6.2 \$\_SERVER[PHP\_SELF] 131
    - 4.6.3 变量覆盖 132
- 第5章 XSS Worm剖析 135
  - 5.1 Web 2.0应用安全 135
    - 5.1.1 改变世界的Web 2.0 135
    - 5.1.2 浅谈Web 2.0的安全性 137
  - 5.2 Ajax技术指南 138
    - 5.2.1 使用Ajax 139
    - 5.2.2 XMLHttpRequest对象 140
    - 5.2.3 HTTP请求 142
    - 5.2.4 HTTP响应 142
  - 5.3 浏览器安全 145
    - 5.3.1 沙箱 145
    - 5.3.2 同源安全策略 146
  - 5.4 XSS Worm介绍 147
    - 5.4.1 蠕虫病毒剖析 147
    - 5.4.2 XSS Worm攻击原理剖析 148
    - 5.4.3 XSS Worm剖析 149
    - 5.4.4 运用DOM技术 150
  - 5.5 新浪微博蠕虫分析 153
- 第6章 Flash应用安全 156
  - 6.1 Flash简介 156
    - 6.1.1 Flash Player 与SWF 156
    - 6.1.2 嵌入Flash文件 158

## &lt;&lt;XSS跨站脚本攻击剖析与防御&gt;&gt;

- 6.1.3 ActionScript语言 158
- 6.2 Flash安全模型 160
  - 6.2.1 Flash安全沙箱 161
  - 6.2.2 Cross Domain Policy 162
  - 6.2.3 设置管理器 164
- 6.3 Flash客户端攻击剖析 165
  - 6.3.1 getURL() & XSS 165
  - 6.3.2 Cross Site Flashing 169
  - 6.3.3 Flash参数型注入 171
  - 6.3.4 Flash钓鱼剖析 173
- 6.4 利用Flash进行XSS攻击剖析 174
- 6.5 利用Flash进行CSRF 178
- 第7章 深入XSS原理 181
  - 7.1 深入浅出CSRF 182
    - 7.1.1 CSRF原理剖析 182
    - 7.1.2 CSRF实例讲解剖析 185
    - 7.1.3 CSRF的应用剖析 187
  - 7.2 Hacking JSON 187
    - 7.2.1 JSON概述 187
    - 7.2.2 跨域JSON注入剖析 190
    - 7.2.3 JSON Hijacking 191
  - 7.3 HTTP Response Splitting 193
    - 7.3.1 HTTP Header 193
    - 7.3.2 CRLF Injection原理 195
    - 7.3.3 校内网HRS案例 197
  - 7.4 MHTML协议的安全 199
  - 7.5 利用Data URIs进行XSS剖析 203
    - 7.5.1 Data URIs介绍 203
    - 7.5.2 Data URIs XSS 204
    - 7.5.3 vBulletin Data URIs XSS 206
  - 7.6 UTF-7 BOM XSS 206
  - 7.7 浏览器插件安全 211
    - 7.7.1 Flash后门 211
    - 7.7.2 来自PDF的XSS 213
    - 7.7.3 QuickTime XSS 217
  - 7.8 特殊的XSS应用场景剖析 218
    - 7.8.1 基于Cookie的XSS 218
    - 7.8.2 来自RSS的XSS 220
    - 7.8.3 应用软件中的XSS 222
  - 7.9 浏览器差异 225
    - 7.9.1 跨浏览器的不兼容性 226
    - 7.9.2 IE嗅探机制与XSS 226
    - 7.9.3 浏览器差异与XSS 228
  - 7.10 字符集编码隐患 231
- 第8章 防御XSS攻击 234
  - 8.1 使用XSS Filter 234
    - 8.1.1 输入过滤 235

## <<XSS跨站脚本攻击剖析与防御>>

- 8.1.2 输出编码 237
- 8.1.3 黑名单和白名单 239
- 8.2 定制过滤策略 240
- 8.3 Web安全编码规范 244
- 8.4 防御DOM-Based XSS 248
- 8.5 其他防御方式 250
  - 8.5.1 Anti\_XSS 250
  - 8.5.2 HttpOnly Cookie 252
  - 8.5.3 Noscript 253
  - 8.5.4 WAF 254
- 8.6 防御CSRF攻击 255
  - 8.6.1 使用POST替代GET 256
  - 8.6.2 检验HTTP Referer 257
  - 8.6.3 验证码 258
  - 8.6.4 使用Token 259
- 参考文献 262

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>