

# 《Web应用漏洞侦测与防御》

## 图书基本信息

书名：《Web应用漏洞侦测与防御》

13位ISBN编号：9787111472535

出版时间：2014-8-20

作者：Mike Shema

页数：231

译者：齐宁,庞建民,张铮,单征

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：[www.tushu111.com](http://www.tushu111.com)

# 《Web应用漏洞侦测与防御》

## 内容概要

本书由国际知名网络安全专家亲笔撰写，全面讲解如何预防常见的网络攻击，包括HTML注入及跨站脚本攻击、跨站请求伪造攻击、SQL注入攻击及数据存储操纵、攻破身份认证模式、利用设计缺陷、利用平台弱点、攻击浏览器和隐私等，全书共8章：第1章介绍HTML5的新增特性及使用和滥用HTML5的安全考虑；第2章展示了如何只通过浏览器和最基本的HTML知识就可以利用Web中最常见的漏洞；第3章详细讲解CSRF（跨站请求伪造）攻击的实现机制及应对策略；第4章介绍如何执行SQL注入攻击，并探究了类似攻击的实现机制，提供一些阻止这些攻击的对策；第5章介绍Web站点保护密码失败的常见方式以及阻止这些攻击所能采取的步骤；第6章主要探讨网站底层设计中会导致漏洞的错误；第7章不仅介绍了应用程序代码可能引发的错误，还介绍了除此之外不应当忽略的其他安全性问题；第8章将探讨更多浏览器面临的来自恶意设计的网页或者已经感染了恶意内容网页的风险。

# 《Web应用漏洞侦测与防御》

## 作者简介

Mike Shema 国际知名的网络安全专家，现就职于Qualys，专注于自动化Web评估服务。之前曾是Foundstone信息安全咨询公司首席咨询师和培训师，在网络渗透测试、无线网络安全、代码审核、Web安全等方面有丰富的经验，撰写了多部信息安全技术图书，如《黑客大曝光：Web应用安全机密与解决方案》、《反黑客工具箱》和《黑客札记：Web安全手册》，并经常在世界范围的安全技术大会上演讲。

## 译者简介

齐宁 解放军信息工程大学博士，曾讲授课程有“信息安全”“网络原理与实践”等，曾参研国家重大专项611工程、国家863项目等，涉及漏洞发现技术、逆向分析技术、高性能计算机体系结构等领域。

## 书籍目录

译者序

前言

第1章 HTML5 1

1.1 新的文档对象模型 2

1.2 跨域资源共享 3

1.3 Websocket 6

1.3.1 传输数据 9

1.3.2 数据帧 10

1.3.3 安全性考虑 12

1.4 Web存储 13

1.5 Web Worker 15

1.6 杂七杂八 18

1.6.1 History API 18

1.6.2 API草案 18

1.7 小结 18

第2章 HTML注入及跨站脚本攻击 20

2.1 理解HTML注入 21

2.1.1 确定注入点 26

2.1.2 确定反射类型 33

2.1.3 确定注入呈现位置的上下文 36

2.1.4 攻击汇总 40

2.1.5 利用字符集 42

2.1.6 利用失效模式 49

2.1.7 绕过弱的排除列表 52

2.1.8 利用浏览器的怪异模式 53

2.1.9 不寻常的攻击载体 55

2.1.10 XSS的影响 58

2.2 部署应对措施 59

2.2.1 确定静态字符集 60

2.2.2 规范化字符集及编码 61

2.2.3 对输出进行编码 62

2.2.4 当心排除列表和正则表达式 63

2.2.5 重用代码，不要重新实现代码 64

2.2.6 JavaScript沙盒 65

2.2.7 浏览器内置XSS防御 67

2.3 小结 69

第3章 跨站请求伪造 70

3.1 理解跨站请求伪造 71

3.1.1 CSRF实现机制 73

3.1.2 借助强制浏览的请求伪造 76

3.1.3 无需密码攻击已认证动作 79

3.1.4 危险关系：CSRF和HTML注入 79

3.1.5 当心错综复杂的Web 80

3.1.6 相关主题：点击劫持 81

3.2 部署应对措施 82

3.2.1 朝着正确方向努力 83

3.2.2 保卫Web浏览器 91

- 3.2.3 脆弱性和似真性 92
- 3.3 小结 92
- 第4章 SQL注入攻击及数据存储操纵 94
  - 4.1 理解SQL注入 96
    - 4.1.1 攻击路线：数学和语法 99
    - 4.1.2 攻击SQL语句 99
    - 4.1.3 剖析数据库 107
    - 4.1.4 其他攻击向量 110
    - 4.1.5 真实世界中的SQL注入攻击 111
    - 4.1.6 HTML5的Web存储API 112
    - 4.1.7 不使用SQL的SQL注入攻击 113
  - 4.2 部署应对措施 114
    - 4.2.1 验证输入 115
    - 4.2.2 对语句进行保护 115
    - 4.2.3 保护信息 121
    - 4.2.4 给数据库打最新的补丁 123
  - 4.3 小结 123
- 第5章 攻破身份认证模式 125
  - 5.1 理解身份认证攻击 126
    - 5.1.1 重放会话令牌 126
    - 5.1.2 暴力破解 129
    - 5.1.3 网络嗅探 130
    - 5.1.4 重置密码 132
    - 5.1.5 跨站脚本攻击 133
    - 5.1.6 SQL注入 133
    - 5.1.7 诈骗和易受骗性 134
  - 5.2 部署应对措施 135
    - 5.2.1 保护会话cookie 135
    - 5.2.2 使用安全认证方案 137
    - 5.2.3 借助用户的力量 144
    - 5.2.4 骚扰用户 145
    - 5.2.5 请求限制 146
    - 5.2.6 日志与三角测量 147
    - 5.2.7 击败钓鱼攻击 147
    - 5.2.8 保护密码 148
  - 5.3 小结 148
- 第6章 利用设计缺陷 150
  - 6.1 理解逻辑攻击和设计攻击 153
    - 6.1.1 利用工作流 153
    - 6.1.2 漏洞利用的策略及做法 154
    - 6.1.3 归纳法 158
    - 6.1.4 拒绝服务 160
    - 6.1.5 不安全的设计模式 161
    - 6.1.6 加密中的实现错误 165
    - 6.1.7 信息泄露 177
  - 6.2 部署应对措施 178
    - 6.2.1 记录需求 178
    - 6.2.2 创建强健的测试用例 178
    - 6.2.3 把策略映射到控制 180

- 6.2.4 防御性编程 180
- 6.2.5 验证客户端 181
- 6.2.6 加密指南 181
- 6.3 小结 182
- 第7章 利用平台弱点 183
  - 7.1 攻击是如何实现的 184
    - 7.1.1 识别模式、数据结构以及开发者癖好 184
    - 7.1.2 以操作系统为攻击目标 197
    - 7.1.3 攻击服务器 202
    - 7.1.4 拒绝服务 202
  - 7.2 部署应对措施 206
    - 7.2.1 限制文件访问 207
    - 7.2.2 使用对象引用 207
    - 7.2.3 将不安全函数列入到黑名单 208
    - 7.2.4 强制授权 208
    - 7.2.5 限制网络连接 208
  - 7.3 小结 209
- 第8章 攻击浏览器和隐私 210
  - 8.1 理解恶意软件和浏览器攻击 211
    - 8.1.1 恶意软件 211
    - 8.1.2 插入到浏览器插件中 215
    - 8.1.3 DNS和域 217
    - 8.1.4 HTML5 217
    - 8.1.5 隐私 219
  - 8.2 部署应对措施 227
    - 8.2.1 安全地配置SSL/TLS 227
    - 8.2.2 更加安全地浏览网页 228
    - 8.2.3 隔离浏览器 229
    - 8.2.4 Tor 229
    - 8.2.5 DNSSEC 230
  - 8.3 小结 230

# 《Web应用漏洞侦测与防御》

## 精彩短评

- 1、翻译真的是翻译味道太重了...这很“不能同意更多”...
- 2、概念偏多，还好不太厚，要不一时半会还真啃不完。
- 3、书是好书，可惜翻译的人是个对网络信息安全不懂的傻逼
- 4、看目录不错，web安全，只是还是没记住，有些还是没理解，SQL注入，ARP欺骗，DOS攻击，有机会再看一遍。。。

# 《Web应用漏洞侦测与防御》

## 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:[www.tushu111.com](http://www.tushu111.com)