

<<黑客大曝光>>

图书基本信息

书名：<<黑客大曝光>>

13位ISBN编号：9787111356622

10位ISBN编号：7111356624

出版时间：2011-10

出版时间：机械工业出版社华章公司

作者：Joel Scambray, Vincent Liu, Caleb Sima

页数：319

译者：姚军

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>

<<黑客大曝光>>

内容概要

在网络技术和电子商务飞速发展的今天，web应用安全面临着前所未有的挑战。所有安全技术人员有必要掌握当今黑客们的武器和思维过程，保护web应用免遭恶意攻击。本书由美国公认的安全专家和精神领袖打造，对上一版做了完全的更新，覆盖新的网络渗透方法和对策，介绍如何增强验证和授权、弥补firefox和ie中的漏洞、加强对注入攻击的防御以及加固web 2.0安全，还介绍了如何将安全技术整合在web开发以及更广泛的企业信息系统中。

主要内容：

- 黑客足迹跟踪、扫描和剖析工具，包括shodan、maltego和lowasp dirbuster
- 流行平台（如sun java system web server和oracle weblogic）上新的漏洞攻击
- 攻击者如何挫败常用的web验证技术
- 实际的会话攻击泄漏敏感数据的方法，以及加固应用的途径
- 当今黑客使用的最具毁灭性的方法，包括sql注入、xss、xsrif、网络钓鱼和xml注入技术
- 寻找和修复asp.net、php和j2ee执行环境中的漏洞
- 安全部署xml、社交网络、云计算和web2.0服务
- 防御ria、ajax、ugc和基于浏览器的客户端漏洞利用
- 实现可伸缩的威胁建模、代码评审、应用扫描、模糊测试和安全测试规程

<<黑客大曝光>>

作者简介

Joel

Scambray , CISSP、战略安全咨询服务供应商Consciere的共同创始人和CEO。

他曾经在Microsoft、Foundstone、Ernst

& Young以及其他机构从事互联网安全评估和防御将近15年之久，是国际知名的演说家和多本安全书籍的作者。

<<黑客大曝光>>

书籍目录

对本书的赞誉

译者序

序言

前言

作者简介

致谢

第1章 web应用入侵基础1

1.1 什么是web应用入侵1

1.1.1 gui web入侵1

1.1.2 uri入侵2

1.1.3 方法、首部和主体3

1.1.4 资源4

1.1.5 验证、会话和授权5

1.1.6 web客户端与html5

1.1.7 其他协议6

1.2 为什么攻击web应用7

1.3 谁、何时、何处8

1.4 web应用是如何遭到攻击的9

1.4.1 web浏览器9

1.4.2 浏览器扩展10

1.4.3 http代理14

1.4.4 命令行工具19

1.4.5 较老的工具20

1.5 小结20

1.6 参考与延伸阅读20

第2章 剖析23

2.1 基础架构剖析23

2.1.1 足迹法和扫描：定义范围23

2.1.2 基本的标志获取24

2.1.3 高级http指纹识别25

2.1.4 基础架构中介28

2.2 应用剖析34

2.2.1 手工检查34

2.2.2 剖析所用的搜索工具50

2.2.3 自动化的web爬行55

2.2.4 常见web应用剖析60

2.3 一般对策63

2.3.1 警告63

2.3.2 保护目录63

2.3.3 保护包含文件64

2.3.4 其他技巧64

2.4 小结65

2.5 参考与延伸阅读65

第3章 web平台入侵67

3.1 用metasploit进行点击攻击68

<<黑客大曝光>>

- 3.2 手工攻击70
- 3.3 逃避检测80
- 3.4 web平台安全最佳实践82
 - 3.4.1 通用的最佳实践82
 - 3.4.2 iis加固84
 - 3.4.3 apache加固87
 - 3.4.4 php最佳实践90
- 3.5 小结91
- 3.6 参考与延伸阅读92
- 第4章 攻击web验证94
 - 4.1 web验证威胁94
 - 4.1.1 用户名/密码威胁94
 - 4.1.2 (更)强的web验证108
 - 4.1.3 web验证服务111
 - 4.2 绕过验证114
 - 4.2.1 令牌重放114
 - 4.2.2 跨站请求伪造116
 - 4.2.3 身份管理118
 - 4.2.4 客户端借道法121
 - 4.3 最后一些想法:身份盗窃122
 - 4.4 小结122
 - 4.5 参考与延伸阅读123
- 第5章 攻击web授权126
 - 5.1 授权指纹识别127
 - 5.1.1 acl爬行127
 - 5.1.2 识别访问令牌128
 - 5.1.3 分析会话令牌129
 - 5.1.4 差异分析131
 - 5.1.5 角色矩阵132
 - 5.2 攻击acl132
 - 5.3 攻击令牌134
 - 5.3.1 人工预测134
 - 5.3.2 自动预测140
 - 5.3.3 捕捉/重放145
 - 5.3.4 会话完成146
 - 5.4 授权攻击案例研究147
 - 5.4.1 水平权限提升147
 - 5.4.2 垂直权限提升151
 - 5.4.3 差异分析153
 - 5.4.4 当加密失败时155
 - 5.4.5 使用curl映射权限155
 - 5.5 授权最佳实践158
 - 5.5.1 web acl最佳实践158
 - 5.5.2 web授权/访问令牌安全161
 - 5.5.3 安全日志163
 - 5.6 小结163
 - 5.7 参考与延伸阅读164

<<黑客大曝光>>

- 第6章 输入注入攻击166
 - 6.1 预料到意外情况167
 - 6.2 何处寻找攻击目标167
 - 6.3 绕过客户端校验例程168
 - 6.4 常见输入注入攻击169
 - 6.4.1 缓冲区溢出169
 - 6.4.2 规范化攻击170
 - 6.4.3 html注入174
 - 6.4.4 边界检查177
 - 6.4.5 操纵应用行为178
 - 6.4.6 sql注入179
 - 6.4.7 xpath注入189
 - 6.4.8 ldap注入191
 - 6.4.9 自定义参数注入192
 - 6.4.10 日志注入193
 - 6.4.11 命令执行193
 - 6.4.12 编码误用195
 - 6.4.13 php全局变量195
 - 6.4.14 常见的副作用196
 - 6.5 常见对策196
 - 6.6 小结197
 - 6.7 参考与延伸阅读198
- 第7章 攻击xml web服务200
 - 7.1 web服务是什么200
 - 7.1.1 传输：soap over http201
 - 7.1.2 wsdl204
 - 7.1.3 目录服务：uddi和disco205
 - 7.1.4 与web应用安全的相似性209
 - 7.2 攻击web服务209
 - 7.3 web服务安全基础216
 - 7.4 小结219
 - 7.5 参考与延伸阅读219
- 第8章 攻击web应用管理221
 - 8.1 远程服务器管理221
 - 8.1.1 telnet221
 - 8.1.2 ssh222
 - 8.1.3 专用管理端口222
 - 8.1.4 其他管理服务223
 - 8.2 web内容管理224
 - 8.2.1 ftp224
 - 8.2.2 ssh/scp224
 - 8.2.3 frontpage225
 - 8.2.4 webdav226
 - 8.3 错误的配置231
 - 8.3.1 不必要的web服务器扩展232
 - 8.3.2 引起信息泄露的错误配置234
 - 8.3.3 状态管理的错误配置245

<<黑客大曝光>>

- 8.4 小结249
- 8.5 参考与延伸阅读250
- 第9章 入侵web客户端251
 - 9.1 漏洞利用251
 - 9.2 骗术264
 - 9.3 一般的对策269
 - 9.3.1 低权限浏览269
 - 9.3.2 firefox安全扩展271
 - 9.3.3 activex对策271
 - 9.3.4 服务器端对策273
 - 9.4 小结274
 - 9.5 参考与延伸阅读274
- 第10章 企业web应用安全计划277
 - 10.1 威胁建模277
 - 10.1.1 澄清安全目标278
 - 10.1.2 识别资产279
 - 10.1.3 架构概要279
 - 10.1.4 分解应用280
 - 10.1.5 识别和记录威胁280
 - 10.1.6 威胁排名282
 - 10.1.7 开发威胁缓解策略283
 - 10.2 代码评审284
 - 10.2.1 人工源代码评审284
 - 10.2.2 自动化源代码评审288
 - 10.2.3 二进制分析288
 - 10.3 web应用代码安全测试296
 - 10.3.1 模糊测试296
 - 10.3.2 测试工具、实用程序和框架298
 - 10.3.3 渗透测试298
 - 10.4 web开发过程中的安全299
 - 10.4.1 人员299
 - 10.4.2 过程301
 - 10.4.3 技术303
 - 10.5 小结305
 - 10.6 参考与延伸阅读305
- 附录a web安全检查列表308
- 附录b web黑客工具和技术快速参考312

<<黑客大曝光>>

章节摘录

版权页：插图：剖析是用于研究和精确描述网站结构和应用工作方式的策略，是一个非常重要却常被忽视的Web入侵方向。

最有效的攻击是基于缜密的准备工作，尽可能地说明应用的内部工作原理，包括网站的所有网页、应用和输入/输出控制结构。

剖析过程的勤奋和严格以及投入的时间常常与整个网站上识别出的安全性问题的质量直接相关，并且常常能区分出发现“随手可摘的果实”的“脚本小孩（scriptkiddle）”评估（如简单的sQL注入或者缓冲区溢出攻击）和真正揭露应用核心业务逻辑的渗透之间的差别。

Web剖析中使用许多工具和技术，但是在阅读本章之后，你将能走上专家之路。

我们对剖析的讨论分为两部分：·基础架构剖析·应用剖析我们选择这种组织结构是因为每种类型的剖析的想法、方法和结果都有所不同。

基础架构剖析关注Web应用相对不变的“现有”组件（我们宽泛地使用“现有”这个词来包含所有形式的通用重用软件，包括免费软件、开源软件和商业软件）。

通常，这些组件中的漏洞容易识别并且加以利用。

另一方面，应用剖析处理单独的高度定制Web应用的独特结构、逻辑和功能。

应用漏洞可能很微妙，需要花费大量的研究才能发现和利用。

当然，我们对应用剖析的讨论也将占本章的很大部分。

本章最后将简短讨论对常见剖析策略的一般对策。

<<黑客大曝光>>

媒体关注与评论

“本书对于寻求进入web应用安全世界、有抱负的工程师，以及紧跟最新技术发展、成熟的应用安全和渗透测试专家来说，都是值得一读的。” ——Chad Greene，eBay全球信息安全主管

<<黑客大曝光>>

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>