<<黑客攻防技术宝典>>

图书基本信息

书名：<<黑客攻防技术宝典>>

13位ISBN编号：9787115210777

10位ISBN编号：7115210772

出版时间：2009-8

出版时间：人民邮电出版社

作者：Dafydd Stuttard,Marcus Pinto

页数：495

译者：石华耀

前言

随着网络技术的快速发展以及网络带宽的不断扩张，Web应用程序几乎无处不在，渗透到社会的经济、文化、娱乐等各个方面。
但同时，承载着丰富功能与用途的Web应用程序也成为恶意用户与黑客等攻击者的主要攻击目标。
因此，如何确保Web，应用程序的安全已成为政府、企业，特别是银行等金融机构所面临的主要挑战。

古语云：知己知彼，百战不殆。
只有充分了解攻击者所采用的攻击方法以及Web应用程序中存在的可供攻击者利用的各种漏洞，我们才能针对这些漏洞采取行之有效的防御方法。
本书两位作者都是安全领域的专家，拥有丰富的渗透测试实践经验，因而本书具有极高的实用价值。
书中主要介绍了渗透测试员在测试Web应用程序时所采用的步骤和技巧。
同时，从防御的角度看，这些步骤与技巧也为确保Web应用程序的安全、加强防御措施指明了方向。

本书内容全面，几乎涵盖了所有Web核心技术，如HTTP、客户与服务器端技术、数据编码等；涉及了Web应用程序的主要核心功能，如客户端控件、会话管理、访问控制、应用程序逻辑与体系架构、Web服务器等；详细分析了各种类型的漏洞，如代码注入、路径遍历、跨站点脚本、重定向攻击、跨站点请求伪造、会话劫持、会话固定、缓冲区溢出、整数漏洞、格式化漏洞等；还提供了一些作者作为专业渗透测试员开发的Burphtruder、JAttack、Paros、WebScarab、Nikto、Hydra等工具。
另外，为弥补读者在某些方面的知识欠缺，本书还提供了一些背景知识及相关链.接。
本着实用的原则，作者在分析漏洞、介绍渗透测试步骤与技术的同时，还提供了大量实例与代码片段；每节的“渗透测试步骤”部分还对前面讨论的内容进行了简要总结。
此外，每章最后的“问题”可帮助读者回顾该章的重点知识。

<<黑客攻防技术宝典>>

内容概要

《黑客攻防技术宝典·Web实战篇》是探索和研究Web应用程序安全缺陷的实践指南。
作者利用大量的实际案例、屏幕快照和示例代码，详细介绍了每一种Web应用程序弱点，并深入阐述了如何针对Web应用程序进行具体的渗透测试。
《黑客攻防技术宝典·Web实战篇》从介绍当前Web应用程序安全概况开始，重点讨论渗透测试时使用的技巧和详细步骤，最后总结书中涵盖的主题。
每章后还附有习题，便于读者巩固所学内容。
《黑客攻防技术宝典·Web实战篇》适用于各层次计算机安全和Web开发与管理领域的技术人员。

作者简介

Dafydd Stuttard，世界知名的安全技术专家。
著名Web应用攻击测试工具Burp Suite的开发者。
以网名PortSwigger蜚声安全界。
牛津大学博士，现任Next Generation Security Software公司资深安全顾问，主要负责Web应用程序安全。

<<黑客攻防技术宝典>>

书籍目录

第1章 Web应用程序安全与风险 11.1 Web应用程序的发展历程 11.1.1 Web应用程序的常见功能 21.1.2 Web应用程序的优点 31.2 Web应用程序安全 31.2.1 “ 本站点是安全的 ” 31.2.2 核心安全问题：用户可提交任意输入 51.2.3 关键问题因素 61.2.4 新的安全边界 71.2.5 Web应用程序安全的未来 81.3 小结 8第2章 核心防御机制 92.1 处理用户访问 92.1.1 身份验证 102.1.2 会话管理 102.1.3 访问控制 112.2 处理用户输入 122.2.1 输入的多样性 122.2.2 输入处理方法 132.2.3 边界确认 142.2.4 多步确认与规范化 162.3 处理攻击者 172.3.1 处理错误 172.3.2 维护审计日志 182.3.3 向管理员发出警报 192.3.4 应对攻击 192.4 管理应用程序 202.5 小结 212.6 问题 21第3章 Web应用程序技术 223.1 HTTP 223.1.1 HTTP请求 223.1.2 HTTP响应 233.1.3 HTTP方法 243.1.4 URL 253.1.5 HTTP消息头 263.1.6 cookie 273.1.7 状态码 283.1.8 HTTPS 293.1.9 HTTP代理 293.1.10 HTTP验证 293.2 Web功能 303.2.1 服务器端功能 303.2.2 客户端功能 323.2.3 状态与会话 353.3 编码方案 363.3.1 URL编码 363.3.2 Unicode编码 363.3.3 HTML编码 373.3.4 Base64编码 373.3.5 十六进制编码 383.4 下一步 383.5 问题 38第4章 解析应用程序 394.1 枚举内容与功能 394.1.1 Web抓取 394.1.2 用户指定的抓取 414.1.3 发现隐藏的内容 434.1.4 应用程序页面与功能路径 504.1.5 发现隐藏的参数 514.2 分析应用程序 524.2.1 确定用户输入进入点 524.2.2 确定服务器端技术 534.2.3 确定服务器端功能 584.2.4 解析受攻击面 604.3 小结 604.4 问题 61第5章 避开客户端控件 625.1 通过客户端传送数据 625.1.1 隐藏表单字段 625.1.2 HTTP cookie 645.1.3 URL参数 655.1.4 Referer消息头 655.1.5 模糊数据 665.1.6 ASP.NET ViewState 675.2 收集用户数据：HTML表单 705.2.1 长度限制 705.2.2 基于脚本的确认 715.2.3 禁用的元素 735.3 收集用户数据：厚客户端组件 745.3.1 Java applet 745.3.2 ActiveX控件 805.3.3 Shockwave Flash对象 845.4 安全处理客户端数据 875.4.1 通过客户传送数据 875.4.2 确认客户生成的数据 885.4.3 日志与警报 895.5 小结 895.6 问题 89第6章 攻击验证机制 916.1 验证技术 916.2 验证机制设计缺陷 926.2.1 密码保密性不强 926.2.2 蛮力攻击登录 936.2.3 详细的失败消息 956.2.4 证书传输易受攻击 976.2.5 密码修改功能 986.2.6 忘记密码功能 996.2.7 “ 记住我 ” 功能 1016.2.8 用户伪装功能 1026.2.9 证书确认不完善 1046.2.10 非唯一性用户名 1046.2.11 可预测的用户名 1056.2.12 可预测的初始密码 1056.2.13 证书分配不安全 1066.3 验证机制执行缺陷 1076.3.1 故障开放登录机制 1076.3.2 多阶段登录机制中的缺陷 1086.3.3 不安全的证书存储 1106.4 保障验证机制的安全 1116.4.1 使用可靠的证书 1116.4.2 安全处理证书 1116.4.3 正确确认证书 1126.4.4 防止信息泄露 1136.4.5 防止蛮力攻击 1146.4.6 防止滥用密码修改功能 1166.4.7 防止滥用账户恢复功能 1166.4.8 日志、监控与通知 1176.5 小结 1176.6 问题 118第7章 攻击会话管理 1197.1 状态要求 1197.2 会话令牌生成过程中的薄弱环节 1227.2.1 令牌有一定含义 1227.2.2 令牌可预测 1247.3 会话令牌处理中的薄弱环节 1307.3.1 在网络上泄露令牌 1307.3.2 在日志中泄露令牌 1337.3.3 令牌-会话映射易受攻击 1357.3.4 会话终止易受攻击 1367.3.5 客户暴露在令牌劫持风险之中 1377.3.6 宽泛的cookie范围 1387.4 保障会话管理的安全 1407.4.1 生成强大的令牌 1407.4.2 在整个生命周期保障令牌的安全 1427.4.3 日志、监控与警报 1447.5 小结 1457.6 问题 145第8章 攻击访问控制 1478.1 常见漏洞 1478.1.1 完全不受保护的功能 1488.1.2 基于标识符的功能 1498.1.3 多阶段功能 1508.1.4 静态文件 1508.1.5 访问控制方法不安全 1518.2 攻击访问控制 1518.3 保障访问控制的安全 1548.4 小结 1588.5 问题 158第9章 代码注入 1599.1 注入解释型语言 1599.2 注入SQL 1609.2.1 利用一个基本的漏洞 1619.2.2 避开登录 1639.2.3 查明SQL注入漏洞 1649.2.4 注入不同的语句类型 1669.2.5 UNION操作符 1689.2.6 “ 指纹识别 ” 数据库 1729.2.7 提取有用的数据 1729.2.8 利用ODBC错误消息(仅适用于MS-SQL) 1779.2.9 避开过滤 1809.2.10 二阶SQL注入 1839.2.11 高级利用 1849.2.12 SQL注入之外：扩大数据库攻击范围 1939.2.13 SQL语法与错误参考 1959.2.14 防止SQL注入 2009.3 注入操作系统命令 2029.3.1 例1：通过Perl注入 2039.3.2 例2：通过ASP注入 2049.3.3 查找OS命令注入漏洞 2059.3.4 防止OS命令注入 2079.4 注入Web脚本语言 2089.4.1 动态执行漏洞 2089.4.2 文件包含漏洞 2109.4.3 防止脚本注入漏洞 2119.5 注入SOAP 2129.5.1 查找并利用SOAP注入 2139.5.2 防止SOAP注入 2149.6 注入XPath 2149.6.1 破坏应用程序逻辑 2159.6.2 谨慎XPath注入 2169.6.3 盲目XPath注入 2169.6.4 查找XPath注入漏洞 2179.6.5 防止XPath注入 2189.7 注入SMTP 2189.7.1 操纵电子邮件消息头 2189.7.2 SMTP命令注入 2199.7.3 查找SMTP注入漏洞 2219.7.4 防止SMTP注入 2229.8 注入LDAP 2229.8.1 注入查询属性 2239.8.2 修改查询过滤器 2249.8.3 查找LDAP注入漏洞 2249.8.4 防止LDAP注入 2259.9 小结 2259.10 问题 225第10章 利用路径遍历 22710.1 常见漏洞 22710.2 查找并利用路径遍历漏洞 22810.2.1 确定攻击目标

22810.2.2 探查路径遍历漏洞 22910.2.3 避开遍历攻击障碍 23110.2.4 利用遍历漏洞 23410.3 防止路径遍历漏洞 23410.4 小结 23510.5 问题 236第11章 攻击应用程序逻辑 23711.1 逻辑缺陷的本质 23711.2 现实中的逻辑缺陷 23811.2.1 例1：欺骗密码修改功能 23811.2.2 例2：直接结算 23911.2.3 例3：修改保险单 24011.2.4 例4：入侵银行 24111.2.5 例5：擦除审计追踪 24311.2.6 例6：规避交易限制 24411.2.7 例7：获得大幅折扣 24511.2.8 例8：避免转义 24511.2.9 例9：滥用搜索功能 24711.2.10 例10：利用调试消息 24811.2.11 例11：与登录机制竞赛 24911.3 避免逻辑缺陷 25011.4 小结 25111.5 问题 252第12章 攻击其他用户 25312.1 跨站点脚本 25412.1.1 反射型XSS漏洞 25412.1.2 保存型XSS漏洞 25912.1.3 基于DOM的XSS漏洞 26112.1.4 现实世界中的XSS攻击 26212.1.5 链接XSS与其他攻击 26412.1.6 XSS攻击有效载荷 26512.1.7 XSS攻击的传送机制 27012.1.8 查找并利用XSS漏洞 27112.1.9 HttpOnly cookie与跨站点追踪 28512.1.10 防止XSS攻击 28712.2 重定向攻击 29012.2.1 查找并利用重定向漏洞 29112.2.2 防止重定向漏洞 29412.3 HTTP消息头注入 29412.3.1 利用消息头注入漏洞 29512.3.2 防止消息头注入漏洞 29712.4 框架注入 29812.4.1 利用框架注入 29812.4.2 防止框架注入 29912.5 请求伪造 29912.5.1 本站点请求伪造 29912.5.2 跨站点请求伪造 30112.6 JSON劫持 30312.6.1 JSON 30312.6.2 攻击JSON 30412.6.3 查找JSON劫持漏洞 30512.6.4 防止JSON劫持 30612.7 会话固定 30612.7.1 查找并利用会话固定漏洞 30812.7.2 防止会话固定漏洞 30912.8 攻击ActiveX控件 30912.8.1 查找ActiveX漏洞 31012.8.2 防止ActiveX漏洞 31212.9 本地隐私攻击 31212.9.1 持久性cookie 31212.9.2 缓存Web内容 31212.9.3 浏览历史记录 31312.9.4 自动完成 31312.9.5 防止本地隐私攻击 31412.10 高级利用技巧 31412.10.1 利用Ajax 31412.10.2 反DNS Pinning 31712.10.3 浏览器利用框架 31912.11 小结 32012.12 问题 321第13章 定制攻击自动化 32213.1 应用定制自动化攻击 32213.2 枚举有效的标识符 32313.2.1 基本步骤 32313.2.2 探测“ 触点 ” 32413.2.3 编写攻击脚本 32513.2.4 JAttack 32613.3 获取有用的数据 33113.4 常见漏洞模糊测试 33413.5 整合全部功能：Burp Intruder 33713.6 小结 34413.7 问题 345第14章 利用信息泄露 34614.1 利用错误消息 34614.1.1 错误消息脚本 34614.1.2 栈追踪 34714.1.3 详尽的调试消息 34814.1.4 服务器与数据库消息 34914.1.5 使用公共信息 35014.1.6 制造详尽的错误消息 35114.2 收集公布的信息 35114.3 使用推论 35214.4 防止信息泄露 35314.4.1 使用常规错误消息 35314.4.2 保护敏感信息 35414.4.3 尽量减少客户端信息泄露 35414.5 小结 35414.6 问题 355第15章 攻击编译型应用程序 35715.1 缓冲区溢出漏洞 35715.1.1 栈溢出 35815.1.2 堆溢出 35815.1.3 “ 一位偏移 ” 漏洞 35915.1.4 查找缓冲区溢出漏洞 36115.2 整数漏洞 36215.2.1 整数溢出 36215.2.2 符号错误 36315.2.3 查找整数漏洞 36315.3 格式化字符串漏洞 36415.4 小结 36515.5 问题 366第16章 攻击应用程序架构 36716.1 分层架构 36716.1.1 攻击分层架构 36816.1.2 保障分层架构的安全 37016.2 共享主机与应用程序服务提供商 37116.2.1 虚拟主机 37216.2.2 共享的应用程序服务 37216.2.3 攻击共享环境 37316.2.4 保障共享环境的安全 37616.3 小结 37816.4 问题 378第17章 攻击Web服务器 37917.1 Web服务器配置缺陷 37917.1.1 默认证书 37917.1.2 默认内容 38017.1.3 目录列表 38317.1.4 危险的HTTP方法 38417.1.5 Web服务器作为代理服务器 38517.1.6 虚拟主机配置缺陷 38717.1.7 保障Web服务器配置的安全 38717.2 Web服务器软件漏洞 38817.2.1 缓冲区溢出漏洞 38817.2.2 路径遍历漏洞 38917.2.3 编码与规范化漏洞 38917.2.4 查找Web服务器漏洞 39117.2.5 保障Web服务器软件的安全 39217.3 小结 39317.4 问题 393第18章 查找源代码中的漏洞 39418.1 代码审查方法 39418.1.1 “ 黑盒 ” 测试与 “ 白盒 ” 测试 39418.1.2 代码审查方法 39518.2 常见漏洞签名 39618.2.1 跨站点脚本 39618.2.2 SQL注入 39718.2.3 路径遍历 39718.2.4 任意重定向 39818.2.5 OS命令注入 39918.2.6 后门密码 39918.2.7 本地代码漏洞 39918.2.8 源代码注释 40118.3 Java平台 40118.3.1 确定用户提交的数据 40118.3.2 会话交互 40218.3.3 潜在危险的API 40218.3.4 配置Java环境 40518.4 ASP.NET 40618.4.1 确定用户提交的数据 40618.4.2 会话交互 40718.4.3 潜在危险的API 40718.4.4 配置ASP.NET环境 41018.5 PHP 41018.5.1 确定用户提交的数据 41118.5.2 会话交互 41218.5.3 潜在危险的API 41218.5.4 配置PHP环境 41618.6 Perl 41818.6.1 确定用户提交的数据 41818.6.2 会话交互 41818.6.3 潜在危险的API 41918.6.4 配置Perl环境 42018.7 JavaScript 42118.8 数据库代码组件 42118.8.1 SQL注入 42218.8.2 调用危险的函数 42218.9 代码浏览工具 42318.10 小结 42418.11 问题 424第19章 Web应用程序黑客工具包 42619.1 Web浏览器 42619.1.1 Internet Explorer 42619.1.2 Firefox 42719.1.3 Opera 42819.2 集成测试套件 42919.2.1 工作原理 42919.2.2 特性比较 43919.2.3 拦截代理服务器替代工具 44319.3 漏洞扫描器 44519.3.1 扫描器探测到的漏洞 44519.3.2 扫描器的内在限制 44719.3.3 扫描器面临的技术挑战 44819.3.4 当前产品 44919.3.5 使用漏洞扫描器 45119.4 其他工具 45119.4.1 Nikto 45119.4.2 Hydra 45219.4.3 定制脚本 45219.5 小结 454第20章 Web应用程序渗透测试方法论 456

章节摘录

第1章　Web应用程序安全与风险　　Web应用程序安全无疑是当务之急，也是值得关注的话题。对相关各方而言，这一问题都至关重要。
这里的相关各方包括因特网业务收入日益增长的公司、向web应用程序托付敏感信息的用户，以及通过窃取支付信息或入侵银行账户偷窃巨额资金的犯罪分子。
可靠的信誉也非常重要，没人愿意与不安全的web站点进行交易，也没有组织愿意披露有关其安全方面的漏洞或违规行为的详细情况。
因此，获取当前web应用程序安全状况的可靠信息不可小视。
本章简要介绍web应用程序的发展历程及它们提供的诸多优点，并且列举我们亲身体验过的在目前web应用程序中存在的漏洞，这些漏洞表明绝大多数应用程序还远远不够安全。
本章还将描述web应用程序面临的核心安全问题（即用户可提交任意输入的问题），以及造成安全问题的各种因素。
最后讨论web应用程序安全方面的最新发展趋势，并预测其未来的发展方向。
1.1 Web应用程序的发展历程　　在因特网发展的早期阶段，万维网（world Wideweb）仅由web站点构成，这些站点基本上是包含静态文档的信息库。
随后人们发明了web浏览器，通过它来提取和显示那些文档，如图1.1所示。
这种相关信息流仅由服务器向浏览器单向传送。
多数站点并不验证用户的合法性，因为根本没有必要这样做；所有用户同等对待，收取同样的信息。
创建一个web站点所带来的安全威胁主要与web服务器软件的（诸多）漏洞有关。
攻击者入侵web站点并不能获取任何敏感信息，因为服务器上保存的信息可以公开查看。

<<黑客攻防技术宝典>>

编辑推荐

跟安全技术大师学习黑客攻防技术，全面分析Web应用程序安全漏洞，大量实例和代码片段。

越来越多的关键应用现在已经迁移到网站上，这些Web应用的安全已经成为各机构的重要挑战。知己知彼，方能百战不殆。

只有了解Web应用程序中存在的可被利用的漏洞和攻击者所采用的攻击方法，才能更有效地确保Web安全。

《黑客攻防技术宝典·Web实战篇》是Web安全领域专家的经验结晶，系统阐述了如何针对Web应用程序展开攻击与反攻击，详细剖析了攻击时所使用的技巧、步骤和工具，条理清晰，内容全面，几乎涵盖了所有Web核心技术以及Web应用程序的核心功能，另外还为读者提供了作者自己开发的几个探查漏洞的工具，是一本难得一见的黑客技术实用宝典。

版权说明