<<黑客攻防技术宝典（第2版）>>

图书基本信息

书名：<<黑客攻防技术宝典（第2版）>>

13位ISBN编号：9787115283924

10位ISBN编号：7115283923

出版时间：2012-7

出版时间：人民邮电出版社

作者：[英] Dafydd Stuttard,[英] Marcus Pinto

页数：626

字数：957000

译者：石华耀,傅志红

<<黑客攻防技术宝典（第2版）>>

内容概要

《黑客攻防技术宝典：Web实战篇(第2版)》是探索和研究Web应用程序安全漏洞的实践指南。作者利用大量的实际案例和示例代码，详细介绍了各类Web应用程序的弱点，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(第2版)》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详细步骤和技巧，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。

第2版新增了Web应用程序安全领域近年来的发展变化新情况，并以尝试访问的链接形式提供了几百个互动式“漏洞实验室”，便于读者迅速掌握各种攻防知识与技能。

《黑客攻防技术宝典：Web实战篇(第2版)》适合各层次计算机安全人士和Web开发与管理领域的技术人员阅读。

作者简介

Dafydd Stuttard 世界知名安全顾问、作家、软件开发人士。
牛津大学博士，MDSec公司联合创始人，尤其擅长Web应用程序和编译软件的渗透测试。
Dafydd以网名PortSwigger蜚声安全界，是众所周知的Web应用程序集成攻击平台Burp Suite的开发者。

Marcus Pinto 资深渗透测试专家，剑桥大学硕士，MDSec公司联合创始人。
Marcus为全球金融、政府、电信、博彩、零售等行业顶尖组织和机构提供Web应用程序渗透测试和安全防御的咨询与培训。

书籍目录

目　录

章节摘录

版权页： 插图： 10.2.2文件包含漏洞 许多脚本语言支持使用包含文件（include file）。
这种功能允许开发者把可重复使用的代码插入到单个的文件中，并在需要时将它们包含在特殊功能的代码文件中。
然后，包含文件中的代码被解释，就好像它插人到包含指令的位置一样。
1.远程文件包含 PHP语言特别容易出现文件包含漏洞，因为它的包含函数接受远程文件路径。
这种缺陷已经成为PHP应用程序中大量漏洞的根源。
以一个向不同位置的人们传送各种内容的应用程序为例。
用户选择他们的位置后，这个信息通过一个请求参数传送给服务器，代码如下： https：／／wahh—app.com／main.php?Country=US 应用程序通过以下方式处理Country参数： 这使执行环境加载位于Web服务器文件系统中的US.php文件。
然后，这个文件的内容被复制至Umain.php文件中，并得以执行。
攻击者能够以各种方式利用这种行为，最严重的情况是指定一个外部URL作为包含文件的位置。
PHP包含函数接受这个位置作为输入，接着，执行环境将获取指定的文件并执行其内容。
因此，攻击者能够构建一个包含任意复杂内容的恶意脚本，将其寄存在他控制的web服务器上，并通过易受攻击的应用程序函数调用它然后执行。
例如： 2.本地文件包含 有时，应用程序根据用户可控制的数据加载包含文件，但这时不可能给位于外部服务器上的文件指定URL。
例如，如果用户可控制的数据被提交给ASP函数Server.Execute，那么攻击者就可以执行任意一段ASP脚本，只要这段脚本属于调用这个函数的相同应用程序。
在这种情况下，攻击者仍然可以利用应用程序的行为执行未授权操作。
口在服务器上可能有一些通过正常途径无法访问的文件，例如，任何访问路径／admin的请求都会被应用程序实施的访问控制阻止。
如果能够将敏感功能包含在一个授权访问的页面中，那么就可以访问那个功能。
口服务器上的一些静态资源也受到同样的保护，无法直接访问。
如果能够将这些文件动态包含在其他应用程序页面中，那么执行环境就会将静态资源的内容复制到它的响应中。
3.查找文件包含漏洞 任何用户提交的数据项都可能引起文件包含漏洞。
它们经常出现在指定一种语言或一个位置的请求参数中，也常常发生在以参数形式传送服务器端文件名的情况下。

媒体关注与评论

关于黑客攻防技术，没有一本书能比这本书讲解得更为透彻和全面！

——Jason Haddix，惠普公司渗透测试总监　如果你对Web应用程序安全感兴趣，我强烈推荐本书，它实为Web安全人士必读之作。

——Robert Wesley McGrew，McGrew安全公司研究人员　第1版本来就是Web安全领域的扛鼎之作，第2版可谓经典之上的完善，绝对值得拥有！

——Daniel Miessler，安全顾问

编辑推荐

安全技术宝典全新升级　深入剖析，实战演练，使你如饮醍醐

名人推荐

“关于黑客攻防技术，没有一本书能比这本书讲解得更为透彻和全面！”——Jason Haddix，惠普公司渗透测试总监“如果你对Web应用程序安全感兴趣，我强烈推荐本书，它实为Web安全人士必读之作。”——Robert Wesley McGrew，McGrew安全公司研究人员“第1版本来就是Web安全领域的扛鼎之作，第2版可谓经典之上的完善，绝对值得拥有！”——Daniel Miessler，安全顾问

版权说明