<<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

<<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owasp 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、xsrf、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

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

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。

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

版权说明