<<Web系统安全和渗透性测试基础>>

图书基本信息

书名：<<Web系统安全和渗透性测试基础>>

13位ISBN编号：9787802433410

10位ISBN编号：780243341X

出版时间：2009-6

出版时间：航空工业出版社

作者：中国信息安全测评中心

页数：183

前言

世界正经历一场伟大的信息革命，信息成为一种重要的战略资源。
它改变着人们的生活方式和工作方式，形成新的社会形态。
随着我国社会信息化进程的不断发展，计算机网络及信息系统在政府机构、企事业单位及社会团体的工作中发挥着越来越重要的作用。
然而，信息化水平的提高在带来巨大发展机遇的同时也带来了严峻的挑战。
由于信息系统是一个复杂巨系统，它存在着脆弱性，信息安全问题不断暴露。
信息安全关系到国家的经济安全、政治安全、军事安全和文化安全。
信息安全已经成为维护国家安全和社会稳定的一个重要因素。
当前，社会对信息安全专业人员的需求逐年增加。
发展信息安全技术与产业，关键是人才。
培养信息安全领域的专业人才，已成为当务之急。
高素质的信息安全人才队伍是保障国家重点基础网络和重要系统安全的基石，是制定信息安全发展战略规划与政策并建设国家信息安全保障体系的骨干力量，是发展我国信息安全产业的排头兵。
目前我国的信息安全教育工作仍相对滞后，信息安全人才十分匮乏，社会需求与人才供给间还存在着很大差距。
如何培养信息安全的专业人才，是我国目前面临的重要问题。

<<Web系统安全和渗透性测试基础>>

内容概要

本书内容从浅入深，依次逐步展开。
本书共分两部分：第一部分是Web系统安全基础，主要介绍了Web系统的基础和Web系统安全的基础；第二部分是Web系统渗透性测试基础，主要讲述了Web渗透测试的步骤、Web应用渗透性测试的框架以及如何撰写Web渗透测试报告。
另外，书中附录部分介绍了一些常用的Web系统安全渗透性测试工具。
本书是中国信息安全测评中心注册信息安全专业人员（CISP）和注册信息安全员（CISM）的正式教材，可作为高等院校信息安全类专业学生教材，亦可作为信息安全培训教材和IT信息安全从业人员的参考书籍。

<<Web系统安全和渗透性测试基础>>

书籍目录

章节摘录

插图：4．4．1．12．2堆溢出（1）概述这一测试中，我们将检验测试者是否能造成一个堆溢出，对内存片段进行攻击。
（2）问题描述“堆”是指用于存储动态分配数据和全局变量的内存片段。
堆中的每一个存储块都有包含着内存管理信息的标签，用于指明边界。
当一个基于堆的缓冲区出现溢出时，这些标签中的控制信息就会被覆盖；在堆管理例程释放该缓冲区时，由于内存地址被覆盖将导致访问异常。
攻击者可以利用该漏洞将某个设定的值写入一段内存单元中，覆盖掉该内存单元中原来的值，人为地造成溢出。
实际上，攻击者甚至可以使用恶意地址来覆盖函数指针和存储在GOT、．dtors或者TEB这类结构中的各种地址。
有许多堆溢出漏洞的变体，如允许对函数指针进行覆盖，又如由于执行了恶意代码造成内存管理结构被破坏。
与栈溢出相比，对堆溢出进行定位需要更为细密的检查，因为代码中需要存在一些特定的条件这些漏洞才能显露。

编辑推荐

《Web系统安全和渗透性测试基础》编辑推荐：信息化是当今世界发展的大趋势，是推动经济社会变革的重要力量。
大力推进信息化，是覆盖我国现代化建设全局的战略举措，是贯彻落实科学发展观，全面建设小康社会、构建社会主义和谐社会和建设创新型国家的迫切需要和必然选择。
如何以信息化提升综合国力，如何在信息化快速发展的同时确保国家信息安全，这已经成为各国政府关心的热点问题。
信息安全已经从国家政治、经济、军事、文化等领域普及到社会团体、企业，直到普通百姓，信息安全成为信息化的最主要的基础建设之一。
〈br〉从当前形势分析，信息安全教育工作滞后，信息安全人才极度匮乏，社会需求与人才供给间还存在着很大差距。
如何培养信息安全的专业人才，这一新问题困扰着人们，是我国目前面临的重要问题。
〈br〉《国家信息安全培训丛书》从根本出发，以求解决这一问题，推进信息安全人员培训工作的顺利开展。
作者对于本套教材花费了大量的精力，力图能描画出信息安全保障的基础性的概貌，是一套十分宝贵的信息安全专业人员培训丛书。
相信这套丛书的出版，能成为我国培养信息安全专业人员的重要基石。

版权说明