<<软件安全的24宗罪>>

图书基本信息

书名：<<软件安全的24宗罪>>

13位ISBN编号：9787302226345

10位ISBN编号：7302226342

出版时间：2010-6

出版时间：清华大学出版社

作者：（美）霍华德，（美）勒布朗，（美）维维 著，董艳，包战，程文俊 译

页数：306

前言

在应用计算机工程领域中，使安全工作切实可行是我们面临的最大挑战。
所有的工程系统都有指导性需求——它们已成为可测量的要素，如果达不到这些要求，系统就会失败。
例如，大楼必须是安全的（不能倒塌！
），但这还不够，大楼还必须是可用的（里面的空间可以使用）、能盖得起来、可以维护（建筑和维护的成本必须使大楼在投入使用后可以盈利），最后，大楼还应有一定的吸引力（大楼的外观与其居住者的状态以及该属性的价值相关）。
每个需求都有自己的优先级，但它们必须都得到满足。
在许多应用计算机工程领域中，人们不大重视安全。
一些项目只是轻描淡写地提到了安全，这使安全无法成为真正的工程实践要求。
这样很糟糕。
软件的复杂性是毋庸置疑的——现代操作系统，甚至是现代网络浏览器，都比航天飞机复杂得多。
航天飞机可以杀人，但带有极少的几个异常的软件却不会杀人。
所以，安全的基本核心——“正确”，从来都没有成为软件的明确设计规则，更不用说成为根本的设计规则了。
于是，软件中对安全的这种漠视使我们不得不忍受大量的重复设计（往好听了说）或错误（往难听了说）。
毕竟，无论软件编写得多糟糕，在几乎所有的情况下，都不会有人因此丢掉性命。
破产则完全是另一回事，并不是只有人才会死，公司也会消亡。
计算机安全研究已经持续了数十年，但直到2000年以后，不安全软件的后果才最终为外界所知。
2003年“夏虫”（‘Me Summer of Worms）肆虐——简言之，几个恶意操作使整个商业界的IT资源完全不可靠达到3个月之久，2006年出了TJX事件——攻击者利用无线天线光顾了T.J.Maxx，盗走了大量的信用卡账户。
2008年，攻击率再创新高，据Vefizon.Business报告，2008年受到威胁的个人财务记录超过了2004、2005、2006和2007年的总和。
人们仍没有醒悟。
“正确”还是没有受到人们的重视，却得到寄生虫的青睐——这些坏家伙远程闯入系统，利用不正确的代码绕过安全设施、盗取财物。
对于用户和公司来说，这都是一个非常显著的问题。
事情这么糟糕，而工程师看到了什么？
一天结束时，地位低的开发人员必须把他听到的所有命令都转换为代码。
软件有许多工程要求：性能、可用性、可靠性等。
这些要求都有一个非常重要的特点：如果这些要求没有满足，它们就会变成非常明显的问题。
可是，安全问题却没有那么明显。
考虑下面的情形：假定软件有一个性能问题。
甚至未受过培训的工程师都会注意到，某个操作需要执行很长时间。
为了解决这个问题，工程师可以使用标准的数据集，找出运行过于频繁的代码块。

<<软件安全的24宗罪>>

内容概要

软件安全是一个不断变化的主题,不仅不断出现新的漏洞类型,而且出现了漏洞的各种变体.本书总结了目前最危险的24个安全漏洞,给出了丰富的漏洞示例,并且提供了相应的修复措施。

● 各种Web应用程序漏洞及修复措施 ● 各种实现漏洞及修复措施 ● 各种加密漏洞及修复措施 ● 各种联网漏洞及修复措施

作者简介

作者：（美国）Michael Howard （美国）David LeBlanc （美国）John Viega 译者：董艳 包战 程文俊Michael Howard是Microsoft公司Trustworthy Computing（TWC）Group（可信赖计算组）下属安全工程组的高级安全项目经理，负责管理整个公司的安全设计、编程和测试技术。
Howard是一位Security Development Lifecycle（SDL）构建师，SDL是一个提高微软软件安全性的过程。
Howard于1992年开始在微软公司工作，那时他在微软公司的新西兰分部，刚开始的前两年在产品支持服务小组为Windows和编译器提供技术支持，接着为MicrosoftConsulting Services提供技术支持，在此阶段，他为客户提供安全基础架构支持，并帮助设计定制的解决方案和软件开发。
1997年，Howard调到美国，为微软的Web服务程序InternetInformation Services的Windows分部工作，2000年开始担任目前的工作。
Howard是IEEE Security＆Privacy一书的编辑，经常在与安全相关的会议上发言，定期发表安全编码和设计方面的文章。
Howard与他人一起编写了6本安全图书，包括获奖书籍Writing Secure Code（第二版，Microsoft Press，2003年1、19 Deadly Sins ofSoftware Security（McGraw.Hill Professional出版社，2005年）、The Security Development Llyecycle（MicrosoftPress，2006年），最近出版的图书Writing Secure Code for WindoWS Vista（Microsoft Press，2007年）。
David LeBlanc博士目前是Microsoft Office Trustworthy Computing工作组的一位主要软件开发工程师，负责设计和实现Microsoft Office中的安全技术。
他还给其他开发人员提供安全编程技术方面的建议。
自从1999年加入微软公司以来，他一直负责操作网络安全，还是可信赖主动计算（Trustworthy computing Initiative）的创始人之一。
David与他人合著了获奖书籍WritingSecure Code（第二版，MicrosoftPress，2003年）、19 Deadly Sins of Software Security（McGraw-Hill Professional出版社，2005年）、WritingSecure Code for WindoWS Vista（Microsoft Press，2007年1，还发表了许多文章。
John Viega是McAfee的SaaS Business Unit的CTO，是19 deadly programmingflaws一书的作者，这本书引起了出版社和媒体的极大关注。
本书就是以该书为基础的。
他和其他人共同编写了许多其他关于软件安全的图书，包括Building Secure Software（Addison-Wesley Press，200 1年），Network Security with OpenSSL（O’Reilly Press，2002年），以及Myths of Security（O’Reilly Press，2009年）。
他负责许多软件安全工具，是Mailman（GNU邮件列表管理器）的第一作者，他为IEEE和IETF中的标准化做了大量的工作，还与他人一起开发了GCM（NIST已标准化的一种加密算法）。
John还是几家安全公司的安全顾问，包括Fortify和Bit9公司。
他拥有Virginia大学的硕士和学士学位。

<<软件安全的24宗罪>>

书籍目录

章节摘录

插图：第1章SQL注入1.1 漏洞概述SQL注入是一种非常严重的代码漏洞，它可以导致机器被入侵，敏感数据泄漏，最近，这种漏洞还会传播恶意软件。
而真正让人担心的是：受这些漏洞影响的系统通常都是电子商务系统或用来处理敏感数据或PII（personallyidentifiableinformation，个人身份信息）的应用程序。
从作者的经验来看，许多家用或者商用的数据库驱动应用程序都会有SQL注入的漏洞。
下面将清晰阐述这个漏洞的潜在威胁。
如果所建立的应用程序与数据库通信，且代码中有一个或多个SQL注入漏洞（无论您知道与否），就会把数据库中的所有数据置于危险之中。
如果不明白这句话的含义，请继续阅读。
有时，即使没有SQL注入漏洞，数据也会被入侵。
入侵数据库的一种常见方式是通过打开如下数据库端口，例如：·MicrosoftSQLServer的TCP／1433端口·Oracle的TCP／1521端口·IBMDB2的TCP／523的端口·MySQL的TCP／3306端口而进入一直处于打开状态的前门。
如果这些端口对Internet是开放的，则使用默认的系统管理员账户登录，很可能会引发灾难。
有数据就是有DATA。
SQL注入攻击的一个最大危害是攻击者可以获得隐私、PII或者敏感数据。
攻击者不需要使用系统管理员的身份，就可以盗取数据。
在一些国家、州或者工作单位里.如果发生了这种情况，当事人要负相应的责任。
例如，在加利福尼亚州，如果您负责的数据库被入侵，而数据库含有隐私或者个人数据，那么OnlinePrivacyProtectionAct（在线隐私保护法案）可能会让您吃官司；在德国，§9BDSG（FederalDataProtectionAct，联邦数据保护法案）要求为处理PII的系统提供恰当的组织上和技术上的安全保护。

媒体关注与评论

《软件安全的24宗罪——编程缺陷与修复之道》是由两位业界经验最丰富的专家撰写通过学习本书中给出的实践经验，读者就能够理解编写安全代码的具体含义.MichaelHoward和David LeBlanc在本书中展示了如何解决若干年前发布的代码出现的问题。

——Dan Kaminsky，IOActive渗透测试主管。

<<软件安全的24宗罪>>

编辑推荐

《软件安全的24宗罪:编程缺陷与修复之道》介绍了最新的安全问题，指出了最常见的设计和编码错误，解释了如何修复每个漏洞——更美妙的是，如何从一开始就避免出现这些错误。
《软件安全的24宗罪:编程缺陷与修复之道》的作者Michael Howard和David LeBlanc曾教授微软员工如何保护代码，他们与第一个发现19个致命编程漏洞的John Viega合作，探讨了最新的漏洞，并且增加了5个全新的漏洞。
这本实践指南涵盖了所有的平台、语言和应用程序类型。
由著名软件安全专家编写的安全漏洞专业书籍，发现和修复各种安全漏洞的最佳指导，丰富的安全漏洞示例以及修复措施，作者长期实践经验的总结。

<<软件安全的24宗罪>>

版权说明