

Mc
Graw
Hill Education

SQL Server SECURITY

From the
publisher of
**HACKING
EXPOSED**

"When Chip Andrews and David Litchfield write a book on SQL Server security, the only question you have to ask yourself is: How can I NOT afford to get this asap?"

— Joel Scambray, Co-Author, Hacking Exposed: Fourth Edition, Hacking Exposed Web Applications, and the upcoming Hacking Exposed Windows Server 2003, Senior Director of Security, Microsoft's MSN

Covers SQL Server 2000
and SQL Server 7 Security

SQL Server 安全性

Chip Andrews
(美) David Litchfield
Bill Grindlay
周俊杰

著
等译



清华大学出版社

SQL Server 安全性

Chip Andrews
(美) David Litchfield 著
Bill Grindlay

周俊杰 等译

清华大学出版社

北 京

Chip Andrews, David Litchfield, Bill Grindlay

SQL Server Security

EISBN: 0-07-222515-7

Copyright © 2003 by The McGraw-Hill Companies Inc.

Original language published by The McGraw-Hill Companies, Inc. All Rights reserved. No part of this publication may be reproduced or distributed by any means, or stored in a database or retrieval system, without the prior written permission of the publisher.

Simplified Chinese translation edition is published and distributed exclusively by Tsinghua University Press under the authorization by McGraw-Hill Education(Asia) Co., within the territory of the People's Republic of China only (excluding Hong Kong, Macao SAR and Taiwan). Unauthorized export of this edition is a violation of the Copyright Act. Violation of this Law is subject to Civil and Criminal Penalties.

本书中文简体字翻译版由美国麦格劳-希尔教育出版(亚洲)公司授权清华大学出版社在中华人民共和国境内(不包括中国香港、澳门特别行政区和中国台湾地区)独家出版发行。未经许可之出口视为违反著作权法,将受法律之制裁。未经出版者预先书面许可,不得以任何方式复制或抄袭本书的任何部分。

北京市版权局著作权合同登记号 图字: 01-2003-3809

版权所有, 翻印必究。举报电话: 010-62782989 13901104297 13801310933

本书封面贴有 McGraw-Hill 公司防伪标签, 无标签者不得销售。

图书在版编目(CIP)数据

SQL Server 安全性/(美)安朱丝(Andrews,C.), (美)里奇菲尔德(Litchfield,D.), (美)格兰德雷(Grindlay,B.)著; 周俊杰等译. —北京: 清华大学出版社, 2004.10

书名原文: SQL Server Security

ISBN 7-302-09266-4

I. S… II. ①安…②里…③格…④周… III. 关系数据库—数据库管理系统, SQL Server—安全技术 IV.TP311.138

中国版本图书馆 CIP 数据核字(2004) 第 085133 号

出 版 者: 清华大学出版社 地 址: 北京清华大学学研大厦

<http://www.tup.com.cn> 邮 编: 100084

社 总 机: 010-62770175 客 户 服 务: 010-62776969

组稿编辑: 曹 康

文稿编辑: 杜一民

封面设计: 康 博

版式设计: 康 博

印 装 者: 北京鑫海金澳胶印有限公司

发 行 者: 新华书店总店北京发行所

开 本: 185×260 印 张: 16.75 字 数: 347 千字

版 次: 2004 年 10 月第 1 版 2004 年 10 月第 1 次印刷

书 号: ISBN 7-302-09266-4/TP·6506

印 数: 1~4000

定 价: 35.00 元

本书如存在文字不清、漏印以及缺页、倒页、脱页等印装质量问题, 请与清华大学出版社出版部联系调换。联系电话: (010)62770175-3103 或(010)62795704

作者简介

Chip Andrews 是一位具有 12 年安全软件开发经验的软件工程师和开发顾问。同时还是 SQLSecurity.com 网站的所有者和维护者,该站点自 1999 年以来,一直致力于解决 SQL Server 的安全问题。Chip 的主要著作有 *Hacking Exposed: Windows 2000* (McGraw-Hill/Osborne) 和 *Special Ops: Host and Network Security for Microsoft, UNIX, and Oracle* (Syngress)。他也为一些杂志,如 *Microsoft Certified Professional*、*SQL Server Magazine* 和 *Dr. Dobbs Journal* 撰写论文,其论文主要解决 SQL Server 安全性和软件开发中的问题。Chip 已经成为 Black Hat (www.blackhat.com)安全会议上关于 Microsoft SQL Server 的安全问题和安全应用程序设计的重要发言人。

David Litchfield 是 NGS 软件公司的创始人。他是一位全球闻名的安全专家,专门研究 Windows NT 和 Internet 的安全问题。他对一些产品,例如 Microsoft 的 Internet Information Server 和 Oracle 的 Application Server 中 100 多个漏洞的发现与修补,已经帮助了全球无数站点加强了安全防护。David Litchfield 还是 Cerberus Internet Scanner (CIS; 以前是 NTInfoscan)的创作者,该扫描软件是当今最流行的一个免费的漏洞监测软件。除了 CIS 以外,David 还编写了一些实用程序,帮助查找和修补一些安全漏洞。David 是安全领域中很多重要技术文献的作者,其中 *Hacking Exposed* (McGraw-Hill/Osborne)一书中就引用到他在 *Exploiting Windows NT Buffer Overruns* 上的指导手册。

NGS 软件公司是在 2001 年创建的,它是在安全漏洞研究领域处于世界领先地位的技术公司。NGS 扮演着通信电子安全组织(Communications-Electronics Security Group, CESG)安全问题顾问的角色, CESG 是英联邦负责计算机安全的一个政府部门。除此以外,NGS 还签署了 CESG IT Health CHECK Service。NGS 利用它的独特技术,不仅保护了互联网的安全,还开发了一套边缘安全攻击工具,该工具能够检测标准软件和自定义程序中最新的安全缺陷。David Litchfield、Bill Grindlay 和 Chris Anley (本书的另一位合作者)都为 NGS 效力。

Bill Grindlay 是 NGS 软件公司的高级安全顾问。他曾是互联网安全系统软件工程师和 Defcom Internet Security 的安全入侵分析师。在没有提出网络渗透测试的时候,他是开发安全审核软件的开发小组的成员。他最近开发的项目包括 Microsoft SQL Server 的扫描软件 NGSSquirrel 和已经被广泛推广使用的漏洞检测仪 Typhon III。

Steve Wright 是 Nebraska 州 Omaha 市 Planet Consulting 有限公司的一位具有 15 年经验的资深顾问。他持有很多微软的证书,包括 MCDBA、MCSD、MCSE、MCAD

和 MCSA。Steve 的主要身份是使用微软技术的业务应用程序的设计师和技术顾问。Steve 已经开发的系统涵盖各种工业领域和应用学科范围,包括实时系统、数据库设计和管理、经纪人系统、保险系统、供应链管理系统和金融管理系统。Steve 还为微软开发那些没有发行的示例程序。Steve 持有数学和计算机科学的双学士学位,并拿到了计算机科学的硕士学位。

Ted Malone 现在是 Configuresoft 公司的高级工程师,该公司专为大型企业开发管理软件。在来 Configuresoft 工作以前, Ted 曾是专门研究电子商务安全技术的技术咨询公司 eKnowlogist 的合作者和执行主席。Ted 从一开始就与 SQL Server 合作,已经写了很多 SQL 安全和性能优化方面的文章。Ted 是在很多重要会议上都极具号召力的人物,如 SQL Server 专业协会(Professional Association for SQL Server, PASS)的年会、计算机分销商展览会和 IT 安全世界博览会和研讨会等。Ted 每月还为 Microsoft Rocky Mountain Region 撰写专栏,名为“The SQL Agent Man”。

Louis Garrett 是 Candler Park Computer Pros 公司的一位高级顾问和首席技术设计师。Louis 有 14 年的数据库开发和程序设计经验,这些开发经验涉及的平台从巨型机到 PC 机。他还花费了十年的时间,使用微软的工具设计和开发了复杂贸易系统。他持有微软的 MCSD、MCDBA 和 MCSE 证书,并即将成为 Microsoft Certified Trainer。Louis 现在专注于通过在多种数据源中集成各种信息,创建健壮的决策支持系统。在整个社会都更加依赖于相互连接的 PC 系统的时代,他还致力于推进数据库领域和应用程序安全领域的发展。

Erik Pace Birkholz (CISSP、MCSE)是 Foundstone 的首席顾问和高级培训师。Foundstone 是计算机安全咨询、漏洞评估分析软件和全球闻名的安全教学课程的提供者。他参加了三本畅销书的撰写,其中包括 *Hacking Exposed* 系列,并是 *Special Ops: Network and Host Security for Microsoft, Oracle and UNIX* 的第一作者。Erik 是一位杰出的会议发言人,他出席了 Black Hat Windows Security Briefings、Microsoft 和 The Internet Security Conference (TISC)会议。他是 Microsoft MEC 2002 会议的 VIP 发言人。在他的职业生涯中, Erik 还提出了一些黑客方法、工具和技术,并成为美国的一些政府职能机构,包括 FBI、NSA 和国防部的一些分支机构的重要成员之一。在加入 Foundstone 以前,他是 Internet 安全系统 ISS 的评估负责人,并兼任 Ernst & Young's National Attack 和 Penetration 小组的高级顾问。

前言

最近，计算机系统安全方面的书似乎都在讨论防火墙、网络、操作系统、Web 服务器、电子邮件服务器和域名服务器。但是，实际的情况正如我们现在已经体验到的一样，计算机系统安全所涉及的领域非常宽广——错误的配置不是导致安全问题的惟一原因。安全技术基于当今现代化的信息系统基础架构而建立，系统架构本身的各种缺陷为那些潜在的攻击者提供了肥沃的土壤。我们必须比以前任何时候都要更加清楚我们所面对的这个环境。

在安全领域中，有一件事情是非常滑稽的——对系统基础架构花费大量精力而对数据库则关注甚少。而实际上，攻击者的主要目标恰恰是数据库，这一点是合乎逻辑的——毕竟，数据库才是最终存储数据的地方，难道您不承认吗？当 Web 站点被攻击和电子邮件病毒的报道充斥媒体的时候，数据库的入侵问题好像仍然没有得到应有的重视。这是因为它们很少发生呢？还是因为只有一小部分人才知道它们正在发生呢？

创作本书的最初动机是发现 SQL Server 是一个常常被人们忽视的安全领域。SQL Server 功能强大，应用广泛，它已经找到了进入第三方软件、开发者的工作站和全球范围内重要后台终端系统的方法。在进行安全审核的时代，我们可以明确地告诉您，无论是从系统内部或外部威胁到系统安全的时候，SQL Server 都已经成为并继续成为最成功的突破目标之一。无论是那些远程开发者或在宾馆房间中连接 Internet 的 Microsoft Data Engine (MSDE) 的开发者，或者是在需要的时候，能很容易连接 Internet 的那些没有经过过滤的后台服务器的用户，他们在 DMZ 中使用测试数据库时，SQL Server 对那些热衷于安全问题的专家——包括保护者和攻击者而言都是一个丰富的资源。

本书的主要读者对象定位在计算机安全领域的专业人员、数据库管理员和兼负 SQL Server 服务器和服务器应用程序安全管理任务的所有人。本书详细地介绍了各种基础知识，因此学习本书没有必要事先了解整个 SQL Server 的内置安全机制。但是理解这些内置安全机制，对理解某些概念，例如加解密技术、报文嗅探技术和防火墙技术等安全概念，是非常有好处的。

在阅读本书的时候，您可能会注意到书中并没有讨论 SQL Server 的下一版本——名为 Yukon 的新版本的问题。本书的多位作者以及出版者正在忙于该产品 beta 版的开发工作。同样，我们依法在该产品公开发行之前去介绍该产品的任何信息。毫无疑问，我们正在与微软密切合作，以保证其官方的软件能够具有最高的品质，但

是在事情将会变得更好的时候，当然也有我们自己的一些想法。其中的有些想法会一直延续到产品中，而有些则不会。无论怎样，当 Yukon 发行以后，我们都将考虑推出第二版，以研究与 Yukon 相关的安全问题、优秀的经验和那些被禁用的脚本。我们感谢您对这些信息的期待和在这些法律问题上对我们的谅解。

我们希望这本书能激发您去关注企业中 SQL Server 的安全问题，并使用书中详细讲解的那些策略和过程来保护您的数据资产。SQL Server 对那些具有或不具有微软技术的攻击者而言永远都是一个攻击目标。对有些工具(例如 FreeTDS——www.freetds.org)的引入，已经使那些运行在 Unix 平台上的自动攻击工具也同样可以威胁到 SQL Server 的安全。

最后需要说明的是，不要因为本书所列举的安全问题而拒绝使用 SQL Server。我们已经在多种操作系统中使用过多种数据库，发现它们都有自己不同的安全缺陷。您的目标应该是尽可能地利用您选择使用的具体技术的问题来提高自身的安全性，并帮助您规划、开发和这些系统的最终配置。如果在您的冒险经历中，发现了一些您觉得值得人们注意的问题的话，请将您的建议发送到 sqlwish@microsoft.com。我们诚恳地希望，您天才的想法能够帮助您自己和我们大家共同提高 SQL Server 的安全性能。

本书的结构如下：

- 第 1 章回顾了 SQL Server 的发展历史。在理解为什么有些功能依然存在于 SQL Server 之中，或您在哪里可以找到关于那些没有归档的特性和一些陈旧的表列(例如在古老的 Sybase 文件中)等问题时，了解 SQL Server 的历史就显得非常重要。另外，我们还会讨论 SQL Server 安全的现状和最新的一些像瘟疫一样的蠕虫病毒。这些背景知识有助于您理解掌握本书中的一些材料，以及处理将来可能产生的一些安全问题的方法。
- 第 2 章详细介绍了攻击者是怎样对 SQL Server 进行攻击的，清晰地解释了 SQL Server 为什么会成为一个主要的攻击目标。直接介绍 SQL Server 攻击过程的原因，是为了给本书剩下的内容提供一些上下文信息。学会在偶然事件发生时如何保护系统是一件非常有意思的事情。将这些信息预先写出将会使您能持续地学习和关注这个主要的目标——安全而可靠的 SQL Server 安装。
- 第 3 章详细审核了 SQL Server 的安装过程。安装是 SQL Server 安全防护工作的起点。本章对于在安装过程中需要考虑的问题进行了深入的阐述。众多令 SQL Server 饱受折磨的蠕虫病毒，通过正常的安装，已经得到很好的遏制。当您阅读本章的时候，别忘了您会多次用到带有多种第三方产品的 MSDE 安装。一定要询问您的软件销售商是否使用 MSDE，这样您就可以通过使用恰当的服务包、配置设置和关闭脚本等方法锁定(Lockdown)安装完毕的 SQL Server。

- 第4章对 SQL Server 怎样在网络上进行通信和怎样保护这些通信通道进行了深入详细的介绍。本章的重点是清晰地介绍 SQL Server 怎样通过网络进行通信,以及您能采取哪些措施来确保那些不必要并具有潜在威胁的网络库不再保留在机器上,给入侵者攻击的机会。第4章的另外一个关键概念是理解 SQL Server 安装的目的,确定网络库是否应该在服务器上启用。基本的方针就是只启用完成程序目标所必需的程序功能,而同时尽可能地减少攻击的范围。
- 第5章详细地介绍了怎样进行与保护服务器安全相关的授权和认证工作。本章也涉及到 SQL Server 安全工作中一些核心和神秘的内容,详细地告诉您应该在服务器端采取什么样的措施才能保护您的数据库应用程序的安全。关于 SQL Server 的一个真正的难题是怎样使用各种 SQL Server 的认证机制,以及在多种环境下如何使用这些认证机制。我们将详细地讨论其中复杂的关系,使您可以对采用什么样的认证模式来满足您的需求做出正确的选择。除了认证以外,本章还将介绍 SQL Server 的授权机制,这样您就可以有效地将权限委派给您信任的用户,而不用将每一个人都变为系统管理员。没有绝对合适的权限或绝对错误的认证/授权模式——只有能够满足特定应用程序安全级别需求的模式才是最佳的模式。
- 第6章介绍企业集成技术,例如复制、多服务器系统管理等,使您能很好地略过 SQL Server 文档中(被称为 SQL Server Books Online)那些草率的解释,并准确地解释必须采取什么措施来保护企业中的 SQL Server。我们将审核在启用这些技术的时候,可能会面临的挑战,以及应该怎样处理这种挑战。另外,我们将指出您在企业中部署这些技术的过程中将会面临的所有可能的陷阱。记住,我们并非试图劝说您们不要使用这些技术,或暗示如果您启用它们的时候,会受到怎样的攻击。本章的基本出发点是,您应该了解正在配置使用的技术,如果它们配置不当的话,它会怎样被别人发现,怎样被别人利用去做一些对您不利的事情。要放心地去使用这些技术,但是同时一定要睁大您的眼睛。
- 第7章深入介绍了各种审核技术。它详细地介绍了怎样使用 SQL Server 内置工具配置入侵检测,怎样进行每天活动的鉴定。到这里为止,如果您所做的所有决策都正确,仍然可能面临应用程序的安全问题,或一些新的 SQL Server 攻击的问题,这些问题可能在您有机会屏蔽它们之前就已经产生了。在这些情况下,您需要一个允许您检测并做出反应或能够证明那些潜在的攻击或系统滥用的登录审核策略。一般来讲,SQL Server 以前有一些很弱的审核功能,但是随着 C2 级审核功能的引入,为本地审核功能带来了希望。本章介绍了用户应该怎样使用这些新的功能,并介绍了一些关于用户怎样处理数据这方面的知识。

- 第 8 章讨论了怎样进行加密，和应用程序的开发者该怎样扩展 SQL Server 的功能，以保证他们的数据能够进行安全的存储和传输的问题。在介绍怎样进行加密以前，本章先花了很多篇幅介绍加密的目的和可以用于保护数据的各种方法。讨论加密技术的原因是让您首先理解加密有什么作用，哪些加密措施是没有意义的。记住，加密不是一劳永逸的方法，只有通过适当的加密方法和程序进行仔细的检查，您才可以对在哪里使用加密技术和使用怎样的加密技术做出正确的选择。
- 第 9 章深入地介绍了 SQL 注入式攻击是怎样发生的。程序的开发者需要做哪些工作来保护程序免受这种流行而又阴险的攻击。本章抛开对 SQL Server 展开和配置细节问题的讨论，只关注当前的安全专家正面对的那些非常普遍的问题。SQL 注入攻击特别阴险，因为它们超越了所有已经深入到保护 SQL Server 安装领域的各种完善的计划，允许未受到信任的用户通过有漏洞的程序，直接在 SQL Server 中注入代码。本章不仅介绍 SQL 注入是怎样发生的，还介绍了怎样在您的程序中检测和防止这种注入。
- 第 10 章对应用程序层上的安全问题进行了深入的介绍，并给出了开发安全的 SQL Server 应用程序的一个非常详细的流程图。记住，开发一个真正安全的应用程序、仅仅检查并删除 SQL 注入漏洞是不够的。一个经过谨慎的构造策略、适当的计划、开发和配置的应用程序，对以后可能发生的各种问题都会有预防作用的。本章通过强调在开发过程的早期就启动对安全计划的研究，强调了这样的一个谚语“预防时的一盎司等于治疗时的一英镑”。前期考虑应用程序的安全问题，比后期对它进行各种修补要简单得多。
- 附录 A 详细地列举了 SQL Server 中一些很容易产生漏洞的系统存储过程和扩展存储过程，并介绍了它们的作用和使用限制。其中的很多存储过程都是非常有用的，但是通常只是在一些高级的工具，例如企业管理器和查询分析器或服务包的安装中使用。因为这些存储过程主要是由系统管理员使用的，所以要将其从权限较低的用户(例如公共角色的成员)中删除。该附录允许您决定将哪些存储过程移除，同时仍然允许您的应用程序和用户能够执行正常的操作。像大多数事情一样，这将包括很多很好的计划和相当可观的测试。一定要确保您在系统环境中移除这些存储过程以前进行过详细的测试。我们已经测试过那些能够产生极大危害的存储过程，但是并不是所有的存储过程都产生相同的结果。
- 附录 B 概括了与 SQL Server 一起使用的各种技术。其中很多技术可以成为 SQL Server 潜在攻击、缓冲区溢出或误配置攻击的携带者。理解您在配置这些产品时可能碰到的问题是非常重要的，因为您可以决定在您的企业中具体采用哪些技术。记住，这些信息都是概括性的。虽然该附录介绍了一些通用的技术，并对各个安全问题的内涵都进行了逐一的检查，但是由于本附录篇

幅的限制，这里列出的技术细节还只是概括性的。如果您需要这些技术的更详细的信息，请在互联网和其他书上查找相应的参考信息。本附录的目标是让您在保护系统安全的时候，能将 SQL Server 作为需要考虑的多层安全问题中的一层。

- 附录 C 主要介绍了连接字符串和它们在保证应用程序安全中的重要性。一个不健壮的连接字符串可能会暴露出很多重要的机密，或阻止用户对密码进行频繁地更改，甚至是限制您的应用程序的可扩展性。我们主要关注用于 ADO 技术(ActiveX Data Objects)和在 OLE DB Provider for SQL Server 的连接字符串，但是这些设置也会在其他提供者中用到。您在这一附录中将会学到的一个关键概念是怎样定制连接字符串来满足复杂的网络系统(例如防火墙)的需求，以及限制应用程序使用加密技术和保护 TCP 端口安全的安全规则。最后，在该附录中，我们还介绍了应该在哪里存储连接字符串的问题和什么时候使用加密的连接字符串的问题。本附录还对每一种连接字符串的存储方法，以及它们的优点、不足和建议使用的方法等给出了详细的对照。
- 附录 D 提供若干列表，您可以用它们锁定新的 SQL Server 安装，维护与监控已经配置好的 SQL Server 系统。记住，并不是所有的措施对每一个程序都适用。其基本的指导思想是移除那些您能够确定在系统中使用频率不高的功能，而且在需要的时候，可以将它们添加进来。该核对列表可以适用于 SQL Server 和 MSDE。对那些带有 SQL Slammer 蠕虫的发行版，我们知道的是怎样去安装流行的 MSDE，并将它们打上相同版本的补丁，并对标准版或企业版的 SQL Server 的配置进行处理。

最后，再次感谢您使用这本书。我们希望在随后的实践中，您能真正地发现这本书的价值。请记住，我们已经尽力来保证书中每一个知识点的准确性，但是因为错误在所难免。如果您发现了书中的错误，请立即通知我们，我们会在以后的版本中尽快地进行更正。最后，代表为本书付出宝贵时间和巨大努力的所有作者说一句话，那就是希望在保护您的 SQL Server 安全的工作中，能做得更好！

目 录

第 1 章 SQL Server 安全：基础知识	1
1.1 SQL Server 的历史	1
1.2 SQL Server 的版本	4
1.3 通用数据库安全技术	5
1.4 SQL Server 的安全漏洞	6
1.4.1 病毒解析：Slammer 为什么会如此成功	7
1.4.2 预防另一个可能的 Slammer	8
1.5 小结	9
第 2 章 围攻 SQL Server：攻击过程分析	10
2.1 挑选理想的工具	11
2.2 数据还是主机	12
2.3 无需认证的攻击	12
2.3.1 利用缓冲区溢出	12
2.3.2 SQL 监控器端口攻击	13
2.3.3 “hello” 故障	15
2.3.4 猎取密码	15
2.4 需要认证的攻击	18
2.4.1 缓冲区溢出	19
2.4.2 扩展存储过程	19
2.4.3 绕过访问控制机制	21
2.5 资源	24
2.6 代码列表 1	24
2.7 代码列表 2	31
2.8 代码列表 3	34
第 3 章 SQL Server 的安装技巧	36
3.1 规划安装过程	36
3.1.1 数据安全	37
3.1.2 容错能力	37
3.1.3 备份方案	37

3.1.4 灾难恢复	38
3.2 操作系统的因素	38
3.3 运行安装程序	39
3.4 锁定服务器	42
3.5 核对列表	45
第 4 章 网络库和安全连接	47
4.1 客户/服务器连接	47
4.2 安全套接字层	49
4.2.1 SSL 基础	49
4.2.2 SSL 的配置	52
4.3 SQL Server 网络库	53
4.3.1 主网络库	53
4.3.2 从网络库	54
4.4 配置连接	55
4.4.1 服务器网络实用程序	56
4.4.2 客户端网络实用程序	57
4.5 优秀的经验	59
4.5.1 永远不要向互联网暴露您的 SQL Server 端口	59
4.5.2 尽可能使用 TCP/IP 网络库	60
4.5.3 在确实需要时再配置网络库	60
4.5.4 使用 128 位的 SSL 连接而不要使用 40 位的 SSL 连接	61
4.5.5 设置一个 SSL 证书以确保进行安全登录	61
4.5.6 对高敏感的数据进行强制加密	61
4.5.7 配置 TCP/IP 的时候, 请使用“隐藏服务器”选项	61
第 5 章 认证和授权	62
5.1 认证(Authentication)	63
5.1.1 登录	63
5.1.2 数据库用户	69
5.1.3 角色	73
5.2 授权(Authorization)和许可(Permissions)	80
5.2.1 GRANT、REVOKE 和 DENY	81
5.2.2 审核访问(Auditing Access)	87
5.2.3 所有权链(Ownership Chains)	87
5.3 Syslogins、Sysprotects、Syspermissions 和其他特殊账户	89
5.3.1 SID 与 SUID	90

5.3.2	syslogins 和 sysxlogins	90
5.3.3	sysusers	90
5.3.4	syspermissions	91
5.3.5	sysprotects	91
5.4	优秀的经验	91
5.4.1	Windows 活动目录：集中式管理	92
5.4.2	SQL Server 集中式角色管理	93
5.4.3	挑选适当的方法	94
第 6 章	企业中的 SQL Server	95
6.1	SQL Server 的复制	95
6.1.1	复制操作概论	95
6.1.2	复制时要考虑的安全问题	99
6.2	多服务器系统管理	105
6.3	活动目录集成	109
第 7 章	审核与入侵检测	112
7.1	案例分析	112
7.1.1	RetailCo 数据库的运作规模	113
7.1.2	RetailCo 的管理结构	113
7.1.3	安全策略	113
7.1.4	怪异之事和合乎法律程序的检查	113
7.1.5	结论	114
7.2	SQL Server 审核	114
7.2.1	启用标准的审核	114
7.2.2	C2 级审核	118
7.2.3	扩展审核功能	121
7.2.4	使用内置跟踪函数配置手动审核	122
7.3	SQL Server 警报	126
7.3.1	配置 SQL Server 警报	127
7.3.2	将 SQL Server 警报用作入侵检测系统	130
第 8 章	数据加密技术	133
8.1	加密技术概览	134
8.2	哈希算法	135
8.3	Salt(Salts)	137
8.4	密钥管理	137

8.5	内置加密函数	138
8.6	加密自定义存储过程	139
8.7	加密 SQL Server 表数据	140
8.8	SQL Server 网络通信的加密	141
8.9	中间层加密	143
8.10	第三方 COM 组件	144
8.11	加密 API	144
第 9 章	SQL 注入：当防火墙鞭长莫及时	148
9.1	SQL 注入简述	148
9.2	案例研究：在线外贸交易系统	149
9.2.1	审核技术	149
9.2.2	漏洞识别	149
9.2.3	攻击系统	150
9.2.4	案例分析	154
9.3	高级主题	154
9.3.1	利用时间延迟提取有用信息	154
9.3.2	系统级攻击	155
9.3.3	为什么 SQL Server 容易受到 SQL 注入的攻击	157
9.3.4	攻击方式	157
9.4	SQL 注入的防护	160
9.4.1	输入验证(Input Validation)	160
9.4.2	鉴别不好的设计	162
9.4.3	增强设计	163
9.5	优秀的经验	165
9.5.1	设计	165
9.5.2	开发/实现	165
9.5.3	QA/测试	165
9.5.4	配置	166
第 10 章	安全体系结构	167
10.1	深度防护	167
10.2	安全性需求	168
10.2.1	收集需求	169
10.2.2	已有的环境	169
10.2.3	理解应用程序的安全需求	169
10.2.4	保护您的应用程序	170

10.3	规划	170
10.3.1	依托技术做决策	171
10.3.2	依托评审过程做决策	171
10.3.3	依托代码标准做决策	171
10.3.4	防止安全水准的下降	172
10.4	开发	172
10.4.1	良好的编码习惯	172
10.4.2	编写存储过程的一些良好的习惯	173
10.4.3	输入验证	174
10.4.4	推荐的开发防护措施	176
10.4.5	一些不好的编码习惯及其克服方法	176
10.5	测试	177
10.5.1	测试的手段	177
10.5.2	模糊化处理(Fuzzing)	179
10.5.3	一些技巧	179
10.5.4	深度覆盖	180
10.5.5	结果报告	180
10.6	配置	181
10.6.1	配置的规划	181
10.6.2	过程的构造	181
10.6.3	问题的解决方法	182
10.7	维护	182
10.7.1	安全+不安全=不安全	183
10.7.2	阅读日志	183
10.7.3	注意收集证据	183
附录 A	系统存储过程与扩展存储过程	184
A.1	限制存储过程的风险	185
A.1.1	将攻击范围压缩到最小	185
A.1.2	将访问权限降到最低	186
A.1.3	将应用程序运行时的账户权限调整到最小	186
A.2	存储过程的攻击策略	187
A.2.1	创建特洛伊木马存储过程	187
A.2.2	利用社会工程学使用系统存储过程	188
A.3	高危险性的系统存储过程和扩展存储过程	189
A.3.1	访问注册表的扩展存储过程	189

A.3.2	暴露 SQL Server 开发环境中的存储过程	190
A.3.3	OLE 自动化扩展存储过程	191
A.3.4	访问操作系统的存储过程	192
A.3.5	使用电子邮件的存储过程	195
A.4	防御策略	196
A.4.1	删除不需要的存储过程	196
A.4.2	撤销存储过程的公共访问权限	198
A.4.3	审核和跟踪对于 SQL Server 源代码和许可的变更	199
附录 B	影响 SQL Server 安全的一些其他技术	200
B.1	Visual Studio、Microsoft Office 和 COM 连通性工具	200
B.1.1	Visual Studio	201
B.1.2	Microsoft Office	201
B.1.3	数据访问 API	201
B.2	SQL Server Mail 接口	205
B.2.1	SQL Mail	205
B.2.2	SQLAgent Mail	206
B.3	Internet 信息服务集成	207
B.4	SQL Server 开发员和系统管理员工具	209
B.4.1	SQL-DMO	209
B.4.2	SQL-NS	210
B.4.3	DB-Library API	211
B.4.4	ISQL.exe 和 OSQL.exe 工具	211
B.4.5	分发组件	211
B.4.6	服务器的连接	211
B.4.7	数据传输服务 DTS	212
B.4.8	批复制 DTS 任务	213
B.4.9	扩展存储过程的开发	213
B.4.10	列表数据流 TDS	214
附录 C	连接字符串	215
C.1	连接属性	215
C.2	连接字符串示例	218
C.3	连接字符串的存放位置	219
C.3.1	Web.config (ASP.NET) 或 global.asa (ASP) 文件	220
C.3.2	注册表	221
C.3.3	使用 DPAPI 加密的文本文件	222

C.3.4	UDL 文件	224
C.3.5	包含文本文件	225
C.3.6	COM+目录	226
附录 D	安全核对列表	229
D.1	SQL Server 版本核对列表	229
D.2	Post-Install 核对列表	232
D.3	维护核对列表	246