

DATABASE SECURITY

Alfred Basta, Melissa Zgola, Dana Bullaboy, Thomas L. Whitlock Sr.



PREPARING TOMORROW'S
INFORMATION
SECURITY
PROFESSIONALS



Database Security

Alfred Basta, Ph.D.

Melissa Zgola, M.A., M.S.I.S.

Contributions made by Dana Bullaboy



Australia • Brazil • Japan • Korea • Mexico • Singapore • Spain • United Kingdom • United States

Copyright 2011 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

This is an electronic version of the print textbook. Due to electronic rights restrictions, some third party content may be suppressed. Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. The publisher reserves the right to remove content from this title at any time if subsequent rights restrictions require it. For valuable information on pricing, previous editions, changes to current editions, and alternate formats, please visit www.cengage.com/highered to search by ISBN#, author, title, or keyword for materials in your areas of interest.

Database Security**Alfred Basta and Melissa Zgola**

Vice President, Editorial: Dave Garza

Director of Learning Solutions:
Matthew Kane

Executive Editor: Stephen Helba

Managing Editor: Marah Bellegarde

Product Manager: Natalie Pashoukos

Editorial Assistant: Jennifer Wheaton

Vice President, Marketing:
Jennifer Ann Baker

Marketing Director: Deborah S. Yarnell

Associate Marketing Manager:
Erica Ropitzky

Production Director: Wendy Troeger

Production Manager: Andrew Crouth

Senior Content Project Manager:
Andrea Majot

Senior Art Director: Jack Pendleton

© 2012 Course Technology, Cengage Learning

ALL RIGHTS RESERVED. No part of this work covered by the copyright herein may be reproduced, transmitted, stored or used in any form or by any means graphic, electronic, or mechanical, including but not limited to photocopying, recording, scanning, digitizing, taping, Web distribution, information networks, or information storage and retrieval systems, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the publisher.

For product information and technology assistance, contact us at
Cengage Learning Customer & Sales Support, 1-800-354-9706

For permission to use material from this text or product,
submit all requests online at cengage.com/permissions
Further permissions questions can be emailed to
permissionrequest@cengage.com

Example: Microsoft® is a registered trademark of the Microsoft Corporation.

Library of Congress Control Number: 2011930892

ISBN-13: 978-1-4354-5390-6

ISBN-10: 1-4354-5390-5

Course Technology20 Channel Center Street
Boston, MA 02210
USA

Cengage Learning is a leading provider of customized learning solutions with office locations around the globe, including Singapore, the United Kingdom, Australia, Mexico, Brazil, and Japan. Locate your local office at: international.cengage.com/region

Cengage Learning products are represented in Canada by Nelson Education, Ltd.

For your lifelong learning solutions, visit www.cengage.com/coursetechnology

Purchase any of our products at your local college store or at our preferred online store www.cengagebrain.com

Visit our corporate website at cengage.com.

Microsoft and the Office logo are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Course Technology, a part of Cengage Learning, is an independent entity from the Microsoft Corporation, and not affiliated with Microsoft in any manner.

Any fictional data related to persons or companies or URLs used throughout this book is intended for instructional purposes only. At the time this book was printed, any such data was fictional and not belonging to any real persons or companies.

The programs in this book are for instructional purposes only. They have been tested with care, but are not guaranteed for any particular intent beyond educational purposes. The author and the publisher do not offer any warranties or representations, nor do they accept any liabilities with respect to the programs.

Printed in the United States of America**1 2 3 4 5 6 7 12 11**



INTRODUCTION	xi
CHAPTER 1	
Security and Information Technology	1
CHAPTER 2	
Database Review	43
CHAPTER 3	
Database Installation 1: MySQL	77
CHAPTER 4	
Database Installation 2: Microsoft SQL Server	113
CHAPTER 5	
Database Installation 3: Oracle	145
CHAPTER 6	
Password, Profiles, Privileges, and Roles	173
CHAPTER 7	
SQL Injection I: Identification	201
CHAPTER 8	
SQL Injection Exploitation and Defense	219
CHAPTER 9	
Security Auditing	241
CHAPTER 10	
Security Testing	261
GLOSSARY	281
INDEX	291



Table of Contents

INTRODUCTION	xi
CHAPTER 1	
Security and Information Technology	1
Why Database Security?	3
A Secure Data Environment	4
Database Security Objectives	5
Who Are We Securing Ourselves Against?	7
Hackers	7
Social Engineers	9
Computer Users	9
Network and Database Administrators	10
The Internet	10
Misleading Applications	15
E-Mails	15
Instant Messages	17
Tweets	17
Malware	18
Computer Viruses	18
Worms	21
Trojan Viruses	22
Bots	24
Security Architecture: A Never-ending Cycle	24
Phase 1: Assessment and Analysis	25
Phase 2: Design and Modeling	25
Phase 3: Deployment	26
Phase 4: Management and Support	27
Global Policies for the Database Environment	27
Security Policies	27
Update and Upgrade Management	28
Backup Management Plan	31
The Disaster Plan	33
Chapter Summary	34
Key Terms	35
Review Questions	39
Case Projects	39
Hands-On Projects	40
CHAPTER 2	
Database Review	43
Database Defined	44
Database Structure Components	45
Tables	45
Keys	45
Queries	48
Database Models	48
Flat Model	48
Hierarchical Model	49

Network Model	50
Relational Database	50
Object-Oriented Databases	51
Object-Relational Database	53
Relationships	53
Database Types	54
OLTP	54
OLAP/DSS	54
Database Management Systems	54
Oracle	55
MySQL	55
Microsoft SQL	55
Database Similarities	55
Read Consistency	55
Query Management	56
Oracle Architecture	57
The Instance and the Database	57
The Physical Structure	58
The Memory Structure	58
The Processes	60
MySQL Architecture	60
Database Connection Manager	61
Query Engine	62
Transaction Manager	62
Storage Management	63
The Storage Engine	63
Microsoft SQL Server Architecture	65
Architecture and Engines	65
The Physical Structure	66
Memory Management	67
Buffer Management	69
Threads and Processes	69
Chapter Summary	70
Key Terms	71
Review Questions	74
Case Projects	75
Hands-On Projects	75

CHAPTER 3

Database Installation 1: MySQL	77
Preinstallation Preparation	79
Choosing a Distribution Format	79
Choosing a Version of MySQL	80
Supported Platforms	83
Locating Help	83
Downloading MySQL	84
Installation	85
Installing on Windows	85
Adding a MySQL Port in Windows Vista	86
Adding a MySQL Port in Windows 7	86
Installation Instructions	87

Installing on UNIX	93
Installing UNIX Binary Distributions	93
Installing Tar.gz	93
Installing Linux Binary Distributions Using RPM	94
Installing RPM	94
Configuration	95
Configuring MySQL on Windows	95
Standard Configuration Using the Windows Configuration Wizard	96
Detailed Configuration Using the Windows Configuration Wizard	98
Configuring MySQL on UNIX	106
Using a Configuration Script	106
Setting Passwords	107
Additional Security Suggestions	107
Passwords	108
Account Access and User Privileges	108
Network Connection Administration	108
Chapter Summary	108
Key Terms	109
Review Questions	110
Case Projects	110
Hands-On Projects	111
 CHAPTER 4	
Database Installation 2: Microsoft SQL Server	113
Planning for a Microsoft SQL Server Installation	115
Meeting the Requirements	115
Hardware Requirements	115
Supported Platforms	119
64-bit and 32-bit	119
Operating System Requirements	119
Other Software Prerequisites	120
Network Resource Requirements	120
Making the Difficult Decisions	120
Choosing an Edition	121
SQL Server Features and Components	122
Licensing Options	124
Locating Help	125
Help Resources	125
Installation	126
The Server Installation Center	126
The Installation Page	127
The Maintenance Page	127
The Tools Page	127
The Resources Page	128
The Advanced Page	128
The Options Page	128
Step-by-Step Installation	128
Additional Security Considerations for SQL Server 2008	140
Security Steps Prior to Installation	140
During Installation	140
After Installation	141

Chapter Summary	141
Key Terms	143
Review Questions	143
Case Projects	143
Hands-On Projects	144
 CHAPTER 5	
Database Installation 3: Oracle	145
Planning for an Oracle Deployment	147
Checking the Requirements	149
Hardware Requirements	149
Operating System Requirements	150
64-bit and 32-bit	150
Other Software Requirements	151
Network Resource Requirements	152
Preinstallation Decisions	152
Choosing an Edition	152
Oracle Extra-Cost Enterprise Edition Options	154
Licensing Options	155
Free Unlimited Downloads of Oracle	157
Locating Help	157
Installation	158
The Oracle University Installer	158
Step-by-Step Installation for Windows	158
Quick Installation for UNIX-based Systems	166
Additional Security Considerations for an Oracle Database	166
Security Checklist	167
Take Advantage of Oracle's Security Suite	168
Password Policies and User Accounts	168
Chapter Summary	169
Key Terms	171
Review Questions	171
Case Projects	171
Hands-On Projects	172
 CHAPTER 6	
Password, Profiles, Privileges, and Roles	173
Authentication	175
Operating System Authentication	176
Database Authentication	176
Network or Third-Party Authentication	176
Database Vendor-Specific Authentication Components	178
Password Policies	179
Database-Enforced Password Policies	180
Written Password Policies	180
Database Vendor-Specific Password Management	182
Authorization	183
User Account Management	184
Default User Accounts	184

Adding and Removing Users	185
User Privileges	186
Roles	189
Inference	193
Examples of Inference	193
Minimizing Inference	194
Chapter Summary	196
Key Terms	197
Review Questions	198
Case Projects	199
Hands-On Projects	199
 CHAPTER 7	
SQL Injection I: Identification	201
Understanding SQL Injections	202
Injections and the Network Environment	203
Identifying Vulnerabilities	205
Inferential Testing for Locating SQL Injections	205
Using HTTP	206
Determining Vulnerability Through Errors	207
Typical Conditions with No Error	208
Typical Conditions with Typical Error	209
Injection Conditions with No Error	210
Injection Conditions with Injection-Caused Error	211
Generic Error Messages	211
Direct Testing	212
Using the Code for Locating SQL Injections	212
Source Code Analysis	212
Tools for Searching Source Code	213
String-Based Matching	213
Data Flow Analysis	214
Lexical Analysis	214
Chapter Summary	214
Key Terms	215
Review Questions	215
Case Projects	216
Hands-On Projects	217
 CHAPTER 8	
SQL Injection Exploitation and Defense	219
Exploitation and Information Gathering	221
Information That Aids in Exploitation	221
Extracting the Real Data	225
Statement Exploits	225
Using UNION	226
Using Conditions	228
Large-Scale Extraction	229
Advanced Techniques	231
Exploitation of Privileges and Passwords	232
Identifying Privileges	232

Obtaining Passwords	233
Obtaining Privileges	234
Defending Against Exploitation	235
Using Bond Parameters	236
Sanitizing Data	236
Restricting and Segregating Databases	236
Security-Conscious Database Design	236
Diligent Monitoring	237
Chapter Summary	237
Key Terms	238
Review Questions	238
Case Projects	239
Hands-On Projects	239
CHAPTER 9	
Security Auditing	241
Security Auditing	243
Audit Classification	243
The Goal of an Audit	244
The Auditing Process	245
Database Auditing	249
Preparation and Planning for a Database Security Audit	249
The Database Audit	251
Reporting a Database Security Audit	253
Vendor-Specific Auditing Information	254
Chapter Summary	256
Key Terms	257
Review Questions	258
Case Projects	258
Hands-On Projects	259
CHAPTER 10	
Security Testing	261
Security Testing	263
Security Testing Classification	264
The Goal of Security Testing	265
Testing Methodology	266
Planning and Preparation Phase	266
Execution Phase	267
Escalating Privileges	273
Reporting Phase	274
Chapter Summary	274
Key Terms	276
Review Questions	277
Case Projects	278
Hands-On Projects	278
GLOSSARY	281
INDEX	291



Introduction

Over the last several decades, we have made great advancements in maintaining the confidentiality, integrity, and availability of our networked environments. These achievements are greatly due to the strides that have been made within our educational degree programs. Security research is funded at the highest rates in history, and security courses have become fundamental requirements in almost every IT-related program. Unfortunately, very little emphasis is placed on database security and as a result, IT and security professionals are left uninformed and underprepared to protect their company's most precious assets, their databases. Databases are the most valuable resources that we have. They contain our identities and hold our deepest secrets. Individuals, companies, and even countries could not exist without database security—it is our livelihood that is at stake in this technologically dependent world.

Approach and Audience

This textbook is a detailed guide to maintaining the confidentiality, integrity, and availability of a database environment. From preinstallation to postsecurity auditing, this book provides a comprehensive and in-depth explanation of database security strategies and offers general IT skills and the security know-how that professionals must have to face the growing number of threats to network security.

It has been written for information system and security administrators and analysts and emphasizes best practices in database security strategies. This book does not assume prior knowledge of databases and has been written in a casual style for both technical and nontechnical readers. It can be used in almost any basic or advanced information security or database administration course.

Organization and Chapter Descriptions

- **Part I:**
 - **Chapter 1** provides a full understanding of security and information technology. It defines the different types of security, intruders, attack strategies, and viruses. Security architecture is explored, along with global policy and disaster plans.
 - **Chapter 2** offers a well-rounded discussion of databases, from the definition of basic schema objects to an in-depth description of the architecture of an Oracle, MySQL, and SQL database.
- **Part II:**
 - **Chapters 3, 4, and 5** provide step-by-step installation guides and security practices for different vendors. Chapter 3's focus is MySQL, Chapter 4 focuses on SQL Server, and Chapter 5 focuses on Oracle 11g. With the foundation provided in the first five chapters, the student is well prepared to move on to much more advanced security concepts.
- **Part III:**
 - **Chapter 6** identifies authentication and authorization by covering topics such as profiles, privileges, and roles and by offering insight into how they are administered through specific vendors such as MySQL, SQL Server, and Oracle.
 - **Chapters 7 and 8** investigate the rarely explored topic of SQL injection. Based on cutting-edge research, Chapter 7 teaches learners how to identify SQL injection vulnerability and common injection strategies, while Chapter 8 explores examples of exploits and informs readers of defense techniques.
- **Part IV:**
 - Finally, **Chapters 9 and 10** introduce students to database security testing and auditing, covering vendor-specific processes.

Features

- *Thoughtfully organized*—The text is divided into four main parts to make finding and comparing implementation processes quick and easy.
- *Implementation focuses*—Addressing widely used database implementation, this text demonstrates how to prevent and solve problems with a practical mind-set.
- *SQL injection discussion*—SQL injection poses great challenges to database and security professionals, and *Database Security* is one of the only books on the market to address the topic.
- *Chapter Objectives*—Each chapter begins with a detailed list of the concepts to be mastered. This list gives you a quick reference to the chapter's contents and serves as a useful study aid.
- *Security In Your World*—In each chapter, real-world examples demonstrate viable solutions for various types of threats and intrusions to SQL Server, Oracle, and MySQL databases.
- *Chapter Summary*—Each chapter ends with a summary of the concepts introduced in the chapter. This is a helpful tool for reviewing the material covered in each chapter.
- *Key Terms*—All terms in the chapter introduced with bold text are gathered together in the key terms list at the end of the chapter, with full definitions for each term. This list encourages a more thorough understanding of the chapter's key concepts and is a useful reference.

- **Review Questions**—The end-of-chapter assessment begins with review questions that reinforce the main concepts and techniques covered in each chapter. Answering these questions helps ensure that you have mastered important topics.
- **Case Projects**—One of the best ways to reinforce learning about database security is to practice using the many tools security professionals use. The case projects at the end of the chapters give you practice in applying what you have learned.
- **Hands-On Projects**—Each chapter closes with one or more hands-on projects that help you evaluate and apply the material you have learned. To complete these projects, you must draw on real-world common sense as well as your knowledge of the technical topics covered to that point in the book.

Text and Graphic Conventions

Wherever appropriate, additional information and exercises have been added to this book to help you better understand what is being discussed in the chapter. Icons throughout the text alert you to additional materials. The icons used in this textbook are as follows:



The Note icon is used to present additional helpful material related to the subject being described.



Tips offer extra information on resources and how to solve problems.



Caution icons warn you about potential mistakes or problems and explain how to avoid them.



Each Hands-On Project in this book is preceded by the Activity icon and a description of the exercise that follows.



Case Project icons mark end-of-chapter case projects, which are scenario-based assignments that ask you to apply what you have learned.

Instructor Resources

The Instructor Resources CD includes the following materials (also available online at www.cengage.com):

Electronic Instructor's Manual—The Instructor's Manual that accompanies this book includes additional material to assist in class preparation, including suggestions for classroom activities, discussion topics, and additional activities.

Solutions—The instructor resources include solutions to all end-of-chapter material, including review questions and case projects.

PowerPoint presentations—This book comes with Microsoft PowerPoint slides for each chapter. They're included as a teaching aid for classroom presentation, to make available to students on the network for chapter review, or to be printed for classroom distribution. Instructors, please feel free to add your own slides for additional topics you introduce to the class.

ExamView®—ExamView®, the ultimate tool for objective-based testing needs, is a powerful test generator that enables instructors to create paper-, LAN-, or Web-based tests from test banks designed specifically for their Cengage Course Technology text. Instructors can utilize the ultraefficient QuickTest Wizard to create tests in less than five minutes by taking advantage of Cengage Course Technology's questions banks, or customize their own exams from scratch.

Figure files—All figures and tables in the book are reproduced on the Instructor Resources CD in bitmap format. Similar to the PowerPoint presentations, they're included as a teaching aid for classroom presentation, to make available to students for review, or to be printed for classroom distribution.

- Instructor Resources CD (ISBN 978-1-435-45391-3)

Software and System Requirements

Oracle 11g Release 2 (11.2.0.1.0)

- 2 GB of RAM
- Virtual memory double the amount of RAM
- 5.22 GB of disk space
- 32-bit 550 MHz processor minimum or a 64-bit AMD64, or Intel extended memory
- 256-color video

SQL Server 2008 R2

- 1 GB of RAM
- 3.6 GB disk space
- 1.4 GHz processor or faster
- SuperVGA display
- .NET Framework 3.5 SP1
- SQL Server Native Client
- SQL Server setup support files

MySQL 5.5.13

- 512 MB of RAM
- 200 MB of disk space
- 550 MHz processor
- 256-color video

About the Authors

Alfred Basta, Ph.D., is a Professor of Mathematics, Cryptology, and Information Security. He is a member of the Editorial Board for the *Norwich University Journal of Information Assurance*, and conducts professional speaking engagements on Internet security and networking.

Melissa Zgola, M.A., M.S.I.S., is a professor of Network Technology, Information Security, and Software Architecture. She is a member of A.C.M.'s Special Interest Group for Information Technology Education and the Information System Security Association.

Acknowledgements

Thank you to all of the reviewers of this book who provided insightful comments and constructive feedback and to the Cengage Learning staff for all of the hard work put forth toward making this book possible.

To my friends and family, particularly Erin Lovas and Rae Ann Litzinger, I am enormously grateful for your unwavering compassion and moral support throughout this very long process. Thank you to Angie and Nick Madonna—"Gram and Pap"—for allowing Anthony to keep you up into the wee hours of the night, so that *"mommy can finish her chapter."*

Thank you to my mother Mary, for instilling in me the strength and perseverance to keep writing day after day, and to my late father Joe, whom I am certain was by my side smiling throughout all of the late nights of writing. *Thank you both for the sacrifices that you made in your lives, just so that I could find success in mine.*

Special love goes to my fiancé Tony, for his never-ending words of encouragement and whose constant, steadfast belief in me is what inspired the confidence that made this book a reality. *Thank you for knowing me better than I know myself, I love you!*

Finally, I would like to dedicate this book to my son, Anthony, my greatest motivation for finishing. *The stars are always within reach my sweetie, so never stop believing in the magic that life has to offer.*

—Melissa Zgola

To my wife Nadine

"It is the continuing symphony of your loving thoughts, caring actions, and continuous support that stands out as the song of my life."

To our daughter Rebecca, our son Stavros

"Fix your hearts upon God, and love Him with all your strength, for without this no one can be saved or be of any worth. Develop in yourselves an urge for a life of high and noble values. You are like little birds that will soon spread your wings and fly."

To my mother

"You are a never-ending melody of goodness and kindness. You are without equal in this world."

And to the memory of my father

"If one is weighed by the gifts one gives, your values given are beyond estimation."

—Alfred Basta

Thanks to my writing team for patiently answering my endless questions and giving me the chance to participate on this project. You are great examples of how instructors should be and now

I know that gift flows out of the classroom as well! I would like to thank the Cengage Learning staff for their support during the process. This was a great learning and growth experience for me! A huge thank-you also goes out to my friends and family who supported me during this project.

—Dana Bullaboy

Reviewers

William Figg, M.S., Ph.D., CHFI
Associate Professor
Dakota State University
Madison, SD

Roger Findley
Information Assurance Instructor
Laramie County Community College
Cheyenne, WY

Huiwei Guan, Ph.D.
Professor
North Shore Community College
Davers, MA

Robert Guess
Associate Professor
Tidewater Community College
Chesapeake, VA

Angela Herring
Instructor
Wilson Community College
Wilson, NC

David Hoehn
Assistant Professor
Brown College
Mendota Heights, MN

Britt John
New Horizons Computer Learning Center
Hiawatha, IA

B. Dawn Medlin, Ph.D.
Chair and Associate Professor
Appalachian State University
Boone, NC

Keith A. Morneau, Ed.D.
Faculty Chair
Capella University
Minneapolis, MN

David C. Pope
Instructor
Ozarks Technical Community College
Springfield, MI

Robert Sherman
Associate Professor
Sinclair Community College
Dayton, OH

Shambhu Upadhyaya, Ph.D.
Professor
University at Buffalo, The State University of New York
Buffalo, New York

Dora Zeimens
Instructor
Mid-Plains Community College
North Platte, NE