CONTENTS

Acknowledgments . . . . . *xiii*
Hacknotes: The Series . . . . . *xv*
Introduction . . . . . *xix*

Reference Center

Application Assessment Methodology Checklist . . RC 2
HTTP Protocol Notes . . . . . RC 10
Input Validation Tests . . . . . RC 13
Common Web-Related Ports and Applications . . . . RC 16
Quick-Reference Command Techniques . . . . . RC 18
Application Default Accounts and Configuration Files . . . . . RC 21
"Wargling" Search Terms . . . . . RC 22
IIS Metabase Settings and Recommendations . . . . . RC 23
Online References . . . . . RC 28
Useful Tools . . . . . RC 30

Part I

Hacking Techniques & Defenses

■ **1** Web Hacking & Penetration Methodologies 3

Threats and Vulnerabilities 4
Profiling the Platform 5
Profiling the Application 9
Summary 21

■ **2** Critical Hacks & Defenses 23

Generic Input Validation 25
Common Vectors 27
Source Disclosure 28

Character Encoding 29
URL Encoding (Escaped Characters) 29
Unicode 30
Alternate Request Methods 32
SQL Injection 33
Microsoft SQL Server 39
Oracle 42
MySQL 44
PostgreSQL 46
Putting It Together 47
Cross-Site Scripting 48
Token Analysis 50
Finding Tokens 50
Encoded vs. Encrypted 51
Pattern Analysis 55
Session Attacks 55
Session Correlation 61
XML-Based Services 63
Attacking XML 64
Fundamental Application Defenses 65
Input Validation 65
Summary 72

Part II

Host Assessment & Hardening

■ **3** Platform Assessment Methodology 75

Vulnerability Scanners 76
Whisker and LibWhisker 76
Nikto 78
Nessus 81
Assessment Tools 86
Achilles 86
WebProxy 2.1 87
Curl 91
Replaying Requests 94
Summary 98

■ **4** Assessment & Hardening Checklists 99

An Overview of Web Servers 100
Log File Checklist 101

Apache 101
Compile-Time Options 101
Configuration File: httpd.conf 106
IIS 110
Adsutil.vbs and the Metabase 110
Accounts 112
File Security 112
Logging 116
IIS Lockdown Utility (iislockd.exe) 116
Summary 117

Part III

Special Topics

■ **5** Web Server Security & Analysis 121
Web Server Log Analysis 122
Proxies 129
Load Balancers 130
The Scope of an Attack 132
Read or Write Access to the File System 132
Arbitrary Command Execution 132
Summary 137

■ **6** Secure Coding 139
Secure Programming 140
Language-Specific Items 144
Java 144
ASP 146
Perl 147
PHP 148
Summary 149

■ **A** 7-Bit ASCII Reference 151

■ **B** Web Application Scapegoat 159
Installing WebGoat 160
Using WebGoat 161

■ Index. 165