

CONTENTS

<i>ACKNOWLEDGMENTS</i>	<i>xi</i>
<i>INTRODUCTION</i>	<i>xxi</i>
CHAPTER 1: WHY WEB SECURITY MATTERS	1
<hr/>	
Anatomy of an Attack	2
Risks and Rewards	5
Building Security from the Ground Up	6
Defense in Depth	8
Never Trust Input	8
Fail Gracefully	8
Watch for Attacks	8
Use Least Privilege	8
Firewalls and Cryptography Are Not a Panacea	9
Security Should Be Your Default State	9
Code Defensively	10
The OWASP Top Ten	10
Moving Forward	12
Checklists	12
<hr/>	
PART I: THE ASP.NET SECURITY BASICS	
<hr/>	
CHAPTER 2: HOW THE WEB WORKS	15
<hr/>	
Examining HTTP	15
Requesting a Resource	16
Responding to a Request	18
Sniffing HTTP Requests and Responses	19
Understanding HTML Forms	22
Examining How ASP.NET Works	30
Understanding How ASP.NET Events Work	30
Examining the ASP.NET Pipeline	34
Writing HTTP Modules	34
Summary	37

CHAPTER 3: SAFELY ACCEPTING USER INPUT	39
Defining Input	39
Dealing with Input Safely	41
Echoing User Input Safely	41
Mitigating Against XSS	45
The Microsoft Anti-XSS Library	47
The Security Run-time Engine	48
Constraining Input	50
Protecting Cookies	52
Validating Form Input	53
Validation Controls	55
Standard ASP.NET Validation Controls	57
Using the RequiredFieldValidator	58
Using the RangeValidator	58
Using the RegularExpressionValidator	59
Using the CompareValidator	59
Using the CustomValidator	60
Validation Groups	61
A Checklist for Handling Input	63
CHAPTER 4: USING QUERY STRINGS, FORM FIELDS, EVENTS, AND BROWSER INFORMATION	65
Using the Right Input Type	65
Query Strings	66
Form Fields	68
Request Forgery and How to Avoid It	69
Mitigating Against CSRF	71
Protecting ASP.NET Events	81
Avoiding Mistakes with Browser Information	83
A Checklist for Query Strings, Forms, Events, and Browser Information	85
CHAPTER 5: CONTROLLING INFORMATION	87
Controlling ViewState	87
Validating ViewState	89
Encrypting ViewState	91
Protecting Against ViewState One-Click Attacks	92
Removing ViewState from the Client Page	94
Disabling Browser Caching	94

Error Handling and Logging	95
Improving Your Error Handling	97
Watching for Special Exceptions	98
Logging Errors and Monitoring Your Application	99
Using the Windows Event Log	99
Using Email to Log Events	100
Using ASP.NET Tracing	102
Using Performance Counters	104
Using WMI Events	107
Another Alternative: Logging Frameworks	108
Limiting Search Engines	112
Controlling Robots with a Metatag	113
Controlling Robots with robots.txt	113
Protecting Passwords in Config Files	114
A Checklist for Query Strings, Forms, Events, and Browser Information	116
CHAPTER 6: KEEPING SECRETS SECRET — HASHING AND ENCRYPTION	117
Protecting Integrity with Hashing	118
Choosing a Hashing Algorithm	119
Protecting Passwords with Hashing	120
Salting Passwords	121
Generating Secure Random Numbers	121
Encrypting Data	124
Understanding Symmetric Encryption	124
Protecting Data with Symmetric Encryption	125
Sharing Secrets with Asymmetric Encryption	133
Using Asymmetric Encryption without Certificates	134
Using Certificates for Asymmetric Encryption	136
Getting a Certificate	136
Using the Windows DPAPI	147
A Checklist for Encryption	148
PART II: SECURING COMMON ASP.NET TASKS	
CHAPTER 7: ADDING USERNAMES AND PASSWORDS	151
Authentication and Authorization	152
Discovering Your Own Identity	152
Adding Authentication in ASP.NET	154

Using Forms Authentication	154
Configuring Forms Authentication	154
Using SQL as a Membership Store	158
Creating Users	160
Examining How Users Are Stored	163
Configuring the Membership Settings	164
Creating Users Programmatically	166
Supporting Password Changes and Resets	167
Windows Authentication	167
Configuring IIS for Windows Authentication	168
Impersonation with Windows Authentication	171
Authorization in ASP.NET	172
Examining <allow> and <deny>	173
Role-Based Authorization	174
Configuring Roles with Forms-Based Authentication	174
Using the Configuration Tools to Manage Roles	176
Managing Roles Programmatically	177
Managing Role Members Programmatically	179
Roles with Windows Authentication	179
Limiting Access to Files and Folders	180
Checking Users and Roles Programmatically	183
Securing Object References	183
A Checklist for Authentication and Authorization	184
CHAPTER 8: SECURELY ACCESSING DATABASES	185
Writing Bad Code: Demonstrating SQL Injection	186
Fixing the Vulnerability	190
More Security for SQL Server	194
Connecting Without Passwords	194
SQL Permissions	196
Adding a User to a Database	197
Managing SQL Permissions	197
Groups and Roles	197
Least Privilege Accounts	198
Using Views	198
SQL Express User Instances	200
Drawbacks of the VS Built-in Web Server	200
Dynamic SQL Stored Procedures	200
Using SQL Encryption	201
Encrypting by Pass Phrase	202
SQL Symmetric Encryption	202

SQL Asymmetric Encryption	204
Calculating Hashes and HMACs in SQL	205
A Checklist for Securely Accessing Databases	205
CHAPTER 9: USING THE FILE SYSTEM	207
Accessing Existing Files Safely	207
Making Static Files Secure	213
Checking That Your Application Can Access Files	215
Making a File Downloadable and Setting Its Name	216
Adding Further Checks to File Access	216
Adding Role Checks	216
Anti-Leeching Checks	217
Accessing Files on a Remote System	218
Creating Files Safely	218
Handling User Uploads	220
Using the File Upload Control	221
A Checklist for Securely Accessing Files	224
CHAPTER 10: SECURING XML	225
Validating XML	225
Well-Formed XML	226
Valid XML	226
XML Parsers	227
Querying XML	234
Avoiding XPath Injection	236
Securing XML Documents	237
Encrypting XML Documents	238
Using a Symmetric Encryption Key with XML	238
Using an Asymmetric Key Pair to Encrypt and Decrypt XML	242
Using an X509 Certificate to Encrypt and Decrypt XML	245
Signing XML Documents	246
A Checklist for XML	252
PART III: ADVANCED ASP.NET SCENARIOS	
CHAPTER 11: SHARING DATA WITH WINDOWS COMMUNICATION FOUNDATION	255
Creating and Consuming WCF Services	256
Security and Privacy with WCF	259
Transport Security	259

Message Security	260
Mixed Mode	261
Selecting the Security Mode	261
Choosing the Client Credentials	262
Adding Security to an Internet Service	263
Signing Messages with WCF	274
Logging and Auditing in WCF	277
Validating Parameters Using Inspectors	280
Using Message Inspectors	283
Throwing Errors in WCF	286
A Checklist for Securing WCF	287

CHAPTER 12: SECURING RICH INTERNET APPLICATIONS **289**

RIA Architecture	290
Security in Ajax Applications	290
The XMLHttpRequest Object	291
The Ajax Same Origin Policy	292
The Microsoft ASP.NET Ajax Framework	293
Examining the UpdatePanel	293
Examining the ScriptManager	296
Security Considerations with UpdatePanel and ScriptManager	299
Security in Silverlight Applications	301
Understanding the CoreCLR Security Model	301
Using the HTML Bridge	302
Controlling Access to the HTML DOM	303
Exposing Silverlight Classes and Members to the DOM	304
Accessing the Local File System	306
Using Cryptography in Silverlight	309
Accessing the Web and Web Services with Silverlight	312
Using ASP.NET Authentication and Authorization in Ajax and Silverlight	313
A Checklist for Securing Ajax and Silverlight	314

CHAPTER 13: UNDERSTANDING CODE ACCESS SECURITY **315**

Understanding Code Access Security	316
Using ASP.NET Trust Levels	318
Demanding Minimum CAS Permissions	319
Asking and Checking for CAS Permissions	320
Testing Your Application Under a New Trust Level	321
Using the Global Assembly Cache to Run Code Under Full Trust	324

.NET 4 Changes for Trust and ASP.NET	327
A Checklist for Code not Under Full Trust	328
CHAPTER 14: SECURING INTERNET INFORMATION SERVER (IIS)	329
Installing and Configuring IIS7	330
IIS Role Services	331
Removing Global Features for an Individual Web Site	335
Creating and Configuring Application Pools	335
Configuring Trust Levels in IIS	337
Locking Trust Levels	338
Creating Custom Trust Levels	339
Filtering Requests	340
Filtering Double-Encoded Requests	341
Filtering Requests with Non-ASCII Characters	341
Filtering Requests Based on File Extension	341
Filtering Requests Based on Request Size	342
Filtering Requests Based on HTTP Verbs	342
Filtering Requests Based on URL Sequences	343
Filtering Requests Based on Request Segments	343
Filtering Requests Based on a Request Header	343
Status Codes Returned to Denied Requests	344
Using Log Parser to Mine IIS Log Files	344
Using Certificates	351
Requesting an SSL Certificate	352
Configuring a Site to Use HTTPS	354
Setting up a Test Certification Authority	354
A Checklist for Securing Internet Information Server (IIS)	357
CHAPTER 15: THIRD-PARTY AUTHENTICATION	359
A Brief History of Federated Identity	359
Using the Windows Identity Foundation to accept SAML and Information Cards	362
Creating a “Claims-Aware” Web Site	363
Accepting Information Cards	365
Working with a Claims Identity	373
Using OpenID with Your Web Site	374
Using Windows Live ID with Your Web Site	379
A Strategy for Integrating Third-Party Authentication with Forms Authentication	382
Summary	383

CHAPTER 16: SECURE DEVELOPMENT WITH THE ASP.NET MVC FRAMEWORK	385
MVC Input and Output	386
Protecting Yourself Against XSS	386
Protecting an MVC Application Against CSRF	387
Securing Model Binding	387
Providing Validation for and Error Messages from Your Model	389
Authentication and Authorization with ASP.NET MVC	392
Authorizing Actions and Controllers	392
Protecting Public Controller Methods	393
Discovering the Current User	393
Customizing Authorization with an Authorization Filter	394
Error Handling with ASP.NET MVC	395
A Checklist for Secure Development with the ASP.NET MVC Framework	398
INDEX	399