

Contents

Acknowledgments	ix
Introduction	xix
Who Is This Book For?	xix
What Does This Book Cover?	xix
What You Need to Run the Examples	xxi
Conventions	xxii
Customer Support	xxiii
How to Download the Sample Code for the Book	xxiii
Errata	xxiii
Email Support	xxiii
p2p.wrox.com	xxiv
Chapter 1: Initial Phases of a Web Request	1
<hr/>	
IIS Request Handling	2
Http.sys	3
aspnet_filter.dll	5
Processing Headers	6
Blocking Restricted Directories	8
Dynamic versus Static Content	9
MIME Type Mappings	9
ISAPI Extension Mappings	10
Wildcard Application Mappings	13
aspnet_isapi.dll	14
Starting Up an Application Domain	15
First Request Initialization	23
Summary	28
Chapter 2: Security Processing for Each Request	31
<hr/>	
IIS Per-Request Security	32
ASP.NET Per-Request Security	33
Where Is the Security Identity for a Request?	34
Establishing the Operating System Thread Identity	38
The ASPNET Processing Pipeline	41
Thread Identity and Asynchronous Pipeline Events	43
AuthenticateRequest	48

Contents

DefaultAuthentication and Thread.CurrentPrincipal	54
PostAuthenticateRequest	57
AuthorizeRequest	58
PostAuthorizeRequest through PreRequestHandlerExecute	65
Blocking Requests during Handler Execution	66
Identity during Asynchronous Page Execution	69
EndRequest	74
Summary	75
Chapter 3: A Matter of Trust	77
What Is an ASP.NET Trust Level?	78
Configuring Trust Levels	80
Anatomy of a Trust Level	83
A Second Look at a Trust Level in Action	91
Creating a Custom Trust Level	96
Additional Trust Level Customizations	99
The Default Security Permissions Defined by ASP.NET	105
Advanced Topics on Partial Trust	118
Summary	141
Chapter 4: Configuration System Security	143
Using the <location /> Element	143
The Path Attribute	145
The AllowOverride Attribute	146
Using the lock Attributes	146
Locking Attributes	147
Locking Elements	149
Locking Provider Definitions	151
Reading and Writing Configuration	153
Permissions Required for Reading Local Configuration	155
Permissions Required for Writing Local Configuration	157
Permissions Required for Remote Editing	159
Using Configuration in Partial Trust	161
The requirePermission Attribute	163
Demanding Permissions from a Configuration Class	165
FileIOPermission and the Design-Time API	166
Protected Configuration	166
What Can't You Protect?	168
Selecting a Protected Configuration Provider	169
Defining Protected Configuration Providers	172
DpapiProtectedConfigurationProvider	172

RsaProtectedConfigurationProvider	175
Aspnet_regiis Options	181
Using Protected Configuration Providers in Partial Trust	182
Redirecting Configuration with a Custom Provider	184
Summary	190
Chapter 5: Forms Authentication	191
Quick Recap on Forms Authentication	192
Understanding Persistent Tickets	192
How Forms Authentication Enforces Expiration	194
Securing the Ticket on the Wire	198
How Secure Are Signed Tickets?	198
New Encryption Options in ASP.NET 2.0	201
Setting Cookie-Specific Security Options	204
requireSSL	204
HttpOnly Cookies	206
slidingExpiration	208
Using Cookieless Forms Authentication	208
Cookieless Options	210
Replay Attacks with Cookieless Tickets	215
The Cookieless Ticket and Other URLs in Pages	216
Payload Size with Cookieless Tickets	218
Unexpected Redirect Behavior	221
Sharing Tickets between 1.1 and 2.0	222
Leveraging the UserData Property	224
Passing Tickets across Applications	226
Cookie Domain	226
Cross-Application Sharing of Ticket	227
Enforcing Single Logons and Logouts	247
Enforcing a Single Logon	248
Enforcing a Logout	255
Summary	257
Chapter 6: Integrating ASP.NET Security with Classic ASP	259
IIS5 ISAPI Extension Behavior	260
IIS6 Wildcard Mappings	261
Configuring a Wildcard Mapping	261
The Verify That File Exists Setting	268
DefaultHttpHandler	268
Using the DefaultHttpHandler	270
Authenticating Classic ASP with ASP.NET	272

Contents

Will Cookieless Forms Authentication Work?	273
Passing Data to ASP from ASP.NET	274
Passing Username to ASP	276
Authorizing Classic ASP with ASP.NET	276
Passing User Roles to Classic ASP	277
Safely Passing Sensitive Data to Classic ASP	278
Full Code Listing of the Hash Helper	284
Summary	285
Chapter 7: Session State	287
Does Session State Equal Logon Session?	287
Session Data Partitioning	290
Cookie-Based Sessions	291
Cookie Sharing across Applications	292
Protecting Session Cookies	293
Session ID Reuse	294
Cookieless Sessions	294
Session ID Reuse and Expired Sessions	296
Session Denial of Service Attacks	297
Trust Levels and Session State	300
Serialization and Deserialization Requirements	302
Database Security for SQL Session State	304
Security Options for the OOP State Server	306
Summary	307
Chapter 8: Security for Pages and Compilation	309
Request Validation and Viewstate Protection	309
Request Validation	310
Securing viewstate	311
Page Compilation	314
Fraudulent Postbacks	318
Site Navigation Security	322
Summary	327
Chapter 9: The Provider Model	329
Why Have Providers?	329
Patterns Found in the Provider Model	332
The Strategy Pattern	332
Factory Method	334
The Singleton Pattern	339

Façade	341
Core Provider Classes	342
System.Configuration.Provider Classes	342
System.Web.Configuration Classes	346
System.Configuration Classes	347
Building a Provider-Based Feature	351
Summary	366
Chapter 10: Membership	367
<hr/>	
The Membership Class	368
The MembershipUser Class	371
Extending MembershipUser	373
MembershipUser State after Updates	375
Why Are Only Certain Properties Updatable?	379
DateTime Assumptions	380
The MembershipProvider Base Class	382
Basic Configuration	383
User Creation and User Updates	384
Retrieving Data for a Single User	387
Retrieving and Searching for Multiple Users	387
Validating User Credentials	388
Supporting Self-Service Password Reset or Retrieval	390
Tracking Online Users	392
General Error Handling Approaches	393
The “Primary Key” for Membership	394
Supported Environments	396
Using Custom Hash Algorithms	399
Summary	402
Chapter 11: SqlMembershipProvider	403
<hr/>	
Understanding the Common Database Schema	404
Storing Application Name	404
The Common Users Table	405
Versioning Provider Schemas	408
Querying Common Tables with Views	410
Linking Custom Features to User Records	410
Why Are There Calls to the LOWER Function?	414
The Membership Database Schema	415
SQL Server–Specific Provider Configuration Options	418
Working with SQL Server Express	419

Contents

Sharing Issues with SSE	424
Changing the SSE Connection String	425
Database Security	426
Database Schemas and the DBO User	428
Changing Password Formats	430
Custom Password Generation	432
Implementing Custom Encryption	435
Enforcing Custom Password Strength Rules	437
Hooking the ValidatePassword Event	439
Implementing Password History	440
Account Lockouts	451
Implementing Automatic Unlocking	454
Supporting Dynamic Applications	458
Summary	463
Chapter 12: ActiveDirectoryMembershipProvider	465
Supported Directory Architectures	465
Provider Configuration	468
Directory Connection Settings	468
Directory Schema Mappings	471
Provider Settings for Search	474
Membership Provider Settings	475
Unique Aspects of Provider Functionality	477
ActiveDirectoryMembershipUser	480
IsApproved and IsLockedOut	481
Using the ProviderUserKey Property	482
Working with Active Directory	482
UPNs and SAM Account Names	484
Container Nesting	486
Securing Containers	487
Configuring Self-Service Password Reset	494
Using ADAM	503
Installing ADAM with an Application Partition	504
Using the Application Partition	510
Using the Provider in Partial Trust	512
Summary	515
Chapter 13: Role Manager	517
The Roles Class	517
The RolePrincipal Class	521
The RoleManagerModule	531

PostAuthenticateRequest	531
EndRequest	534
Role Cache Cookie Settings and Behavior	535
Working with Multiple Providers during GetRoles	537
RoleProvider	542
Basic Configuration	544
Authorization Methods	544
Managing Roles and Role Associations	544
WindowsTokenRoleProvider	546
Summary	551
Chapter 14: SqlRoleProvider	553
<hr/>	
SqlRoleProvider Database Schema	553
SQL Server–Specific Provider Configuration Options	555
Transaction Behavior	556
Provider Security	556
Trust-Level Requirements and Configuration	557
Database Security	563
Working with Windows Authentication	563
Running with a Limited Set of Roles	565
Authorizing with Roles in the Data Layer	570
Supporting Dynamic Applications	571
Summary	572
Chapter 15: AuthorizationStoreRoleProvider	573
<hr/>	
Provider Design	573
Supported Functionality	576
Using a File-Based Policy Store	578
Using a Directory-Based Policy Store	580
Working in Partial Trust	589
Using Membership and Role Manager Together	592
Summary	594
Index	595

