

Contents

Introduction	xxiii
Chapter 1: Introducing IIS 7.0	1
Overview of IIS 7.0	2
Modular Architecture	2
Deployment and Configuration Management	4
Improved Administration	6
ASP.NET Integration	9
Security Improvements	11
Troubleshooting Improvements	12
Application Pools	17
Integrated Mode	18
Classic Mode	18
IIS 7.0 Components	19
Protocol Listeners	19
World Wide Web Publishing Service	19
Windows Process Activation Service	20
IIS 7.0 Modules	22
Unmanaged Modules	22
Managed Modules	25
Summary	26
Chapter 2: IIS 7.0 and ASP.NET Integrated Mode	29
Advantages of IIS 7.0 and ASP.NET Integrated Mode	30
IIS 7.0 Integrated Mode Architecture	31
system.webServer Configuration Section Group	34
Migrating ASP.NET Applications to Integrated Mode	42
Extending IIS 7.0 with Managed Handlers and Modules	49
Summary	77
Chapter 3: HTTP Request Processing in IIS 7.0 Integrated Model	79
Built-in IUSR Account and IIS_IUSRS Group	80

Contents

Integrated Mode Per-Request Security	81
Where Is the Security Identity for a Request?	87
Establishing the Operating System Thread Identity	92
The Unified Processing Pipeline	98
Thread Identity and Asynchronous Pipeline Events	100
AuthenticateRequest	110
DefaultAuthentication and Thread.CurrentPrincipal	117
PostAuthenticateRequest	120
AuthorizeRequest	122
PostAuthorizeRequest Through PreRequestHandlerExecute	135
Blocking Requests at the IIS Level	135
Identity during Asynchronous Page Execution	137
EndRequest	143
Summary	144
Chapter 4: A Matter of Trust	147
<hr/>	
What Is an ASP.NET Trust Level?	148
Configuring Trust Levels	150
Anatomy of a Trust Level	155
A Second Look at a Trust Level in Action	162
Creating a Custom Trust Level	167
Additional Trust Level Customizations	171
LINQ in Medium/Partial Trust ASP.NET Applications	179
The Default Security Permissions Defined by ASP.NET	181
Advanced Topics on Partial Trust	195
Summary	221
Chapter 5: Configuration System Security	223
<hr/>	
Using the <location /> Element	223
The Path Attribute	225
The allowOverride Attribute	226
Using the lockAttributes	227
Locking Attributes	227
Locking Elements	229
Locking Provider Definitions	231
Managing IIS 7.0 Configuration versus ASP.NET Configuration	233
Extending IIS 7.0 with Managed Modules and Handlers	236
Managing the Native versus Managed Configuration Systems	236
IIS 7.0 Feature Delegation	238

Reading and Writing Configuration	244
Permissions Required for Reading Local Configuration	247
Permissions Required for Writing Local Configuration	249
Permissions Required for Remote Editing	251
Using Configuration in Partial Trust	253
The requirePermission Attribute	255
Demanding Permissions from a Configuration Class	257
FileIOPermission and the Design-Time API	258
Protected Configuration	259
What Can't You Protect?	260
Selecting a Protected Configuration Provider	261
Defining Protected Configuration Providers	264
DpapiProtectedConfigurationProvider	265
RsaProtectedConfigurationProvider	267
aspnet_regiis Options	273
Using Protected Configuration Providers in Partial Trust	274
Redirecting Configuration with a Custom Provider	278
Summary	285
Chapter 6: Forms Authentication	287
A Quick Recap of Forms Authentication	288
Understanding Persistent Tickets	288
How Forms Authentication Enforces Expiration	291
Securing the Ticket on the Wire	295
How Secure Are Signed Tickets?	295
Encryption Options in ASP.NET 2.0 and 3.5	299
Setting Cookie-Specific Security Options	303
requireSSL	303
HttpOnly Cookies	306
slidingExpiration	308
Using Cookieless Forms Authentication	308
Cookieless Options	310
Replay Attacks with Cookieless Tickets	315
The Cookieless Ticket and Other URLs in Pages	317
Payload Size with Cookieless Tickets	319
Unexpected Redirect Behavior	322
Configuring Forms Authentication Inside IIS 7.0	323
Sharing Tickets between 1.1 and 2.0/3.5	324
Using Forms Authentication Across Different Content Types	326
Leveraging the UserData Property	329

Contents

Passing Tickets Across Applications	332
Cookie Domain	332
Cross-Application Sharing of Ticket	333
Enforcing Single Logons and Logouts	358
Enforcing a Single Logon	359
Enforcing a Logout	368
Summary	372
Chapter 7: Integrating ASP.NET Security with Classic ASP	373
IIS 5 ISAPI Extension Behavior	374
IIS 7.0 Wildcard Mappings	375
Configuring a Wildcard Mapping	376
The Resource Type Setting	382
DefaultHttpHandler	383
Using the DefaultHttpHandler	384
Serving Classic ASP in IIS 7.0 Integration Mode	387
Authenticating Classic ASP with ASP.NET	389
Will Cookieless Forms Authentication Work?	391
Passing Data to ASP from ASP.NET	392
Passing Username to ASP	394
Authenticating Classic ASP with IIS 7.0 Integrated Mode	394
Authorizing Classic ASP with ASP.NET	396
Passing User Roles to Classic ASP	397
Safely Passing Sensitive Data to Classic ASP	398
Full Code Listing of the Hash Helper	407
Authorizing Classic ASP with IIS 7.0 Integrated Mode	410
Passing Data from ASP.NET to Classic ASP in IIS 7.0 Integrated Mode	411
Summary	414
Chapter 8: Session State	417
Does Session State Equal Logon Session?	417
Session Data Partitioning	420
Cookie-Based Sessions	421
Sharing Cookies Across Applications	422
Protecting Session Cookies	423
Session ID Reuse	424
Cookieless Sessions	424
Configuring Session State Inside IIS 7.0	426
Session State for Applications Running in IIS 7.0 Integrated Mode	427
Session ID Reuse and Expired Sessions	435
Session ID Denial-of-Service Attacks	437

Trust Levels and Session State	439
Serialization and Deserialization Requirements	441
Database Security for SQL Session State	445
Security Options for the OOP State Server	447
Summary	447
<hr/> Chapter 9: Security for Pages and Compilation	<hr/> 449
Request Validation and Viewstate Protection	449
Request Validation	450
Securing viewstate	451
Page Compilation	454
Fraudulent Postbacks	458
Site Navigation Security	462
Summary	468
<hr/> Chapter 10: The Provider Model	<hr/> 469
Why Have Providers?	469
Patterns Found in the Provider Model	472
The Strategy Pattern	472
Factory Method	474
The Singleton Pattern	481
Façade	482
Core Provider Classes	484
System.Configuration.Provider Classes	484
System.Web.Configuration Classes	489
System.Configuration Classes	490
Building a Provider-Based Feature	495
Summary	518
<hr/> Chapter 11: Membership	<hr/> 519
The Membership Class	520
The MembershipUser Class	523
Extending MembershipUser	526
MembershipUser State After Updates	529
Why Are Only Certain Properties Updatable?	534
DateTime Assumptions	536
The MembershipProvider Base Class	537
Basic Configuration	541
User Creation and User Updates	541
Retrieving Data for a Single User	544

Contents

Retrieving and Searching for Multiple Users	545
Validating User Credentials	545
Supporting Self-Service Password Reset or Retrieval	547
Tracking Online Users	549
General Error-Handling Approaches	550
The “Primary Key” for Membership	552
Supported Environments	554
Using Custom Hash Algorithms	557
Summary	560
Chapter 12: SqlMembershipProvider	561
Understanding the Common Database Schema	562
Storing Application Name	562
The Common Users Table	563
Versioning Provider Schemas	566
Querying Common Tables with Views	568
Linking Custom Features to User Records	569
Why Are There Calls to the LOWER Function?	572
The Membership Database Schema	573
SQL Server-Specific Provider Configuration Options	576
Working with SQL Server Express	577
Sharing Issues with SSE	582
Changing the SSE Connection String	583
Database Security	584
Database Schemas and the DBO User	586
Changing Password Formats	588
Custom Password Generation	590
Implementing Custom Encryption	594
Enforcing Custom Password Strength Rules	598
Hooking the ValidatePassword Event	600
Implementing Password History	602
Account Lockouts	618
Implementing Automatic Unlocking	621
Supporting Dynamic Applications	626
Managing an Application’s Users Through IIS 7.0	632
Summary	637
Chapter 13: ActiveDirectoryMembershipProvider	639
Supported Directory Architectures	640

Provider Configuration	642
Directory Connection Settings	642
Directory Schema Mappings	645
Provider Settings for Search	648
MembershipProvider Settings	649
Unique Aspects of Provider Functionality	651
ActiveDirectoryMembershipUser	654
IsApproved and IsLockedOut	655
Using the ProviderUserKey Property	655
Working with Active Directory	657
UPNs and SAM Account Names	659
Container Nesting	660
Securing Containers	662
Configuring Self-Service Password Reset	667
Using ADLDS	675
Installing ADLDS with an Application Partition	677
Using the Application Partition	682
Using the Provider in Partial Trust	685
Summary	690
Chapter 14: Role Manager	691
The Roles Class	692
The RolePrincipal Class	695
The RoleManagerModule	707
PostAuthenticateRequest	707
EndRequest	711
Role Cache Cookie Settings and Behavior	712
Working with Multiple Providers during GetRoles	714
RoleProvider	722
Basic Configuration	724
Authorization Methods	724
Managing Roles and Role Associations	725
WindowsTokenRoleProvider	726
Summary	733
Chapter 15: SqlRoleProvider	735
SqlRoleProvider Database Schema	735
SQL Server-Specific Provider Configuration Options	737
Transaction Behavior	738

Contents

Provider Security	739
Trust-Level Requirements and Configuration	739
Database Security	745
Working with Windows Authentication	746
Running with a Limited Set of Roles	748
Authorizing with Roles in the Data Layer	755
Supporting Dynamic Applications	757
Managing an Application's Roles Through IIS 7.0	758
Summary	760
Chapter 16: AuthorizationStoreRoleProvider	763
Provider Design	763
Supported Functionality	766
Using a File-Based Policy Store	768
Using a Directory-Based Policy Store	771
Using a Microsoft SQL Server Database-Based Policy Store	780
Working in Partial Trust	783
Using Membership and Role Manager Together	786
Summary	789
Chapter 17: Membership and Role Management in ASP.NET AJAX 3.5	791
ASP.NET Membership and Role Services Overview	792
ASP.NET Membership	792
ASP.NET Role Management	794
ASP.NET AJAX Application Services	796
Enabling ASP.NET Applications with ASP.NET AJAX 3.5	796
Enabling ASP.NET Application Services	801
AuthenticationServiceManager and RoleServiceManager Classes	803
Authentication Service	804
Role Service	816
Summary	822
Chapter 18: Best Practices for Securing ASP.NET Web Applications	823
Web Application Security Threats Overview	824
Developers Beware	827
Know Your Users	827
Run Applications with Minimum Privileges	829
Validate User Input	829
Secure Cookies	838

Secure Database Access	841
SQL Injection Attacks	849
Cross-Site Scripting	853
Cross-Site Request Forgery	857
Handle Exceptions Properly	861
Guard Against Denial-of-Service Threats	866
Secure Data Transmission	872
AJAX-Enabled Application Threats	872
Information Leakage	872
JSON Hijacking	874
Amplified Cross-Site Scripting	876
Summary	878
Index	879

