The Pragmatic Programmers

Covers Rails 2

Agile Web Development with Rails

Third Edition

Sam Ruby
Dave Thomas
David Heinemeier Hansson

with Leon Breedt, Mike Clark, Justin Gehtland, James Duncan Davidson, and Andreas Schwarz

The Facets of Ruby Series

Prepared exclusively for Vanilton

Important Information About Rails Versions

This book is written for Rails 2. As this printing of the book is going to press, the current generally available Gem version of Rails is 2.1. The code in this book has been tested against this version.

This book started life with the same text as the Second Edition, which covered Rails 1.2.6. Pages containing this original text have a gray heading and footer. As we migrate content to Rails 2, you'll find the header color changes to red. The Third Edition preface contains a table summarizing the status of this update process. In particular, note that in many of the chapters the screenshots have not yet been updated to match the results produced by Rails 2.1.

The Rails core team is continuing to work on Rails 2. From time to time, new releases may introduce incompatibilities for applications written for prior versions of Rails. In order to experiment with these changes, the Rails developers are making the changes available via Edge Rails (discussed starting on page 244). These changes won't affect you unless you explicitly install this experimental code—you won't find yourself running it unless you overide Gem defaults or deliberately choose to use Edge Rails. However, if you do decide to run this experimental Rails code, you'll find that some stuff in this book (and some stuff in your existing Rails applications) may no longer run.

To determine the version of Rails that you are running, you can issue `rails -v` at a command prompt.

► **Sam, Dave, and David**

Prepared exclusively for Vanilton

Agile Web Development with Rails

Third Edition

Sam Ruby
Dave Thomas
David Heinemeier Hansson

with Leon Breedt
Mike Clark
James Duncan Davidson
Justin Gehtland
Andreas Schwarz

The Pragmatic Bookshelf
Raleigh, North Carolina Dallas, Texas

Prepared exclusively for Vanilton

Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book, and The Pragmatic Programmers, LLC was aware of a trademark claim, the designations have been printed in initial capital letters or in all capitals. The Pragmatic Starter Kit, The Pragmatic Programmer, Pragmatic Programming, Pragmatic Bookshelf and the linking *g* device are trademarks of The Pragmatic Programmers, LLC.

Every precaution was taken in the preparation of this book. However, the publisher assumes no responsibility for errors or omissions, or for damages that may result from the use of information (including program listings) contained herein.

Our Pragmatic courses, workshops, and other products can help you and your team create better software and have more fun. For more information, as well as the latest Pragmatic titles, please visit us at

http://www.pragprog.com

Copyright © 2008 The Pragmatic Programmers LLC.

All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form, or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior consent of the publisher.

Printed in the United States of America.

ISBN-10: 1-934356-16-6

ISBN-13: 978-1-9343561-6-6

Printed on acid-free paper with 50% recycled, 15% post-consumer content.

B1.3 printing, June 4, 2008

Version: 2008-6-4

Prepared exclusively for Vanilton

Contents

Preface to the Second Edition 12

Preface to the Third Edition 14

1 Introduction 16
- 1.1 Rails Is Agile . . . 18
- 1.2 Finding Your Way Around . . . 19
- 1.3 Acknowledgments . . . 21

Part I—Getting Started 23

2 The Architecture of Rails Applications 24
- 2.1 Models, Views, and Controllers . . . 24
- 2.2 Active Record: Rails Model Support . . . 27
- 2.3 Action Pack: The View and Controller . . . 31

3 Installing Rails 33
- 3.1 Your Shopping List . . . 33
- 3.2 Installing on Windows . . . 33
- 3.3 Installing on Mac OS X . . . 35
- 3.4 Installing on Linux . . . 36
- 3.5 Development Environments . . . 37
- 3.6 Rails and Databases . . . 41
- 3.7 Keeping Up-to-Date . . . 42
- 3.8 Rails and ISPs . . . 43

4 Instant Gratification 44
- 4.1 Creating a New Application . . . 44
- 4.2 Hello, Rails! . . . 46
- 4.3 Linking Pages Together . . . 57
- 4.4 What We Just Did . . . 60

Prepared exclusively for Vanilton

Part II—Building an Application **62**

5 The Depot Application **63**
5.1 Incremental Development 63
5.2 What Depot Does 64
5.3 Let's Code 68

6 Task A: Product Maintenance **69**
6.1 Iteration A1: Get Something Running 69
6.2 Create the Products Model and Maintenance Application . . . 74
6.3 Iteration A2: Add a Missing Column 79
6.4 Iteration A3: Validate! 84
6.5 Iteration A4: Prettier Listings 88

7 Task B: Catalog Display **95**
7.1 Iteration B1: Create the Catalog Listing 95
7.2 Iteration B2: Add a Page Layout 99
7.3 Iteration B3: Use a Helper to Format the Price 101
7.4 Iteration B4: Linking to the Cart 101

8 Task C: Cart Creation **105**
8.1 Sessions 105
8.2 Iteration C1: Creating a Cart 109
8.3 Iteration C2: A Smarter Cart 112
8.4 Iteration C3: Handling Errors 115
8.5 Iteration C4: Finishing the Cart 120

9 Task D: Add a Dash of AJAX **124**
9.1 Iteration D1: Moving the Cart 125
9.2 Iteration D2: An AJAX-Based Cart 130
9.3 Iteration D3: Highlighting Changes 133
9.4 Iteration D4: Hide an Empty Cart 135
9.5 Iteration D5: Degrading If Javascript Is Disabled 139
9.6 What We Just Did 140

10 Task E: Check Out! **142**
10.1 Iteration E1: Capturing an Order 142

11 Task F: Administration **158**
11.1 Iteration F1: Adding Users 158
11.2 Iteration F2: Logging In 168
11.3 Iteration F3: Limiting Access 171
11.4 Iteration F4: A Sidebar, More Administration 174

Prepared exclusively for Vanilton

12 Task G: One Last Wafer-Thin Change **181**
12.1 Generating the XML Feed 181
12.2 Finishing Up 188

13 Task T: Testing **192**
13.1 Tests Baked Right In 192
13.2 Unit Testing of Models 193
13.3 Functional Testing of Controllers 205
13.4 Integration Testing of Applications 221
13.5 Performance Testing 229
13.6 Using Mock Objects 233

Part III—The Rails Framework **236**

14 Rails in Depth **237**
14.1 So, Where's Rails? 237
14.2 Directory Structure 237
14.3 Rails Configuration 244
14.4 Naming Conventions 248
14.5 Logging in Rails 252
14.6 Debugging Hints 252
14.7 What's Next 254

15 Active Support **256**
15.1 Generally Available Extensions 256
15.2 Enumerations and Arrays 257
15.3 String Extensions 258
15.4 Extensions to Numbers 260
15.5 Time and Date Extensions 261
15.6 An Extension to Ruby Symbols 263
15.7 with_options 264
15.8 Unicode Support 265

16 Migrations **270**
16.1 Creating and Running Migrations 272
16.2 Anatomy of a Migration 273
16.3 Managing Tables 277
16.4 Data Migrations 282
16.5 Advanced Migrations 285
16.6 When Migrations Go Bad 289
16.7 Schema Manipulation Outside Migrations 289
16.8 Managing Migrations 290

Prepared exclusively for Vanilton

17 Active Record: The Basics **292**
17.1 Tables and Classes . . . 293
17.2 Columns and Attributes . . . 293
17.3 Primary Keys and IDs . . . 297
17.4 Connecting to the Database . . . 299
17.5 CRUD—Create, Read, Update, Delete . . . 304
17.6 Aggregation and Structured Data . . . 322
17.7 Miscellany . . . 329

18 Active Record: Relationships between Tables **332**
18.1 Creating Foreign Keys . . . 333
18.2 Specifying Relationships in Models . . . 335
18.3 belongs_to and has_xxx Declarations . . . 337
18.4 Joining to Multiple Tables . . . 352
18.5 Self-referential Joins . . . 363
18.6 *Acts As* . . . 364
18.7 When Things Get Saved . . . 368
18.8 Preloading Child Rows . . . 370
18.9 Counters . . . 371

19 Active Record: Object Life Cycle **373**
19.1 Validation . . . 373
19.2 Callbacks . . . 384
19.3 Advanced Attributes . . . 391
19.4 Transactions . . . 394

20 Action Controller: Routing and URLs **403**
20.1 The Basics . . . 403
20.2 Routing Requests . . . 404
20.3 Resource-Based Routing . . . 420
20.4 Testing Routing . . . 436

21 Action Controller and Rails **439**
21.1 Action Methods . . . 439
21.2 Cookies and Sessions . . . 450
21.3 Flash—Communicating between Actions . . . 460
21.4 Filters and Verification . . . 462
21.5 Caching, Part One . . . 470
21.6 The Problem with GET Requests . . . 477

Prepared exclusively for Vanilton

22 Action View **481**
22.1 Templates . . . 481
22.2 Using Helpers . . . 487
22.3 Helpers for Formatting, Linking, and Pagination . . . 489
22.4 How Forms Work . . . 496
22.5 Forms That Wrap Model Objects . . . 498
22.6 Custom Form Builders . . . 510
22.7 Working with Nonmodel Fields . . . 515
22.8 Uploading Files to Rails Applications . . . 518
22.9 Layouts and Components . . . 522
22.10 Caching, Part Two . . . 530
22.11 Adding New Templating Systems . . . 535

23 The Web, V2.0 **538**
23.1 Prototype . . . 538
23.2 Script.aculo.us . . . 559
23.3 RJS Templates . . . 575
23.4 Conclusion . . . 582

24 Action Mailer **584**
24.1 Sending E-mail . . . 584
24.2 Receiving E-mail . . . 595
24.3 Testing E-mail . . . 596

25 Web Services on Rails **600**
25.1 What AWS Is (and What It Isn't) . . . 600
25.2 The API Definition . . . 601
25.3 Dispatching Modes . . . 606
25.4 Using Alternate Dispatching . . . 607
25.5 Method Invocation Interception . . . 609
25.6 Testing Web Services . . . 611
25.7 Protocol Clients . . . 614

Part IV—Secure and Deploy Your Application **615**

26 Securing Your Rails Application **616**
26.1 SQL Injection . . . 616
26.2 Creating Records Directly from Form Parameters . . . 618
26.3 Don't Trust ID Parameters . . . 620
26.4 Don't Expose Controller Methods . . . 621
26.5 Cross-Site Scripting (CSS/XSS) . . . 622
26.6 Avoid Session Fixation Attacks . . . 624
26.7 File Uploads . . . 625

Prepared exclusively for Vanilton

26.8 Don't Store Sensitive Information in the Clear 626
26.9 Use SSL to Transmit Sensitive Information 627
26.10 Don't Cache Authenticated Pages 628
26.11 Knowing That It Works 628

27 Deployment and Production **630**
27.1 Starting Early 631
27.2 How a Production Server Works 632
27.3 Comparing Front-End Web Servers 634
27.4 Repeatable Deployments with Capistrano 635
27.5 Setting Up a Deployment Environment 636
27.6 Checking Up on a Deployed Application 642
27.7 Production Application Chores 643
27.8 Moving On to Launch and Beyond 645

Part V—Appendices **646**

A Introduction to Ruby **647**
A.1 Ruby Is an Object-Oriented Language 647
A.2 Ruby Names 648
A.3 Methods 649
A.4 Classes 651
A.5 Modules 653
A.6 Arrays and Hashes 654
A.7 Control Structures 655
A.8 Regular Expressions 656
A.9 Blocks and Iterators 656
A.10 Exceptions 657
A.11 Marshaling Objects 658
A.12 Interactive Ruby 658
A.13 Ruby Idioms 658
A.14 RDoc Documentation 660

B Configuration Parameters **661**
B.1 Top-Level Configuration 661
B.2 Active Record Configuration 663
B.3 Action Controller Configuration 665
B.4 Action View Configuration 666
B.5 Action Mailer Configuration 667
B.6 Test Case Configuration 668

Prepared exclusively for Vanilton

C Source Code **669**
C.1 The Full Depot Application 669

D Resources **696**
D.1 Online Resources 696

Index **697**

Prepared exclusively for Vanilton