

Extracted from:

Security on Rails

This PDF file contains pages extracted from Security on Rails, published by the Pragmatic Bookshelf. For more information or to purchase a paperback or PDF copy, please visit <http://www.pragprog.com>.

Note: This extract contains some colored text (particularly in code listing). This is available only in online versions of the books. The printed versions are black and white. Pagination might vary between the online and printer versions; the content is otherwise identical.

Copyright © 2009 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.

The
Pragmatic
Programmers

Security on Rails



*Ben Poweski
David Raphael*

Edited by Colleen Toporek



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 © 2010 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: 1-934356-48-4

ISBN-13: 978-1-934356-48-7

Printed on acid-free paper.

P1.0 printing, December 2009

Version: 2010-1-16

Contents

1	Security in Ruby on Rails	12
1.1	Who's This Book For?	12
1.2	What Does This Book Cover?	13
1.3	Entering a Security Mind-Set	14
1.4	Defense in Depth	15
1.5	Only Secure as the Weakest Link	16
1.6	Fail Close	17
1.7	Whitelisting	18
1.8	Least Privilege	19
1.9	Do Not Repeat Yourself	21
1.10	Avoid Complexity	21
1.11	Acknowledgments	23
I	Getting Started	24
2	Hacking the Example	25
2.1	Getting Started with LunchedIn	25
2.2	The Tools of the Trade	26
2.3	Exploit: Parameter Manipulation	28
2.4	Exploit: Broken Authorization	33
2.5	Exploit: SQL Injection	38
2.6	Exploit: Cross-Site Scripting	42
2.7	Exploit: Cross-Site Request Forgery	47

3	Fixing the Example	51
3.1	Protecting Against Parameter Manipulation	51
3.2	Adding Authorization	54
3.3	Preventing SQL Injection	59
3.4	Cross-Site Scripting Countermeasures	62
3.5	Protecting Against a Cross-Site Request Forgery	66
II	Building on the Basics	69
4	Testing for Security	70
4.1	Things You Should Test	70
4.2	Testing in Layers	72
4.3	Authentication Tests	72
4.4	Authorization Tests	75
4.5	Data Protection Tests	76
4.6	Input Validation and Sanitization Tests	80
4.7	Measuring Test Coverage	83
4.8	Other Testing Frameworks	84
5	Validation	86
5.1	Command Injection	87
5.2	SQL Injection	90
5.3	Mitigating SQL Injection	91
5.4	Built-in SQL Injection Mitigation in Rails	94
6	Authentication: Decentralized Authentication	97
6.1	Authentication Concepts	97
6.2	User Registration	101
6.3	LDAP/Directory-Based Authentication	109
6.4	Flexible Authentication	124
7	Authorization	137
7.1	What Is Authorization?	137
7.2	Mandatory Access Control	138
7.3	Discretionary Access Control	140
7.4	Role-Based Access Control	142
7.5	Implementing RBAC	144
7.6	A Simple Approach to Model Security	153

8	Data Protection Using Cryptography	157
8.1	Message Digests	158
8.2	Encrypting Data	160
8.3	Using Cryptography with ActiveRecord	167
9	Digital Signatures and Email	174
9.1	Digital Signatures	174
9.2	Storing Certificates	180
9.3	Secure Email Exchange	180
9.4	Sending Signed Messages	184
9.5	Verifying Received Messages	189
10	SSO: Centralized Authentication	193
10.1	Public Versus Private	193
10.2	OpenID	195
10.3	Implementing an OpenID Provider	206
10.4	Kerberos, GSSAPI, and SPNEGO	221
10.5	CAS	253
III	Reference	262
11	Web Application Proxies	263
11.1	Web Application Proxies	263
12	Authentication Appendix	265
12.1	OpenLDAP Setup	265
12.2	GSSAPI	269
12.3	SPNEGO	282
13	Bibliography	283
	Index	284

The Pragmatic Bookshelf

The Pragmatic Bookshelf features books written by developers for developers. The titles continue the well-known Pragmatic Programmer style and continue to garner awards and rave reviews. As development gets more and more difficult, the Pragmatic Programmers will be there with more titles and products to help you stay on top of your game.

Visit Us Online

Security on Rails' Home Page

http://pragprog.com/titles/fr_secure

Source code from this book, errata, and other resources. Come give us feedback, too!

Register for Updates

<http://pragprog.com/updates>

Be notified when updates and new books become available.

Join the Community

<http://pragprog.com/community>

Read our weblogs, join our online discussions, participate in our mailing list, interact with our wiki, and benefit from the experience of other Pragmatic Programmers.

New and Noteworthy

<http://pragprog.com/news>

Check out the latest pragmatic developments, new titles and other offerings.

Buy the Book

If you liked this eBook, perhaps you'd like to have a paper copy of the book. It's available for purchase at our store: pragprog.com/titles/fr_secure.

Contact Us

Online Orders:	www.pragprog.com/catalog
Customer Service:	support@pragprog.com
Non-English Versions:	translations@pragprog.com
Pragmatic Teaching:	academic@pragprog.com
Author Proposals:	proposals@pragprog.com
Contact us:	1-800-699-PROG (+1 919 847 3884)