

The Web Application Hacker's Handbook

Discovering and Exploiting
Security Flaws



■ Dafydd Stuttard ■ Marcus Pinto



The Web Application Hacker's Handbook

Discovering and Exploiting Security Flaws

Dafydd Stuttard
Marcus Pinto



Wiley Publishing, Inc.



The Web Application Hacker's Handbook

Discovering and Exploiting Security Flaws

Dafydd Stuttard
Marcus Pinto



Wiley Publishing, Inc.

The Web Application Hacker's Handbook: Discovering and Exploiting Security Flaws

Published by
Wiley Publishing, Inc.
10475 Crosspoint Boulevard
Indianapolis, IN 46256
www.wiley.com

Copyright © 2008 by Dafydd Stuttard and Marcus Pinto.

Published by Wiley Publishing, Inc., Indianapolis, Indiana

Published simultaneously in Canada

ISBN: 978-0-470-17077-9

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

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, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600. Requests to the Publisher for permission should be addressed to the Legal Department, Wiley Publishing, Inc., 10475 Crosspoint Blvd., Indianapolis, IN 46256, (317) 572-3447, fax (317) 572-4355, or online at <http://www.wiley.com/go/permissions>.

Limit of Liability/Disclaimer of Warranty: The publisher and the author make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the author shall be liable for damages arising herefrom. The fact that an organization or Website is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or Website may provide or recommendations it may make. Further, readers should be aware that Internet Websites listed in this work may have changed or disappeared between when this work was written and when it is read.

For general information on our other products and services or to obtain technical support, please contact our Customer Care Department within the U.S. at (800) 762-2974, outside the U.S. at (317) 572-3993 or fax (317) 572-4002.

Library of Congress Cataloging-in-Publication Data

Stuttard, Dafydd, 1972-

The web application hacker's handbook : discovering and exploiting security flaws / Dafydd Stuttard, Marcus Pinto.

p. cm.

Includes index.

ISBN 978-0-470-17077-9 (pbk.)

1. Internet--Security measures. 2. Computer security. I. Pinto, Marcus, 1978- II. Title.

TK5105.875.I57S85 2008

005.8--dc22

2007029983

Trademarks: Wiley and related trade dress are registered trademarks of Wiley Publishing, Inc., in the United States and other countries, and may not be used without written permission. All other trademarks are the property of their respective owners. Wiley Publishing, Inc., is not associated with any product or vendor mentioned in this book.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.



About the Authors

Dafydd Stuttard is a Principal Security Consultant at Next Generation Security Software, where he leads the web application security competency. He has nine years' experience in security consulting and specializes in the penetration testing of web applications and compiled software.

Dafydd has worked with numerous banks, retailers, and other enterprises to help secure their web applications, and has provided security consulting to several software manufacturers and governments to help secure their compiled software. Dafydd is an accomplished programmer in several languages, and his interests include developing tools to facilitate all kinds of software security testing.

Dafydd has developed and presented training courses at the Black Hat security conferences around the world. Under the alias "PortSwigger," Dafydd created the popular Burp Suite of web application hacking tools. Dafydd holds master's and doctorate degrees in philosophy from the University of Oxford.

Marcus Pinto is a Principal Security Consultant at Next Generation Security Software, where he leads the database competency development team, and has lead the development of NGS' primary training courses. He has eight years' experience in security consulting and specializes in penetration testing of web applications and supporting architectures.

Marcus has worked with numerous banks, retailers, and other enterprises to help secure their web applications, and has provided security consulting to the development projects of several security-critical applications. He has worked extensively with large-scale web application deployments in the financial services industry.

Marcus has developed and presented database and web application training courses at the Black Hat and other security conferences around the world. Marcus holds a master's degree in physics from the University of Cambridge.



Credits

Executive Editor

Carol Long

Development Editor

Adaobi Obi Tulton

Production Editor

Christine O'Connor

Copy Editor

Foxxe Editorial Services

Editorial Manager

Mary Beth Wakefield

Production Manager

Tim Tate

**Vice President and Executive Group
Publisher**

Richard Swadley

Vice President and Executive Publisher

Joseph B. Wikert

Project Coordinator, Cover

Lynsey Osborn

Compositor

Happenstance Type-O-Rama

Proofreader

Kathryn Duggan

Indexer

Johnna VanHoose Dinse

Anniversary Logo Design

Richard Pacifico



Contents

Acknowledgments	xxiii
Introduction	xxv
Chapter 1 Web Application (In)security	1
The Evolution of Web Applications	2
Common Web Application Functions	3
Benefits of Web Applications	4
Web Application Security	5
“This Site Is Secure”	6
The Core Security Problem: Users Can Submit Arbitrary Input	8
Key Problem Factors	9
Immature Security Awareness	9
In-House Development	9
Deceptive Simplicity	9
Rapidly Evolving Threat Profile	10
Resource and Time Constraints	10
Overextended Technologies	10
The New Security Perimeter	10
The Future of Web Application Security	12
Chapter Summary	13
Chapter 2 Core Defense Mechanisms	15
Handling User Access	16
Authentication	16
Session Management	17
Access Control	18
Handling User Input	19
Varieties of Input	20
Approaches to Input Handling	21

"Reject Known Bad"	21
"Accept Known Good"	21
Sanitization	22
Safe Data Handling	22
Semantic Checks	23
Boundary Validation	23
Multistep Validation and Canonicalization	26
Handling Attackers	27
Handling Errors	27
Maintaining Audit Logs	29
Alerting Administrators	30
Reacting to Attacks	31
Managing the Application	32
Chapter Summary	33
Questions	34
Chapter 3 Web Application Technologies	35
The HTTP Protocol	35
HTTP Requests	36
HTTP Responses	37
HTTP Methods	38
URLs	40
HTTP Headers	41
General Headers	41
Request Headers	41
Response Headers	42
Cookies	43
Status Codes	44
HTTPS	45
HTTP Proxies	46
HTTP Authentication	47
Web Functionality	47
Server-Side Functionality	48
The Java Platform	49
ASP.NET	50
PHP	50
Client-Side Functionality	51
HTML	51
Hyperlinks	51
Forms	52
JavaScript	54
Thick Client Components	54
State and Sessions	55
Encoding Schemes	56
URL Encoding	56
Unicode Encoding	57

HTML Encoding	57
Base64 Encoding	58
Hex Encoding	59
Next Steps	59
Questions	59
Chapter 4 Mapping the Application	61
Enumerating Content and Functionality	62
Web Spidering	62
User-Directed Spidering	65
Discovering Hidden Content	67
Brute-Force Techniques	67
Inference from Published Content	70
Use of Public Information	72
Leveraging the Web Server	75
Application Pages vs. Functional Paths	76
Discovering Hidden Parameters	79
Analyzing the Application	79
Identifying Entry Points for User Input	80
Identifying Server-Side Technologies	82
Banner Grabbing	82
HTTP Fingerprinting	82
File Extensions	84
Directory Names	86
Session Tokens	86
Third-Party Code Components	87
Identifying Server-Side Functionality	88
Dissecting Requests	88
Extrapolating Application Behavior	90
Mapping the Attack Surface	91
Chapter Summary	92
Questions	93
Chapter 5 Bypassing Client-Side Controls	95
Transmitting Data via the Client	95
Hidden Form Fields	96
HTTP Cookies	99
URL Parameters	99
The Referer Header	100
Opaque Data	101
The ASP.NET ViewState	102
Capturing User Data: HTML Forms	106
Length Limits	106
Script-Based Validation	108
Disabled Elements	110
Capturing User Data: Thick-Client Components	111
Java Applets	112