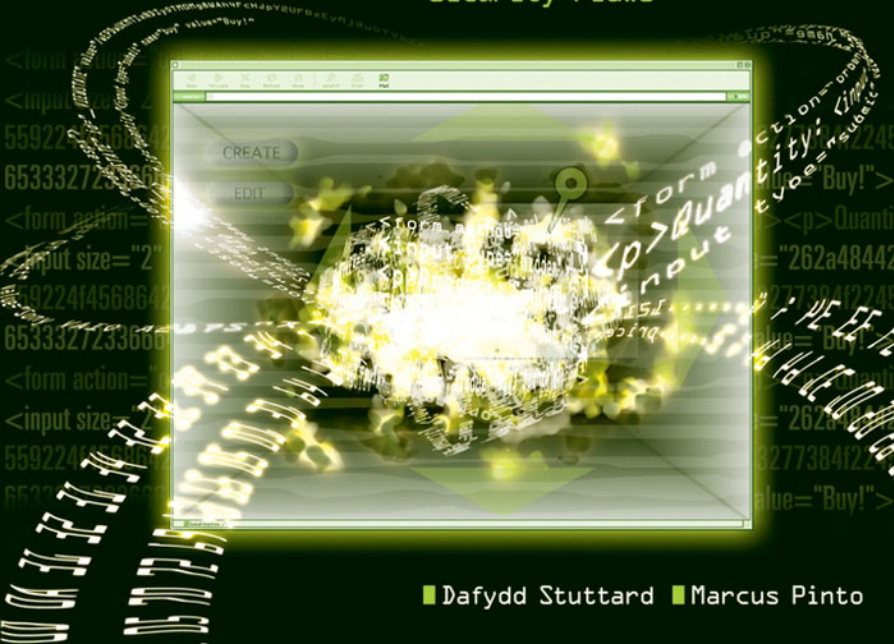
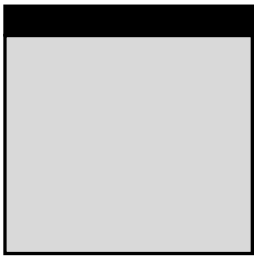
The Web Application Hacker's Handbook

Discovering and Exploiting Security Flaws



Dafydd Stuttard
Marcus Pinto

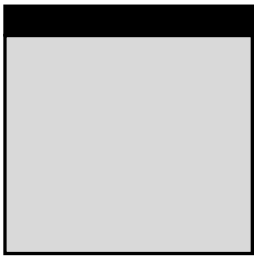


The Web Application Hacker's Handbook

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

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

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

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