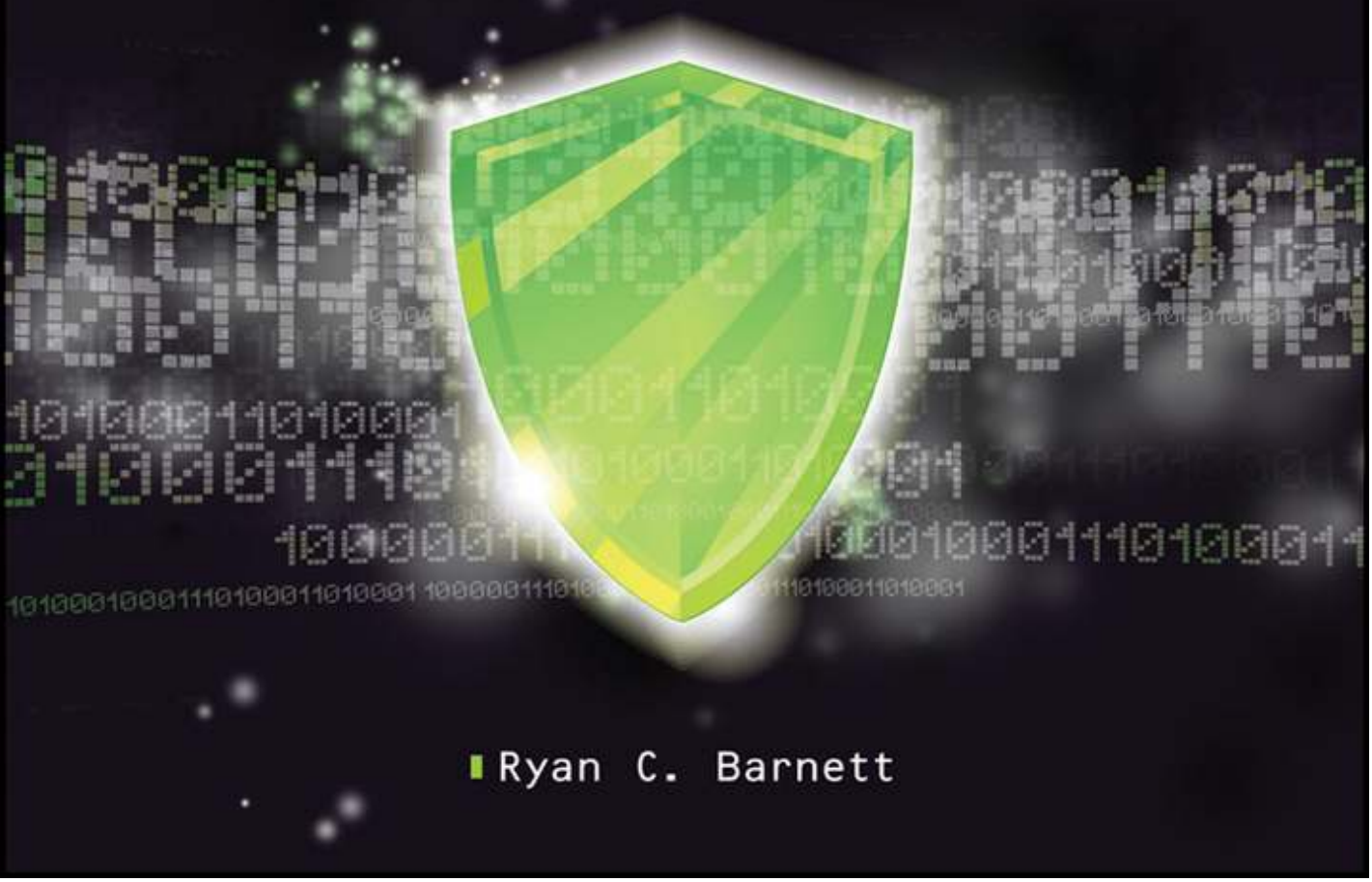
Web Application Defender's Cookbook

Battling Hackers and Protecting Users



Ryan C. Barnett

The Web Application Defender's Cookbook

The Web Application Defender's Cookbook

Battling Hackers and Protecting Users

Ryan Barnett

Wiley Publishing, Inc.

The Web Application Defender's Cookbook: Battling Hackers and Protecting Users

Published by
John Wiley & Sons, Inc.
10475 Crosspoint Boulevard
Indianapolis, IN 46256
www.wiley.com

Published simultaneously in Canada

ISBN: 978-1-118-36218-1
ISBN: 978-1-118-56871-2 (ebk)
ISBN: 978-1-118-41705-8 (ebk)
ISBN: 978-1-118-56865-1 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Library of Congress Control Number: 2012949513

This book is dedicated to my incredible daughter, Isabella. You are so full of imagination, kindness, and humor that I have a constant smile on my face. You are my Supergirl-flying, tae-kwon-do-kicking, fairy princess! I thank God every day for bringing you into my life and for allowing me the joy and privilege of being your father.

I love you Izzy, and I am so proud of you.

Credits

Executive Editor
Carol Long

Project Editor
Ed Connor

Technical Editor
Michael Gregg

Production Editor
Daniel Scribner

Copy Editor
Gayle Johnson

Editorial Manager
Mary Beth Wakefield

Freelancer Editorial Manager
Rosemarie Graham

Associate Director of Marketing
David Mayhew

Marketing Manager
Ashley Zurcher

Business Manager
Amy Knies

Production Manager
Tim Tate

Vice President and Executive Group Publisher
Richard Swadley

Vice President and Executive Publisher
Neil Edde

Associate Publisher
Jim Minatel

Project Coordinator, Cover
Katie Crocker

Compositor
Craig Johnson,
Happenstance Type-O-Rama

Proofreader
Nicole Hirschman

Indexer
Ron Strauss

Cover Image
© Mak_Art / iStockPhoto

Cover Designer
Ryan Sneed

About the Author

Ryan Barnett is renowned in the web application security industry for his unique expertise. After a decade of experience defending government and commercial web sites, he joined the Trustwave SpiderLabs Research Team. He specializes in application defense research and leads the open source ModSecurity web application firewall project.

In addition to his commercial work at Trustwave, Ryan is also an active contributor to many community-based security projects. He serves as the Open Web Application Security Project (OWASP) ModSecurity Core Rule Set project leader and is a contributor on the OWASP Top Ten and AppSensor projects. He is a Web Application Security Consortium Board Member and leads the Web Hacking Incident Database and the Distributed Web Honeypot projects. At the SANS Institute, he is a certified instructor and contributor on the Top 20 Vulnerabilities and CWE/SANS Top 25 Most Dangerous Programming Errors projects.

Ryan is regularly consulted by news outlets that seek his insights into and analysis of emerging web application attacks, trends, and defensive techniques. He is a frequent speaker and trainer at key industry events including Black Hat, SANS AppSec Summit, and OWASP AppSecUSA.

About the Technical Editor

Michael Gregg is the CEO of Superior Solutions, Inc. (www.thesolutionfirm.com), a Houston-based IT security-consulting firm. His organization performs security assessments and penetration testing for Fortune 1000 firms. He is frequently cited by major and trade print publications as a cyber security expert. He has appeared as an expert commentator for network broadcast outlets and print publications and has spoken at major security conferences such as HackerHalted, Fusion, and CA World.

Acknowledgments

I must begin by thanking my wonderful wife, Linda. When I came to her with the idea of writing another book, she was fully supportive even though she understood the sacrifice it would require. I thank her for her continued patience and for enduring many late nights of "angry typing." She has always encouraged and supported me both professionally and personally. The completion of this book is not my accomplishment alone but our whole family's because it was truly a team effort. I love you Linda and am honored that you are my partner for life.

I would like to thank Nick Percoco, Senior VP of Trustwave SpiderLabs, for his unwavering support of ModSecurity and for appointing me as its manager. I am fortunate to work with intelligent, clever and funny people. Unfortunately I cannot list them all here, however, I must single out Breno Silva Pinto. Breno is the lead developer of ModSecurity and we have worked closely on the project for 2 years. I am constantly impressed with his insights, ingenuity and technical skill for web application security. This book would not have been possible without Breno's contributions to ModSecurity features and capabilities.

I would also like to thank two specific ModSecurity community members who epitomize the "giving back" philosophy of the open source community. Thanks to Christian Bockermann for developing many ModSecurity support tools such as the AuditConsole and to Josh Zlatin for always helping users on the mail-list and for contributions to the OWASP ModSecurity CRS.

Last but not least, I want to specifically thank OWASP members: Tom Brennan, Jim Manico, and Sarah Baso. Your tireless work ethic and commitment to the OWASP mission is undeniable. I would also like to thank Michael Coates for starting the AppSensor project and both Colin Watson and John Melton for expanding its capabilities.

Contents

Foreword

A defender, the person responsible for protecting IT systems from being compromised, could just as easily be the first line of defense as the last line. In fact, a defender working for an average organization might be the *only* line of defense—the only thing standing between the bad guy and a headline-making data breach. Worse yet, perhaps the incident doesn't make headlines, and no one, including the defender, is the wiser.

Either way, when whatever crazy new Web 2.0 Ajax-laced HTML5-laden application has traversed the software development life cycle and successfully made it past the QA gate, when the third-party penetration testers are long gone, after management has signed off on all the security exceptions, and the application has been released to production, with or without the defender's knowledge or consent, "security" then becomes entirely the defender's responsibility. Rest assured that vulnerabilities will remain or will be introduced eventually. So, when all is said and done, a defender's mission is to secure the insecure, to identify incoming attacks and thwart them, and to detect and contain breaches.

That's why there should be no doubt about the importance of the role of a defender. Defenders often safeguard the personal data of millions of people. They may protect millions, perhaps billions, of dollars in online transactions and the core intellectual property of the entire business. You can bet that with so much on the line, with so much valuable information being stored, someone will want to steal it. And the bigger and more high profile the system, the more sustained and targeted the incoming attacks will be.

Making matters even more challenging, the bad guys have the luxury of picking their shots. They may attack a system whenever they want to, or not. A defender's job is 24/7/365, holidays, weekends, vacation days. The system must be ready, and the defender must be ready, at all times.

A defender's job description could read much like Ernest Shackleton's famous advertisement when he was looking for men to accompany him on his next Antarctic expedition:

> *Men wanted for hazardous journey. Low wages, bitter cold, long hours of complete darkness. Safe return doubtful. Honour and recognition in event of success.*

A defender's success really comes down to understanding a few key points about the operational environment in which he or she works:

- Web sites are often deployed in such a way that they cannot be adequately mirrored in development, QA, or even staging. This means that the real and true security posture, the real and true risk to the business, can be fully grasped only when it hits production and becomes an actual risk. As such, defenders must be able to think on their feet, be nimble, and react quickly.
- Defenders will find themselves responsible for protecting web sites they did not create and have little or no insight into or control over. Management may not respect security and may be unwilling to fix identified vulnerabilities in a timely fashion, and that could be the long-term standard operating procedure. And maybe this is the right call, depending on business risk and the estimated cost of software security. Whatever the case may be, defenders must be able to identify incoming attacks, block as many exploits as they can, and contain breaches.
- Fighting fires and responding to daily threats must be an expected part of the role. Whether the business is fully committed to software security is immaterial, because software will always have vulnerabilities. Furthermore, everyone gets attacked eventually. A defender never wants to be late in seeing an attack and the last one to know about a breach. For a defender, attack identification and response time are crucial.
- Defenders, because they are on the front lines, learn a tremendous amount about the application's risk profile and the necessary security readiness required to thwart attackers. This intelligence is like gold when communicated to developers who are interested in creating ever more resilient systems. This intelligence is also like gold when informing the security assessment teams about what types of vulnerabilities they should focus on first when testing systems in either QA or production. Everyone needs actionable data. The best defenders have it.

Putting these practices to use requires specialized skills and experience. Normally, aspiring defenders don't get this type of how-to instruction from product README files or FAQs. Historically, the knowledge came from conversations with peers, blog posts, and mailing list conversations. Information scattered around the Internet is hard to cobble together into anything actionable. By the time you do, you might already have been hacked. Maybe that's why you picked up this book. Clearly web-based attackers are becoming more active and brazen every day, with no signs of slowing.

For a defender to be successful, there is simply no substitute for experience. And this kind of experience comes only from hour after hour, day after day, and year after year of being on the battlefield, learning what strategies and tactics work in a given situation.

This kind of experience certainly doesn't come quickly or easily. At the same time, this kind of information and the lessons learned can be documented, codified, and shared. This is what Ryan Barnett offers in this book: recipes for defense—recipes for success.

To all defenders, I leave you in Ryan's accomplished and capable hands. His reputation speaks for itself. Ryan is one of the original defenders. He has contributed more than anyone else in web security to define the role of the defender. And he's one of the best field practitioners I've ever seen. Good luck out there!

Jeremiah Grossman
Chief Technology Officer
WhiteHat Security, Inc.