The Manager's Guide to Web Application Security:

A Concise Guide to the Weaker Side of the Web

Ron Lepofsky

Apress®

The Manager's Guide to Web Application Security: A Concise Guide to the Weaker Side of the Web

ISBN-13 (pbk): 978-1-4842-0149-7

ISBN-13 (electronic): 978-1-4842-0148-0

Managing Director: Welmoed Spahr
Acquisitions Editor: Robert Hutchinson
Technical Reviewer: Dave Millier
Developmental Editor: Chris Nelson
Editorial Board: Steve Anglin, Mark Beckner, Gary Cornell, Louise Corrigan, James DeWolf, Jonathan Gennick, Robert Hutchinson, Michelle Lowman, James Markham, Matthew Moodie, Jeff Olson, Jeffrey Pepper, Douglas Pundick, Ben Renow-Clarke, Gwenan Spearing, Matt Wade, Steve Weiss
Coordinating Editor: Rita Fernando
Copy Editor: Jana Weinstein
Compositor: SPi Global
Indexer: SPi Global

Distributed to the book trade worldwide by Springer Science+Business Media New York, 233 Spring Street, 6th Floor, New York, NY 10013. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springeronline.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a **Delaware** corporation.

For information on translations, please e-mail rights@apress.com, or visit www.apress.com.

Apress and friends of ED books may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Special Bulk Sales–eBook Licensing web page at www.apress.com/bulk-sales.

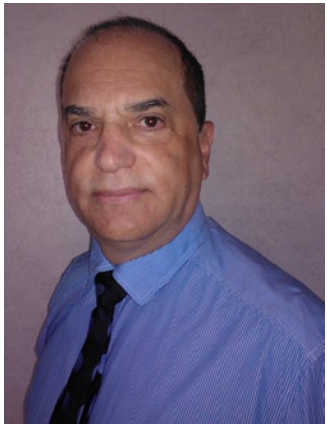
Any source code or other supplementary material referenced by the author in this text is available to readers at www.apress.com. For detailed information about how to locate your book's source code, go to www.apress.com/source-code/.

To my wonderful family: Eilene, Steven, Charlotte, and Alice

Contents at a Glance

Contents

About the Author



Ron Lepofsky, B.A. SC. (Mech Eng), CISSP, CISM is the President of ERE Information Security and Compliance Auditors (www.ere-security.ca). Ron is an active member in ISACA, ISC2, and several online security communities. Ron has written several published articles relating to a wide variety of security topics and makes home-made dark chocolate treats.

About the Technical Reviewer

Dave Millier is well-known in the Canadian high-tech marketplace, where he's been helping customers with their security and compliance needs for over 20 years. For the past 15 years, Dave has focused on growing one of Canada's most recognized MSSPs, Sentry Metrics, where as the founder he created and brought to market the industry-leading security and risk compliance dashboard, theSentry. Dave is continuing the development of this award-winning platform in his new company, Uzado (www.uzado.com).

Dave has presented at many network and security conferences including Network World, Comdex, InfoSecurity Canada, SC Congress, and SecTor (Security Education Conference Toronto), Canada's preeminent security conference. Dave has written numerous articles for security and networking magazines and is often quoted in the press and news stories. Dave was recognized as one of the top eight security professionals you need to know in the GTA.

Dave is a recognized leader in the field of governance and risk compliance and has helped a number of Canada's leading organizations build their corporate security strategies, align them with regulatory and corporate requirements, and then implement strategies to help them "attain and maintain" their overall compliance.

When Dave's not pursuing his plans for world domination, one client at a time, he's an avid (amateur!) dual sport motorcycle rider and loves to spend his spare time off-road motorcycling.

Acknowledgments

First, I would like to express my appreciation and thanks to all my clients, many of whom I have worked with for years. You have taught me much about understanding your needs and how to satisfy them, all based upon the all-important activity of listening. You have taught me how your management views your responsibilities to secure their network infrastructures and applications and how to best articulate your suggestions in terms of their understanding—return on investment.

I would like to thank Dave Millier, Chuck Ben-Tzur, and Assef Levy, a team of information security experts from whom I have learned a great deal.

I am also grateful to the organizations of ISACA and ISC2 for their informative, practical, and highly useful training and certifications.

I would like to thank Experian, ISACA, ISSA, ISO, NERC, PCI, and SANS for graciously extending to me copyright permissions for their content which I have reproduced in this book.

I am grateful for my years as a student at University of Toronto department of Mechanical Engineering, where I was taught critical thinking and project management skills that well prepared me for my career.

My grateful thanks goes to my editors at Apress Media; Robert Hutchinson, Jonathan Hassell, Rita Fernando, and Chris Nelson, and of course to my senior editor Jeff Olson. Jon, Rita, and Chris transformed an immmature draft into hopefully a clear and useful book. My deep thanks also to the Apress editorial board for having the confidence in me to undertake this project.

Last, but most important, I thank my wife Eilene for her wise counsel and for her uncanny instincts that have directed me well in all things. And a special thank you to her for her generous contribution of time and assistance with this book.

Introduction

Executives and security technologists need a common understanding of web application security risks and how to find and fix them. This book provides common points of understanding to enable both groups to collaborate on building secure web application frameworks.

The book translates with simplicity and brevity the technical world of threats, vulnerabilities, mitigation, prevention, and level of technical risk into language that executives can quickly understand.

Similarly, the book shows executives how to express their need to understand cost, risk and risk reduction, and return on investment in terms security technologists can relate to.

About the Book

Chapter 1 explains how to calculate IT security risk, including descriptions of risk-related terms that are applicable. These terms will then be used elsewhere throughout the book. Chapter 2 identifies and explains the various types of web application security audits. Chapter 3 identifies web application vulnerability classes, specific vulnerabilities, and their risks. Chapter 4 covers the vulnerabilities' remediation.

Chapters 5 and 6 discuss the prevention of web application vulnerabilities, including how to manage security of third-party applications. Chapter 7 shows how to integrate compliance to various standards with security. Chapter 8 brings it all together by explaining how to create a business case to cost justify web application security, and Chapter 9 offers some final thoughts.

Appendices A through H provide more details on compliance standards and sources of expert information.

Companion Files

There are several companion spreadsheets which are used in Chapters 1, 7, and 8. You can download them from the Source Code/Downloads tab on the book's Apress web page (www.apress.com/9781484201497).

These spreadsheets are designed for the reader to readily implement the various strategies proposed in this book.

The first set of spreadsheets is used for various calculations of risk in Chapter 1. Another spreadsheet provides a summary of vulnerability classes, specific vulnerabilities, and their remediation and risks discussed in Chapters 3 and 4. The Summary of Risk and Remediation, with Compliance Standards Added table from Chapter 7 also is included.

Finally, the Chapter 8 spreadsheets are calculators of risk, costs, and returns on investment, which form the business case for cost-justifying web application security. These spreadsheets include a template for creating a weighted score of the health of security for any specific environment.

Contact and More Information

I would be happy to answer any questions or respond to any feedback from readers of this book. Perhaps we can implement these discussions into a second edition! Please feel free to contact me at RonL@ere-security.ca or request further documentation on security subjects related to this book at my web site www.ere-security.ca.

Disclaimer

The advice and information I give in this book are of general applicability and may not be suitable in specific applications. I urge managers always to consult their IT security specialists before implementing any security measures. I cannot accept any legal responsibility for any errors or omissions that may be made or information or advice given.