

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

Copyright © 2014 by Ron Lepofsky

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

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

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

Trademarked names, logos, and images may appear in this book. Rather than use a trademark symbol with every occurrence of a trademarked name, logo, or image we use the names, logos, and images only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

The use in this publication of trade names, trademarks, service marks, and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

Portions of this production are provided courtesy of PCI Security Standards Council, LLC ("PCI SSC") and/or its licensors, and are protected by copyright laws. All rights reserved. Neither PCI SSC nor its licensors endorses this production, its providers or the methods, procedures, statements, views, opinions or advice contained herein. All references to documents, materials or portions thereof provided by PCI SSC should be read as qualified by the actual materials made available by PCI SSC. For questions regarding such materials, please contact PCI SSC through its web site at <https://www.pcisecuritystandards.org>.

Portions included within the PCI SSC materials in this production are copyrighted by Experian Information Solutions, Inc. All rights reserved. Experian is the registered trademark of Experian Information Solutions, Inc.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

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

About the Author	xvii
About the Technical Reviewer	xix
Acknowledgments	xxi
Introduction	xxiii
■ Chapter 1: Understanding IT Security Risks.....	1
■ Chapter 2: Types of Web Application Security Testing	13
■ Chapter 3: Web Application Vulnerabilities and the Damage They Can Cause	21
■ Chapter 4: Web Application Vulnerabilities and Countermeasures	47
■ Chapter 5: How to Build Preventative Countermeasures for Web Application Vulnerabilities.....	81
■ Chapter 6: How to Manage Security on Applications Written by Third Parties.....	95
■ Chapter 7: Integrating Compliance with Web Application Security	99
■ Chapter 8: How to Create a Business Case for Web Application Security	111
■ Chapter 9: Parting Thoughts.....	131

■ Appendix A: COBIT® 5 for Information Security	133
■ Appendix B: Experian EI3PA Security Assessment	147
■ Appendix C: ISO/IEC 17799:2005 and the ISO/IEC 27000:2014 Series	161
■ Appendix D: North American Energy Council Security Standard for Critical Infrastructure Protection (NERC CIP)	165
■ Appendix E: NIST 800 Guidelines	177
■ Appendix F: Payment Card Industry (PCI) Data Security Standard	179
■ Appendix G: Sarbanes-Oxley Security Compliance Requirements	197
■ Appendix H: Sources of Information	199
Index	201

Contents

- About the Author xvii**
- About the Technical Reviewer xix**
- Acknowledgments xxi**
- Introduction xxiii**
- Chapter 1: Understanding IT Security Risks..... 1**
 - Web Application Security Terminology 1
 - Risk Calculation Models 4
 - DREAD 5
 - How to Calculate Web Application Security Risk..... 6
 - Standard Calculations.....6
 - A Customized Approach.....7
 - Calculating a Security Risk.....8
 - Calculating Risk from Multiple Vulnerabilities for Any Asset9
 - Calculating the Monetary Value at Risk for Any Asset9
 - Sources of Web Application Security Vulnerability Information..... 10
 - Summary 11
- Chapter 2: Types of Web Application Security Testing 13**
 - Understanding the Testing Process 14
 - Web Application Audits 14
 - Vulnerability Assessment..... 15
 - Postremediation Testing 18

Important Report Deliverables for All Testing Reports.....	18
Summary.....	19
■ Chapter 3: Web Application Vulnerabilities and the Damage They Can Cause	21
Lack of Sufficient Authentication	22
Weak Password Controls.....	22
Passwords Submitted Without Encryption.....	23
Username Harvesting	23
Weak Session Management.....	23
Weak SSL Ciphers Support.....	25
Information Submitted Using the GET Method	25
Self-Signed Certificates, Insecure Keys, and Passwords	25
Username Harvesting Applied to Forgotten Password Process.....	26
Autocomplete Enabled on Password Fields.....	26
Session IDs Nonrandom and Too Short.....	27
Weak Access Control.....	27
Frameable Response (Clickjacking).....	27
Cached HTTPS Response.....	28
Sensitive Information Disclosed in HTML Comments	28
HTTP Server Type and Version Number Disclosed	29
Insufficient Session Expiration	29
HTML Does Not Specify Charset	29
Session Fixation	30
Insecure Cookies	30
Weak Input Validation at the Application Level.....	32
Lack of Validated Input Allowing Automatic Script Execution.....	32
Unauthorized Access by Parameter Manipulation	33
Buffer Overflows.....	33
Forms Submitted Using the GET Method.....	34

Redirects and Forwards to Insecure Sites	34
Application Susceptible to Brute-Force Attacks	34
Client-Side Enforcement of Server-Side Security.....	35
Injection Flaws	35
SQL Injection.....	35
Blind SQL Injection	36
Link Injection	36
HTTP Header Injection Vulnerability.....	36
HTTP Response-Splitting Attack	36
Unauthorized View of Data	37
Web Application Source Code Disclosure	37
Web Directories Enumerated	38
Active Directory Object Default Page on Server	38
Temporary Files Left in the Environment.....	38
Internal IP Address Revealed by Web Server	39
Server Path Disclosed	39
Hidden Directory Detected.....	39
Unencrypted VIEWSTATE.....	40
Obsolete Web Server	40
Query Parameter in SSL Request	40
Error Handling	40
Cross-Site Scripting Attacks.....	41
Reflected Cross-Site Scripting Attack	41
Stored Cross-Site Scripting Attack	42
Cross-Site Request Forgery Attack.....	43
Security Misconfigurations and Use of Known Vulnerable Components	43
Denial-of-Service Attack	44

Related Security Issues	44
Storage of Data at Rest.....	44
Storage of Account Lists.....	45
Password Storage.....	45
Insufficient Patch Management.....	45
Summary	46
■ Chapter 4: Web Application Vulnerabilities and Countermeasures	47
Lack of Sufficient Authentication	48
Weak Password Controls.....	49
Passwords Submitted Without Encryption.....	50
Username Harvesting	50
Weak Session Management	50
Weak SSL Ciphers Support.....	51
Information Submitted Using the GET Method	52
Self-Signed Certificates, Insecure Keys, and Passwords	52
Username Harvesting Applied to Forgotten Password Process.....	53
Autocomplete Enabled on Password Fields.....	53
Session IDs Nonrandom and Too Short.....	53
Weak Access Control	54
Frameable Response (Clickjacking).....	55
Cached HTTP Response	55
Sensitive Information Disclosed in HTML Comments	56
HTTP Server Type and Version Number Disclosed	56
Insufficient Session Expiration	57
HTML Does Not Specify Charset	57
Session Fixation	58
Insecure Cookies	58

Weak Input Validation at the Application Level..... 59

- Lack of Validated Input Allowing Automatic Script Execution..... 59
- Unauthorized Access by Parameter Manipulation 60
- Buffer Overflows..... 60
- Form Submitted Using the GET Method..... 61

Redirects and Forwards to Insecure Sites 61

- Application Susceptible to Brute-Force Attacks 62
- Client-Side Enforcement of Server-Side Security..... 62

Injection Flaws 62

- SQL Injection..... 63
- Blind SQL Injection 64
- Link Injection 65
- HTTP Header Injection Vulnerability..... 65
- HTTP Response-Splitting Attack 66

Unauthorized View of Data 66

- Web Application Source Code Disclosed 67
- Web Directories Enumerated 68
- Active Directory Object Default Page on Server 68
- Temporary Files Left in the Environment..... 69
- Internal IP Address Revealed by Web Server 69
- Server Path Disclosed 69
- Hidden Directory Detected..... 70
- Unencrypted VIEWSTATE..... 70
- Obsolete Web Server 70
- Query Parameter in SSL Request 71

Error Handling 71

Cross-Site Scripting Attacks.....	72
Reflected Cross-Site Scripting Attack	72
Stored Cross-Site Scripting Attack	73
Cross-Site Request Forgery Attack.....	74
Security Misconfigurations and Using Known Vulnerable Components	75
Denial-of-Service Attack	75
Related Security Issues.....	76
Storage of Data at Rest.....	76
Storage of Account Lists.....	77
Password Storage.....	78
Insufficient Patch Management.....	78
Summary.....	79
■ Chapter 5: How to Build Preventative Countermeasures for Web Application Vulnerabilities	81
Security-in-Software-Development Life Cycle	82
Framework for Secure Web Application Code	84
Web Application Security Testing	89
Manual vs. Automated Code Testing.....	90
Multilayered Defense.....	93
Security Technology for Protecting Web Applications and Their Environments	93
Summary.....	94
■ Chapter 6: How to Manage Security on Applications Written by Third Parties.....	95
Transparency of Problem Resolution.....	95
Liability Insurance as Backup for Transparency of Problem Resolution	97
Change Management	97
Summary.....	98

■ Chapter 7: Integrating Compliance with Web Application Security	99
Regulations, Standards, and Expert Organization Recommendations	99
Government Regulations	100
Industry Standards	100
Recommendations from Expert Organizations	101
Financial Auditors' Favorites	102
Leading Standards and Regulations.....	103
COBIT	103
COBIT 5 for IT Security.....	104
E13PA and PCI DSS.....	104
ISO 27000	105
NIST	105
NERC CIP.....	105
Sarbanes-Oxley	106
Integrating Compliance and Security Reporting.....	106
Summary.....	110
■ Chapter 8: How to Create a Business Case for Web Application Security	111
Assessing the Risk	112
Identifying Risk and Its Business Impact	112
Estimating the Chance of Occurrence of Each Event	113
Qualitative and Quantitative Risk Analysis	113
Calculating Annual Loss Expectancy	114
Calculating the Cost of Prevention and Remediation	115
Calculating the Return on Security Investment.....	116
Creating the Business Case for Executives.....	119

Measuring and Cost-Justifying Residual Risk.....	122
Calculating Security Status and Residual Risk with a Monthly Security Health Score	123
How to Cost-Justify and Triage Vulnerabilities for Remediation.....	124
Noting the Difference Between Remediating and Fixing.....	125
Calculating the Cost of Mitigation	126
Measuring the Effectiveness of Mitigation	127
Determining Whether Return on Security Investment Objectives Are Met.....	129
Summary.....	130
■ Chapter 9: Parting Thoughts.....	131
■ Appendix A: COBIT® 5 for Information Security.....	133
F.3 Secure Development.....	134
Description of the Service Capability.....	134
Attributes	134
Goals.....	135
F.4 Security Assessments.....	135
Description of the Service Capability.....	135
Attributes	136
Goals.....	137
F.5 Adequately Secured and Configured Systems, Aligned With Security Requirements and Security Architecture	137
Description of the Service Capability.....	137
Attributes	138
Goals.....	139
F.6 User Access and Access Rights in Line With Business Requirements	139
Description of the Service Capability.....	139
Attributes	140
Goals.....	142

F.7 Adequate Protection Against Malware, External Attacks and Intrusion Attempts	143
Description of the Service Capability.....	143
Attributes	144
Goals.....	145
■ Appendix B: Experian EI3PA Security Assessment	147
■ Appendix C: ISO/IEC 17799:2005 and the ISO/IEC 27000:2014 Series.....	161
ISO/IEC 17799:2005.....	161
The ISO/IEC 27000:2014 Series.....	162
■ Appendix D: North American Energy Council Security Standard for Critical Infrastructure Protection (NERC CIP)	165
NERC CIP Standards Currently in Force.....	166
Future NERC CIP Standards.....	166
Future Standard CIP-007-5: Cyber Security — System Security Management	167
Requirement R1:.....	167
Requirement R2:.....	168
Requirement R3:.....	170
Requirement R4:.....	171
Requirement R5:.....	173
Rationale for R5:.....	175
■ Appendix E: NIST 800 Guidelines.....	177
■ Appendix F: Payment Card Industry (PCI) Data Security Standard	179
Maintain a Vulnerability Management Program	179

■ CONTENTS

■ **Appendix G: Sarbanes-Oxley Security Compliance Requirements** **197**

■ **Appendix H: Sources of Information**..... **199**

Index..... **201**

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 immature 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.