Iron-Clad Java: Building Secure Web Applications

Java™

Best Practices for Secure Java Web Application Development

Jim Manico
August Detlefsen

Contributing Author, Kevin Kenan

Technical Editor, Milton Smith
Oracle Senior Principal Security Product Manager, Java

Oracle Press™

Oracle Press™

Iron-Clad Java

Building Secure Web Applications

Jim Manico
August Detlefsen

New York Chicago San Francisco
Athens London Madrid Mexico City
Milan New Delhi Singapore Sydney Toronto

ISBN: 978-0-07-183589-3

MHID: 0-07-183589-X

The material in this eBook also appears in the print version of this title: ISBN: 978-0-07-183588-6,
MHID: 0-07-183588-1.

eBook conversion by codeMantra
Version 2.0

To all the developers and software professionals we have worked with, whether it was teaching secure coding, ethically hacking your software, or writing code alongside you, it has been an honor working with you. To all hackers, both builder and breaker, and to everyone who has ever poked around an application and said "I wonder what happens if I try …", you are an inspiration. Stay curious. And to anyone who is hungry to learn something new about software development and software security, this book is for you.

About the Authors

Jim Manico (Hawaii) is an author and educator of developer security awareness trainings. He is a frequent speaker on secure software practices and is a member of the JavaOne Rock Star Wall of Fame. Jim is also a Global Board Member for the OWASP Foundation, where he helps drive the strategic vision for the organization. He manages and participates in several OWASP projects, including the OWASP Cheat Sheet series and several secure coding projects. For more information, see www.linkedin.com/in/jmanico.

August Detlefsen (California) is a Senior Application Security Consultant with more than eighteen years' experience in software development, enterprise application architecture, and information security. August works with major clients in financial services, health care, mobile, eCommerce, and technology to help secure web properties from potential threats. His company's consulting services include source code and infrastructure reviews, penetration testing, threat modeling, gap analysis, software security control architecture, and training. August is a graduate of Dartmouth College and an active member of OWASP. He has contributed to several OWASP projects, which provide web developers with APIs for building robust applications. August enjoys developing tools to assist penetration testers, including Burp Suite extensions to test specific frameworks such as Amazon Web Services and Google Web Toolkit. He manages the site http://canyouxssthis.com to test and compare various anti-XSS technologies. August also developed the CodeMagi Clickjacking Defense, which is the current gold standard for clickjacking prevention.

About the Technical Editor

Milton Smith (California) leads the strategic security program for Java platform products as Senior Principal Security PM at Oracle. Milton is responsible for defining the security vision for Java and managing working relationships with security organizations, researchers, and the industry at large. Prior to Oracle, Milton led security for Yahoo's User Data Analytics (UDA) property. For more information, see https://www.linkedin.com/in/spoofzu or www.securitycurmudgeon.com/.