

ORACLE®

# Iron-Clad Java: Building Secure Web Applications



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®**

*Oracle Press™*

# Iron-Clad Java

## Building Secure Web Applications

Jim Manico  
August Detlefsen

**Mc  
Graw  
Hill**  
Education

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

Copyright © 2015 by McGraw-Hill Education (Publisher). All rights reserved. Except as permitted under the United States Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but they may not be reproduced for publication.

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

All trademarks are trademarks of their respective owners. Rather than put a trademark symbol after every occurrence of a trademarked name, we use names in an editorial fashion only, and to the benefit of the trademark owner, with no intention of infringement of the trademark. Where such designations appear in this book, they have been printed with initial caps.

McGraw-Hill Education eBooks are available at special quantity discounts to use as premiums and sales promotions or for use in corporate training programs. To contact a representative, please visit the Contact Us page at [www.mhprofessional.com](http://www.mhprofessional.com).

Information has been obtained by Publisher from sources believed to be reliable. However, because of the possibility of human or mechanical error by our sources, Publisher, or others, Publisher does not guarantee the accuracy, adequacy, or completeness of any information included in this work and is not responsible for any errors or omissions or the results obtained from the use of such information.

Oracle Corporation does not make any representations or warranties as to the accuracy, adequacy, or completeness of any information contained in this Work, and is not responsible for any errors or omissions.

## TERMS OF USE

This is a copyrighted work and McGraw-Hill Education and its licensors reserve all rights in and to the work. Use of this work is subject to these terms. Except as permitted under the Copyright Act of 1976 and the right to store and retrieve one copy of the work, you may not decompile, disassemble, reverse engineer, reproduce, modify, create derivative works based upon, transmit, distribute, disseminate, sell, publish or sublicense the work or any part of it without McGraw-Hill Education's prior consent. You may use the work for your own noncommercial and personal use; any other use of the work is strictly prohibited. Your right to use the work may be terminated if you fail to comply with these terms.

THE WORK IS PROVIDED "AS IS." MCGRAW-HILL EDUCATION AND ITS LICENSORS MAKE NO GUARANTEES OR WARRANTIES AS TO THE ACCURACY, ADEQUACY OR COMPLETENESS OF OR RESULTS TO BE OBTAINED FROM USING THE WORK, INCLUDING ANY INFORMATION THAT CAN BE ACCESSED THROUGH THE WORK VIA HYPERLINK OR OTHERWISE, AND EXPRESSLY DISCLAIM ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. McGraw-Hill Education and its licensors do not warrant or guarantee that the functions contained in the work will meet your requirements or that its operation will be uninterrupted or error free. Neither McGraw-Hill Education nor its licensors shall be liable to you or anyone else for any inaccuracy, error or omission, regardless of cause, in the work or for any damages resulting therefrom. McGraw-Hill Education has no responsibility for the content of any information accessed through the work. Under no circumstances shall McGraw-Hill Education and/or its licensors be liable for any indirect, incidental, special, punitive, consequential or similar damages that result from the use of or inability to use the work, even if any of them has been advised of the possibility of such damages. This limitation of liability shall apply to any claim or cause whatsoever whether such claim or cause arises in contract, tort or otherwise.

*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](http://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://canyousssthis.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/](http://www.securitycurmudgeon.com/).