Hacking Exposed Web Applications: Web Application Security Secrets and Solutions, 3rd Edition

By Joel Scambray, Vincent Liu and Caleb Sima

Reviewed by Connie Spinelli, CISA, CFE, CIA, CMA, CPA, is a risk management consultant providing governance risk and compliance (GRC), enterprise risk management (ERM) and Sarbanes-Oxley/Internal audit program infrastructure solutions and education. Utilizing her experiences and training in the areas of management accounting; internal and external financial, IT and operational audit; and business process risks and controls, Spinelli is in a unique position to strategically work with all members of the C-suite to help them reach their compliance, financial and operational risk management goals. As well as owning her own consulting practice, GRC Solutions LLC, she is a subject matter expert contract writer for Protiviti, a business consulting and internal audit firm.

Do you have something to say about this article?
Visit the Journal pages of the ISACA web site (www.isaca.org/journal), find the article, and choose the Comments tab to share your thoughts.

Hacking Exposed Web Applications: Web Application Security Secrets and Solutions, 5th Edition is an eye-opening resource for grasping the realities of today’s web application security landscape. Accomplished authors Joel Scambray, Vincent Liu and Caleb Sima understand the landscape of the latest web application vulnerabilities as well as the exploitation techniques and tradecrafts that are being deployed against those vulnerabilities.

As businesses push more of their information and commerce to their customers through web applications, the confidentiality and integrity of these transactions is their fundamental, if not mandatory, responsibility. This publication aims to satisfy the needs of those with the need to understand and justify why a control (or corporate expenditure) is necessary. The authors collaborate to provide an easy-to-understand comprehensive blueprint for application developers, security professionals and the auditors charged with living up to this responsibility. Its intended audience is broad, from those with little knowledge or hands-on experience in preventing or detecting web application security to the experienced.

Hacking Exposed Web Applications, begins with a broad overview of web application hacking tools and techniques while showing concrete examples. Each chapter describes one aspect of the attack methodology. Once read as a learning guide or textbook, it should become a desk reference for the business library.

Applicable to all industries, the first section of the book is devoted to describing the basics: web application hacking, infrastructure and application profiling, and web application platforms. The meat of the book is devoted to describing attacks: web authentication and authorization attacks, input injection attacks, web application management attacks, and web client hacks. The second half of the book is devoted to the web application security program and reflects the major components of the full-knowledge methodology: threat modeling, code review and security testing. This third edition embraces the framework concept and integrates the cumulative learning to this point into an “ideal” enterprise web application security program.

Two aspects of the book are of particular note. The book’s focus is on identifying, exploiting and mitigating common web application security holes, with an emphasis on server-side flaws, which is expected. However, the book then addresses web-client exploits and vulnerabilities. The authors go beyond the company boundaries to include client exploits: a best-practice exercise for today’s security professionals to think beyond their corporate perimeters when brainstorming vulnerabilities and developing their security programs. Second, Hacking Exposed Web Applications is written from the perspective of an intruder—another best-practice rule of thumb for those tasked with securing the organization.

The book ends with a comprehensive web application security checklist that summarizes many recommendations and countermeasures made throughout the book, and also serves as a discreet reminder of the many security best practices that should be considered when designing and operating any web application.

The strength of the 450-page book lies in its practicality and usefulness. The authors share a plethora of reference sites and further reading tips, cautions, notes, and best practices. Whether a business leader attempting to understand the threat space for in an enterprise, an engineer tasked with writing code for sites, or a security engineer attempting to identify and mitigate the threats to an application, all readers will benefit from this publication.

EDITOR’S NOTE
Hacking Exposed Web Applications: Web Application Security Secrets and Solutions, 5th Edition is available from the ISACA Bookstore. For information, see the ISACA Bookstore Supplement in this Journal, visit www.isaca.org/bookstore, e-mail bookstore@isaca.org or telephone +1.847.660.5650.