
Date
2011

Author
Scambray, Joel, author.
Liu, Vincent.
Sima, Caleb.

Abstract
Protect your Web applications from malicious attacks by mastering the weapons and thought processes of today's hacker. Written by recognized security practitioners and thought leaders, Hacking Exposed Web Applications, Third Edition is fully updated to cover new infiltration methods and countermeasures. Find out how to reinforce authentication and authorization, plug holes in Firefox and IE, reinforce against injection attacks, and secure Web 2.0 features. Integrating security into the Web development lifecycle (SDL) and into the broader enterprise information security program is also covered in this comprehensive resource. Get full details on the hacker's footprinting, scanning, and profiling tools, including SHODAN, Maltego, and OWASP DirBuster. See new exploits of popular platforms like Sun Java System Web Server and Oracle WebLogic in operation. Understand how attackers defeat commonly used Web authentication technologies. See how real-world session attacks leak sensitive data and how to fortify your applications. Learn the most devastating methods used in today's hacks, including SQL injection, XSS, XSRF, phishing, and XML injection techniques. Find and fix vulnerabilities in ASP.NET, PHP, and J2EE execution environments. Safety deploy XML, social networking, cloud computing, and Web 2.0 services. Defend against RIA, Ajax, UGC, and browser-based, client-side exploits. Implement scalable threat modeling, code review, application scanning, fuzzing, and security testing procedures.

URI
http://dspace.fue.edu.eg/xmlui/handle/123456789/3576

Description
Includes bibliographical references and index.

xxvi, 451 pages: