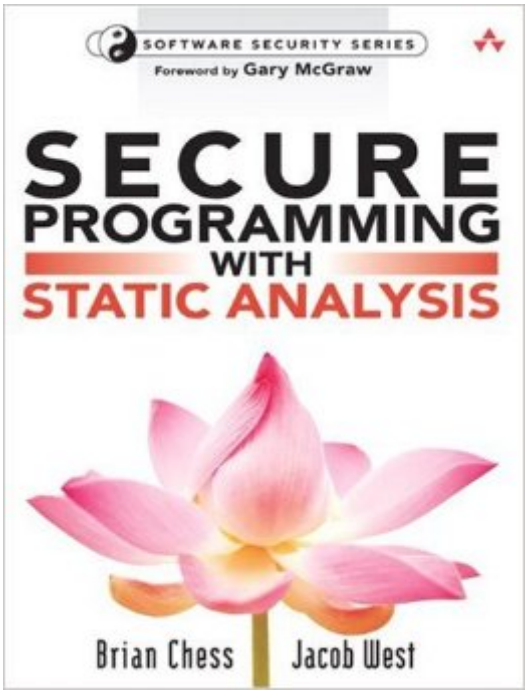
Secure Programming With Static Analysis



Synopsis

The First Expert Guide to Static Analysis for Software Security! Â Creating secure code requires more than just good intentions. Programmers need to know that their code will be safe in an almost infinite number of scenarios and configurations. Static source code analysis gives users the ability to review their work with a fine-toothed comb and uncover the kinds of errors that lead directly to security vulnerabilities. Now, thereâ ™s a complete guide to static analysis: how it works, how to integrate it into the software development processes, and how to make the most of it during security code review. Static analysis experts Brian Chess and Jacob West look at the most common types of security defects that occur today. They illustrate main points using Java and C code examples taken from real-world security incidents, showing how coding errors are exploited, how they could have been prevented, and how static analysis can rapidly uncover similar mistakes. This book is for everyone concerned with building more secure software: developers, security engineers, analysts, and testers. Â Coverage includes: Â Â Why conventional bug-catching often misses security problems Â How static analysis can help programmers get security right Â The critical attributes and algorithms that make or break a static analysis tool Â 36 techniques for making static analysis more effective on your code Â More than 70 types of serious security vulnerabilities, with specific solutions Â Example vulnerabilities from Firefox, OpenSSH, MySpace, eTrade, Apache httpd, and many more Â Techniques for handling untrusted input Â Eliminating buffer overflows: tactical and strategic approaches Â Avoiding errors specific to Web applications, Web services, and Ajax Â Security-aware logging, debugging, and error/exception handling Â Creating, maintaining, and sharing secrets and confidential information Â Detailed tutorials that walk you through the static analysis process Â â œWe designed Java so that it could be analyzed statically. This book shows you how to apply advanced static analysis techniques to create more secure, more reliable software.â • â “Bill Joy, Co-founder of Sun Microsystems, co-inventor of the Java programming language Â â œ'Secure Programming with Static Analysis' is a great primer on static analysis for security-minded developers and security practitioners. Well-written, easy to read, tells you what you need to know.â • â “David Wagner, Associate Professor, University of California Berkeley Â â œSoftware developers are the first and best line of defense for the security of their code. This book gives them the security development knowledge and the tools they need in order to eliminate vulnerabilities before they move into the final products that can be exploited.â • â “Howard A. Schmidt, Former White House Cyber Security Advisor Â BRIAN CHESS is Founder and Chief Scientist of Fortify Software, where his research focuses on practical methods for creating secure systems. He holds a Ph.D. in Computer Engineering from University of California Santa Cruz, where

he studied the application of static analysis to finding security-related code defects. Â JACOB WEST manages Fortify Softwareâ ™s Security Research Group, which is responsible for building security knowledge into Fortifyâ ™s products. He brings expertise in numerous programming languages, frameworks, and styles together with deep knowledge about how real-world systems fail. Â CD contains a working demonstration version of Fortify Softwareâ ™s Source Code Analysis (SCA) product; extensive Java and C code samples; and the tutorial chapters from the book in PDF format. Â Â Part I: Software Security and Static AnalysisÂ Â Â Â Â Â Â 1 1Â Â Â Â Â Â Â Â Â Â The Software Security ProblemÂ Â Â Â Â Â Â Â Â Â 3 2Â Â Â Â Â Â Â Â Â Â Introduction to Static Analysis 21 3Â Â Â Â Â Â Â Â Â Â Static Analysis as Part of the Code Review ProcessÂ Â Â 47 4Â Â Â Â Â Â Â Â Â Â Static Analysis InternalsÂ Â Â Â Â Â Â Â Â Â 71 Part II: Pervasive ProblemsÂ Â Â Â Â Â Â Â Â Â Â 115 5Â Â Â Â Â Â Â Â Â Â Handling Input 117 6Â Â Â Â Â Â Â Â Â Â Buffer OverflowÂ Â Â Â Â Â Â Â Â Â 175 7Â Â Â Â Â Â Â Â Â Â Bride of Buffer OverflowÂ Â Â Â Â Â Â Â 235 8Â Â Â Â Â Â Â Â Â Â Errors and ExceptionsÂ 265 Part III: Features and FlavorsÂ Â Â Â Â Â Â Â 295 9Â Â Â Â Â Â Â Â Â Â Web ApplicationsÂ Â Â Â Â Â Â 297 10Â Â Â Â Â Â Â Â Â XML and Web ServicesÂ Â Â Â Â Â Â Â Â Â 349 11Â Â Â Â Â Â Â Â Â Privacy and SecretsÂ Â Â Â 379 12Â Â Â Â Â Â Â Â Â Privileged ProgramsÂ Â Â 421 Part IV: Static Analysis in PracticeÂ 457 13Â Â Â Â Â Â Â Â Â Source Code Analysis Exercises for JavaÂ Â Â Â Â Â Â 459 14Â Â Â Â Â Â Â Â Â Source Code Analysis Exercises for C 503 EpilogueÂ Â Â Â Â Â Â Â Â Â 541 ReferencesÂ Â Â Â Â 545 IndexÂ Â 559 Â Â

Book Information

Paperback: 624 pages

Publisher: Addison-Wesley Professional (July 9, 2007)

Language: English

ISBN-10: 0321424778

ISBN-13: 978-0321424778

Product Dimensions: 6.9 x 1.4 x 9 inches

Shipping Weight: 2 pounds (View shipping rates and policies)

Average Customer Review: 4.2 out of 5 starsÂ Â See all reviewsÂ (13 customer reviews)

Best Sellers Rank: #723,003 in Books (See Top 100 in Books) #172 inÂ Books > Computers & Technology > Certification > CompTIA #284 inÂ Books > Computers & Technology > Programming > Software Design, Testing & Engineering > Testing #337 inÂ Books > Computers & Technology > Computer Science > Systems Analysis & Design

Customer Reviews

I typically review systems and commercial software from a security stand point. Recently, there has been a push to review software that is developed in-house utilizing tools such as Burpsuite and Fortify SCA. The classes that have been offered to my co-workers have been best described as How-To install the Fortify software. I was hoping to find a book with an in-depth view of utilizing Fortify to analyze source code. While the main focus of the book is not on Fortify, I was hoping that the 2 Chapters (Tutorials) would be a good start as this is the only book I know of that deals with Fortify (except the proprietary HP manuals).Why not just use the proprietary manuals and play with the software at work? Simple, I do not have time to read through manuals and play at work. I need something I can work with at home. The biggest problem I have with this book is that the software included is no longer functional. To install, you have to get a license from the Fortify website which is now owned by HP. Neither the authors nor HP will provide a license so the software is useless.If you are looking for a book to aide in secure code analysis, this is not the book for you. Secure Programming with Static Analysisâ | I read as make your applications secure by using static code analysis to identify problems. While the authors do give a fair amount of bad code to learn from, the details are less forth coming than in other books. Rather than give examples of how to use static code analysis tools to identify and correct problems, the authors give details of how they wrote rules to identify the problematic code. So if you are a programmer wanting to write your own "Fortify" software, this is a great start.

Easy, w/ Essential Programming Learn to Create your * Problem Solving * Algorithms! TODAY! w/ Machine ... engineering, r programming, iOS development) Delphi Programming with COM and ActiveX (Programming Series) (Charles River Media Programming) Java: The Ultimate Guide to Learn Java and Python Programming (Programming, Java, Database, Java for dummies, coding books, java programming) (HTML, ... Developers, Coding, CSS, PHP) (Volume 3) Programming #8:C Programming Success in a Day & Android Programming in a Day! PowerShell: For Beginners! Master The PowerShell Command Line In 24 Hours (Python Programming, Javascript, Computer Programming, C++, SQL, Computer Hacking, Programming) Excel VBA Programming: Learn Excel VBA Programming FAST and EASY! (Programming is Easy) (Volume 9) Python: Python Programming For Beginners - The Comprehensive Guide To Python Programming: Computer Programming, Computer Language, Computer Science (Machine Language) IEC 61131-3: Programming Industrial Automation Systems: Concepts and Programming Languages, Requirements for Programming Systems, Decision-Making Aids Wired for Love: How Understanding Your Partner's Brain and Attachment Style Can Help You Defuse Conflict and Build a Secure Relationship Be Comforted (Isaiah): Feeling Secure in the Arms of God (The BE Series Commentary) The Secure SAP NetWeaver Portal Bulletproof SSL and TLS: Understanding and Deploying SSL/TLS and PKI to Secure Servers and Web Applications