OMB No. 5456120017234

Writing Secure Code Second Edition Amazon Com

Are you writing Secure Code? Coding Secure Code: Best Practices, Advice for Writing Secure Code Andrii Romasiun - Writing secure JavaScript Secure Coding Practices: Writing Secure Software Common Secure Coding Techniques Black Hat Windows 2003 - Writing Secure and Hack Resistant Code 37C3 - Writing secure software Writing Secure JavaScript Why Tanya Janca wrote her book - Alice and Bob Learn Application Security Security Code Review Remarkable 2 thoughts - Distraction free writing for writers 2010 - Everything Useful I Learned About Software Security - Michael Howard CHATBOOKS UNBOXING, REVIEW \u0026 TUTORIAL 2024 || photo book tips and ideas Secure Coding Best Practice I Tested All the Writing Software So You Don't Have To Ruby on Rails - Security Setup a 2FA Key for MAXIMUM Online Security! (Yubikey Tutorial) 2011 - How to influence a Developer to write secure code in 10 minutes Get a Keyboard on Apple Watch. SE, SE 2, \u0026 Series 3 - 6. Best App. 8 Best Practices for Writing Secure Go Code Writing safe and secure code - Daniel Stenberg Writing Secure Code | Rubber Duck Dev Show 7 Webcast: Writing Secure Code for Web Applications and Services Black Hat Windows 2003 - Writing Secure and Hack Resistant Code Pt. 2 Secure Coding Back to Basics - Erlend Oftedal - NDC Security 2022 Empowering Developers to write Secure Code How to Write Safe and Secure Code | TechCode Tanya teaches Secure Coding by telling a story Webcast: Writing Secure Code in ASP.Net Writing Secure Code in Python Yan Orestes PyCon APAC 2022

Pro ASP.NET 2.0 in C# 2005, Special Edition
Assessing Network Security
Writing Secure Code
Writing Secure Code
Hacking the Code
Code
SDL, a Process for Developing Demonstrably More Secure Software
Of Land, Sea and Sky
24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them
The CERT C Secure Coding Standard
Write Better, Faster
Making Passwords Secure
Official (ISC)2 Guide to the CSSLP
Code Complete
Secure Programming with Static Analysis
The CERT® C Coding Standard, Second Edition
Secure Coding
Effective C
Code Complete, 2nd Edition
The CERT C Coding Standard
Exploiting Software: How To Break Code
How To Triple Your Writing Speed and Write More Every Day
Secure Programming Cookbook for C and C++

AIYANA HANEY

Pro ASP.NET 2.0 in C# 2005, Special Edition Addison-Wesley Professional
Widely considered one of the best practical guides to programming, Steve McConnell s original

CODE COMPLETE has been helping developers write better software for more than a decade. Now this classic book has been fully updated and revised with leading-edge practices-and hundreds of new code samples-illustrating the art and science of software construction. Capturing the body of knowledge available from research, academia, and everyday commercial practice, McConnell synthesizes the most effective techniques and must-know principles into clear, pragmatic guidance. No matter what your experience level, development environment, or project size, this book will inform and stimulate your thinking-and help you build the highest quality code.
Assessing Network Security No Starch Press
The story of an unconventional man; tales of adventure, travel and inspirational meetings. From hazardous sports to bold business ventures, music, and dance - all life is here.

Writing Secure Code

Pearson Education
Password sniffing, spoofing, buffer overflows, and denial of service: these are only a few of the attacks on today's computer systems and networks. At the root of this epidemic is poorly written, poorly tested, and insecure code that puts everyone at risk. Clearly, today's developers need help figuring out how to write code that attackers won't be able to exploit. But writing such code is surprisingly difficult. Secure Programming Cookbook for C and C++ is an important new resource for developers serious about writing secure code. It contains a wealth of solutions to problems faced by those who care about the security of their applications. It covers a wide range of topics, including safe initialization, access control, input validation, symmetric and public key cryptography, cryptographic hashes and MACs, authentication and key exchange, PKI, random numbers, and anti-tampering. The rich set of code samples provided in the book's more than 200 recipes will help programmers secure the C and C++ programs they write for both Unix® (including Linux®) and Windows® environments. Readers will learn: How to avoid common programming errors, such as buffer overflows, race conditions, and format string problems How to properly SSL-enable applications How to create secure channels for client-server communication without SSL How to integrate Public Key Infrastructure (PKI) into applications Best practices for using cryptography properly Techniques and strategies for properly validating input to programs How to launch programs securely How to use file access mechanisms properly Techniques for protecting applications from reverse engineering The book's web site supplements the book by providing a place to post new recipes, including those written in additional languages like Perl, Java, and Python. Monthly prizes will reward the best recipes submitted by readers. Secure Programming Cookbook for C and C++ is destined to become an essential part of any developer's library, a code companion developers will turn to again and again as they seek to protect their systems from attackers and reduce the risks they face in today's dangerous world.
Writing Secure Code Microsoft Press
What every software professional should know about security. Designing Secure Software consolidates Loren Kohnfelder’s more than twenty years of experience into a concise, elegant guide to improving the security of technology products. Written for a wide range of software professionals, it emphasizes building security into software design early and involving the entire team in the process. The book begins with a discussion of core concepts like trust, threats, mitigation, secure design patterns, and cryptography. The second part, perhaps this book’s most unique and important contribution to the field, covers the process of designing and reviewing a software design with security considerations in mind. The final section details the most common coding flaws that create vulnerabilities, making copious use of code snippets written in C and Python to illustrate implementation vulnerabilities. You’ll learn how to: • Identify important assets, the attack surface, and the trust boundaries in a system • Evaluate the effectiveness of various threat mitigation candidates • Work with well-known secure coding patterns and libraries • Understand and prevent vulnerabilities like XSS and CSRF, memory flaws, and more • Use security testing to proactively identify vulnerabilities introduced into code • Review a software design for security flaws effectively and without judgment Kohnfelder’s career, spanning decades at Microsoft and Google, introduced numerous software security initiatives, including the co-creation of the STRIDE threat modeling framework used widely today. This book is a modern, pragmatic consolidation of his best practices, insights, and ideas about the future of software.
Hacking the Code "O'Reilly Media, Inc."
"The security of information systems has not improved at a rate consistent with the growth and sophistication of the attacks being made against them. To address this problem, we must improve the underlying strategies and techniques used to create our systems. Specifically, we must build security in from the start, rather than append it as an afterthought. That's the point of Secure Coding in C and C++. In careful detail, this book shows software developers how to build high-quality systems that are less vulnerable to costly and even catastrophic attack. It's a book that every developer should read before the start of any serious project." --Frank Abagnale, author, lecturer, and leading consultant on fraud prevention and secure documents Learn the Root Causes of Software Vulnerabilities and How to Avoid Them Commonly exploited software vulnerabilities are usually caused by avoidable software defects. Having analyzed nearly 18,000 vulnerability reports over the past ten years, the CERT/Coordination Center (CERT/CC) has determined that a relatively small number of root causes account for most of them. This book identifies and explains these causes and shows the steps that can be taken to prevent exploitation. Moreover, this book encourages programmers to adopt security best practices and develop a security mindset that can help protect software from tomorrow's attacks, not just today's. Drawing on the CERT/CC's reports and conclusions, Robert Seacord systematically identifies the program errors most likely to lead to security breaches, shows how they can be exploited, reviews the potential consequences, and presents secure alternatives. Coverage includes technical detail on how to Improve the overall security of any C/C++ application Thwart buffer overflows and stack-smashing attacks that exploit insecure string manipulation logic Avoid vulnerabilities and security flaws resulting from the incorrect use of dynamic memory management functions Eliminate integer-related problems: integer overflows, sign errors, and truncation errors Correctly use formatted output functions without introducing format-string vulnerabilities Avoid I/O vulnerabilities, including race conditions Secure Coding in C and C++ presents hundreds of examples of secure code, insecure code, and exploits, implemented for Windows and Linux. If you're responsible for creating secure C or C++ software--or for keeping it safe--no other book offers you this much detailed, expert assistance.

Code

Createspace Independent Publishing Platform
ASP.NET 4 is the principal standard for creating dynamic web pages on the Windows platform. Pro ASP.NET 4 in C# 2010 raises the bar for high-quality, practical advice on learning and deploying Microsoft's dynamic web solution. This edition is updated with everything you need to master up to version 4 of ASP.NET, including coverage of ASP.NET MVC, ASP.NET AJAX 4, ASP.NET Dynamic Data, and Silverlight 3. Seasoned .NET professionals Matthew MacDonald and Mario Szpuszta explain how you can get the most from these groundbreaking technologies. They cover ASP.NET 4 as a whole, illustrating both the newer features and the functionality carried over from previous versions of ASP. This book will give you the knowledge you need to code real ASP.NET 4 applications in the best possible style.
SDL, a Process for Developing Demonstrably More Secure Software Pearson Education
Six years ago, Infrastructure as Code was a new concept. Today, as even banks and other conservative organizations plan moves to the cloud, development teams for companies worldwide are attempting to build large infrastructure codebases. With this practical book, Kief Morris of ThoughtWorks shows you how to effectively use principles, practices, and patterns pioneered by DevOps teams to manage cloud-age infrastructure. Ideal for system administrators, infrastructure engineers, software developers, team leads, and architects, this updated edition demonstrates how you can exploit cloud and automation technology to make changes easily, safely, quickly, and responsibly. You'll learn how to define everything as code and apply software design and engineering practices to build your system from small, loosely coupled pieces. This book covers: Foundations: Use Infrastructure as Code to drive continuous change and raise the bar of operational quality, using tools and technologies to build cloud-based platforms Working with infrastructure stacks: Learn how to define, provision, test, and continuously deliver changes to infrastructure resources Working with servers and other platforms: Use patterns to design provisioning and configuration of servers and clusters Working with large systems and teams: Learn workflows, governance, and architectural patterns to create and manage infrastructure elements
Of Land, Sea and Sky No Starch Press
“I’m an enthusiastic supporter of the CERT Secure Coding Initiative. Programmers have lots of sources of advice on correctness, clarity, maintainability, performance, and even safety. Advice on how specific language features affect security has been missing. The CERT® C Secure Coding Standard fills this need.” –Randy Meyers, Chairman of ANSI C “For years we have relied upon the CERT/CC to publish advisories documenting an endless stream of security problems. Now CERT has embodied the advice of leading technical experts to give programmers and managers the practical guidance needed to avoid those problems in new applications and to help secure legacy systems. Well done!” –Dr. Thomas Plum, founder of Plum Hall, Inc. “Connectivity has sharply increased the need for secure, hacker-safe applications. By combining this CERT standard with other safety guidelines, customers gain all-round protection and approach the goal of zero-defect software.” –Chris Tapp, Field Applications Engineer, LDRA Ltd. “I’ve found this standard to be an indispensable collection of expert information on exactly how modern software systems fail in practice. It is the perfect place to start for establishing internal secure coding guidelines. You won’t find this information elsewhere, and, when it comes to software security, what you don’t know is often exactly what hurts you.” –John McDonald, coauthor of The Art of Software Security Assessment Software security has major implications for the operations and assets of organizations, as well as for the welfare of individuals. To create secure software, developers must know where the dangers lie. Secure programming in C can be more difficult than even many experienced programmers believe. This book is an essential desktop reference documenting the first official release of The CERT® C Secure Coding Standard . The standard itemizes those coding errors that are the root causes of software vulnerabilities in C and prioritizes them by severity, likelihood of exploitation, and remediation costs. Each guideline provides examples of insecure code as well as secure, alternative implementations. If uniformly applied, these guidelines will eliminate the critical coding errors that lead to buffer overflows, format string vulnerabilities, integer overflow, and other common software vulnerabilities.

24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them

Academic Press
Since its original publication in 1999, this foundational book has become a classic in its field. This second edition, Code Version 2.0, updates the work and was prepared in part through a wiki, a web site allowing readers to edit the text, making this the first reader-edited revision of a popular book. Code counters the common belief that cyberspace cannot be controlled or censored. To the contrary, under the influence of commerce, cyberspace is becoming a highly regulable world where behavior will be much more tightly controlled than in real space. We can - we must - choose what kind of cyberspace we want and what freedoms it will guarantee. These choices are all about architecture: what kind of code will govern cyberspace, and who will control it. In this realm, code is the most significant form of law and it is up to lawyers, policymakers, and especially average citizens to decide what values that code embodies.
The CERT C Secure Coding Standard Apress
The authors look at the problem of bad code in a new way. Packed with advice based on the authors' decades of experience in the computer security field, this concise and highly readable book explains why so much code today is filled with vulnerabilities, and tells readers what they must do to avoid writing code that can be exploited by attackers. Writing secure code isn't easy, and there are no quick fixes to bad code. To build code that repels attack, readers need to be vigilant through each stage of the entire code lifecycle: Architecture, Design, Implementation, Testing and Operations. Beyond the technical, Secure Coding sheds new light on the economic, psychological, and sheer practical reasons why security vulnerabilities are so ubiquitous today. It presents a new way of thinking about these vulnerabilities and ways that developers can compensate for the factors that have produced such unsecured software in the past.

Write Better, Faster

Lovelight Lioness Productions

Learn the Root Causes of Software Vulnerabilities and How to Avoid Them Commonly exploited software vulnerabilities are usually caused by avoidable software defects. Having analyzed tens of thousands of vulnerability reports since 1988, CERT has determined that a relatively small number of root causes account for most of the vulnerabilities. Secure Coding in C and C++, Second Edition, identifies and explains these root causes and shows the steps that can be taken to prevent exploitation. Moreover, this book encourages programmers to adopt security best practices and to develop a security mindset that can help protect software from tomorrow's attacks, not just today's. Drawing on the CERT's reports and conclusions, Robert C. Seacord systematically identifies the program errors most likely to lead to security breaches, shows how they can be exploited, reviews the potential consequences, and presents secure alternatives. Coverage includes technical detail on how to Improve the overall security of any C or C++ application Thwart buffer overflows, stack-smashing, and return-oriented programming attacks that exploit insecure string manipulation logic Avoid vulnerabilities and security flaws resulting from the incorrect use of dynamic memory management functions Eliminate integer-related problems resulting from signed integer overflows, unsigned integer wrapping, and truncation errors Perform secure I/O, avoiding file system vulnerabilities Correctly use formatted output functions without introducing format-string vulnerabilities Avoid race conditions and other exploitable vulnerabilities while developing concurrent code The second edition features Updates for C11 and C++11 Significant revisions to chapters on strings, dynamic memory management, and integer security A new chapter on concurrency Access to the online secure coding course offered through Carnegie Mellon's Open Learning Initiative (OLI) Secure Coding in C and C++, Second Edition, presents hundreds of examples of secure code, insecure code, and exploits, implemented for Windows and Linux. If you're responsible for creating secure C or C++ software–or for keeping it safe–no other book offers you this much detailed, expert assistance.

Making Passwords Secure Packt Publishing Ltd

"Web Security, Privacy & Commerce" cuts through the hype and the front page stories. It tells readers what the real risks are and explains how to minimize them. Whether a casual (but concerned) Web surfer or a system administrator responsible for the security of a critical Web server, this book will tells users what they need to know.

Official (ISC)2 Guide to the CSSLP CRC Press

To celebrate recent innovations, and to demonstrate Apress' commitment to the ASP.NET market, we are publishing a special edition of Pro ASP.NET 2.0 in VB 2005, with new chapters explaining how to use these important new technologies. On top of the book's already extensive coverage, readers will learn how to create Ajax and Atlas applications in ASP.NET 2.0. They will be treated to a deeper coverage of ASP.NET 2.0 Performance Tuning and will be given a slew of bonus material to truly make this special edition special. This includes a free eBook of the title's content and a bonus 150 page eBook of carefully selected ASP.NET 2.0 articles.

Code Complete Simon and Schuster

ASP.NET 2.0 is Microsoft's premier technology for creating dynamic websites, and C# 2005 its preferred language. Development and innovation in this sector has continued at a rapid pace with the "Web 2.0" technologies of Ajax and Microsoft "Atlas" both becoming available since the .NET 2.0 launch. This special edition of Pro ASP.NET 2.0 in C# 2005 includes new chapters explaining how to use important new technologies. Beyond the book's already extensive coverage, readers will learn to create Ajax and Atlas applications in ASP.NET 2.0, and will appreciate its deeper coverage of ASP.NET 2.0 Performance Tuning.

Secure Programming with Static Analysis ReadHowYouWant.com

Get the most out of JavaScript for building web applications through a series of patterns, techniques, and case studies for clean coding Key Features Write maintainable JS code using internal abstraction, well-written tests, and well-documented code Understand the agents of clean coding like SOLID principles, OOP, and functional programming Explore solutions to tackle common JavaScript challenges in building UIs, managing APIs, and writing states Book Description Building robust apps starts with creating clean code. In this book, you'll explore techniques for doing this by learning everything from the basics of JavaScript through to the practices of clean code. You'll write functional, intuitive, and maintainable code while also understanding how your code affects the end user and the wider community. The book starts with popular clean-coding principles such as SOLID, and the Law of Demeter (LoD), along with highlighting the enemies of writing clean code such as cargo culting and over-management. You'll then delve into JavaScript, understanding the more complex aspects of the language. Next, you'll create meaningful abstractions using design patterns, such as the Class Pattern and the Revealing Module Pattern. You'll explore real-world challenges such as DOM reconciliation, state management, dependency management, and security, both within browser and server environments. Later, you'll cover tooling and testing methodologies and the importance of documenting code. Finally, the book will focus on advocacy and good communication for improving code cleanliness within teams or workplaces, along with covering a case study for clean coding. By the end of this book, you'll be well-versed with JavaScript and have learned how to create clean abstractions, test them, and communicate about them via documentation. What you will learn Understand the true purpose of code and the problems it solves for your end-users and colleagues Discover the tenets and enemies of clean code considering the effects of cultural and syntactic conventions Use modern JavaScript syntax and design patterns to craft intuitive abstractions Maintain code quality within your team via wise adoption of tooling and advocating best practices Learn the modern ecosystem of JavaScript and its challenges like DOM reconciliation and state management Express the behavior of your code both within tests and via various forms of documentation Who this book is for This book is for anyone who writes JavaScript, professionally or otherwise. As this book does not relate specifically to any particular framework or environment, no prior experience of any JavaScript web framework is required. Some knowledge of programming is assumed to understand the concepts covered in the book more effectively.

The CERT® C Coding Standard, Second Edition No Starch Press

Hacking the Code has over 400 pages of dedicated exploit, vulnerability, and tool code with corresponding instruction. Unlike other security and programming books that dedicate hundreds of pages to architecture and theory based flaws and exploits, Hacking the Code dives right into deep code analysis. Previously undisclosed security research in combination with superior programming techniques from Foundstone and other respected organizations is included in both the Local and Remote Code sections of the book. The book is accompanied with a FREE COMPANION CD containing

both commented and uncommented versions of the source code examples presented throughout the book. In addition to the book source code, the CD also contains a copy of the author-developed Hacker Code Library v1.0. The Hacker Code Library includes multiple attack classes and functions that can be utilized to quickly create security programs and scripts. These classes and functions simplify exploit and vulnerability tool development to an extent never before possible with publicly available software. Learn to quickly create security tools that ease the burden of software testing and network administration Find out about key security issues regarding vulnerabilities, exploits, programming flaws, and secure code development Discover the differences in numerous types of web-based attacks so that developers can create proper quality assurance testing procedures and tools Learn to automate quality assurance, management, and development tasks and procedures for testing systems and applications Learn to write complex Snort rules based solely upon traffic generated by network tools and exploits

Secure Coding Pearson Education

"What makes this book so important is that it reflects the experiences of two of the industry's most experienced hands at getting real-world engineers to understand just what they're being asked for when they're asked to write secure code. The book reflects Michael Howard's and David LeBlanc's experience in the trenches working with developers years after code was long since shipped, informing them of problems." --From the Foreword by Dan Kaminsky, Director of Penetration Testing, IOActive Eradicate the Most Notorious Insecure Designs and Coding Vulnerabilities Fully updated to cover the latest security issues, 24 Deadly Sins of Software Security reveals the most common design and coding errors and explains how to fix each one-or better yet, avoid them from the start. Michael Howard and David LeBlanc, who teach Microsoft employees and the world how to secure code, have partnered again with John Viega, who uncovered the original 19 deadly programming sins. They have completely revised the book to address the most recent vulnerabilities and have added five brand-new sins. This practical guide covers all platforms, languages, and types of applications. Eliminate these security flaws from your code: SQL injection Web server- and client-related vulnerabilities Use of magic URLs, predictable cookies, and hidden form fields Buffer overruns Format string problems Integer overflows C++ catastrophes Insecure exception handling Command injection Failure to handle errors Information leakage Race conditions Poor usability Not updating easily Executing code with too much privilege Failure to protect stored data Insecure mobile code Use of weak password-based systems Weak random numbers Using cryptography incorrectly Failing to protect network traffic Improper use of PKI Trusting network name resolution

Effective C Pearson Education

Passwords are not the problem. The management of passwords is the real security nightmare. User authentication is the most ignored risk to enterprise cybersecurity. When end users are allowed to generate, know, remember, type and manage their own passwords, IT has inadvertently surrendered the job title Network Security Manager to employees - the weakest link in the cybersecurity chain. Dovell Bonnett reveals the truth about the elephant in the room that no one wants to mention: Expensive backend security is worthless when the virtual front door has a lousy lock! Dovell proves that making passwords secure is not only possible, passwords can actually become an effective, cost efficient and user friendly feature of robust cybersecurity. After examining how encryption keys are secured, this book introduces a new strategy called Password Authentication Infrastructure (PAI) that rivals digital certificates. Passwords are not going away. What needs to be fixed is how passwords are managed.

Code Complete, 2nd Edition Pearson Education

This book illuminates the evolution of Quaker war tax resistance in America, as told by those who resisted and those who debated the limits of the Quaker peace testimony where it applied to taxpaying. Among the writers featured in this documentary history are Isaac Sharpless, Thomas Story, William Penn, James Logan, Benjamin Franklin, John Woolman, John Churchman, James Pemberton, Joshua Evans, Anthony Benezet, Job Scott, Warner Mifflin, Timothy Davis, James Mott, Isaac Grey, Samuel Allinson, Moses Brown, Stephen B. Weeks, Rufus Hall, Gouverneur Morris, Elias Hicks, Joshua Maule, and Cyrus G. Pringle.

The CERT C Coding Standard Apress

Provides information on advanced network testing strategies, covering such topics as detecting vulnerabilities; finding hidden hosts using DNS, WINS, and Net BIOS; war dialing and war driving; and spam and e-mail abuses.

Related with Writing Secure Code Second Edition Amazon Com:
© Writing Secure Code Second Edition Amazon Com Wow Wotlk Classic Alchemy Guide
© Writing Secure Code Second Edition Amazon Com Wowhead Lunar Festival Guide
© Writing Secure Code Second Edition Amazon Com Writing A Character Letter To A Judge