Application Development Security Guidelines

"This book provides innovative ideas and methods on the development, operation, and maintenance of secure software systems and highlights the construction of a functional software system and a secure system simultaneously"--Provided by publisher.

Most security books on Java focus on cryptography and access control, but exclude key aspects such as coding practices, logging, and web application risk assessment. Encapsulating security requirements for web development with the Java programming platform, Secure Java: For Web Application Development covers secure programming, risk assessment, and threat modeling—explaining how to integrate these practices into a secure software development life cycle. From the risk assessment phase to the proof of concept phase, the book details a secure web application development process. The authors provide in-depth implementation guidance and best practices for access control, cryptography, logging, secure coding, and authentication and authorization in web application development. Discussing the latest application exploits and vulnerabilities, they examine various options and protection mechanisms for securing web applications against these multifarious threats. The book is organized into four sections: Provides a clear view of the growing footprint of web applications Explores the foundations of secure web application development and the risk management process Delves into tactical web application security development with Java EE Deals extensively with security testing of web applications This complete reference includes a case study of an e-commerce company facing web application security challenges, as well as specific techniques for testing the security of web applications. Highlighting state-of-the-art tools for web application security testing, it supplies valuable insight on how to meet important security compliance requirements, including PCI-DSS, PA-DSS, HIPAA, and GLBA. The book also includes an appendix that covers the application security guidelines for the payment card industry standards.

Secure JavaFor Web Application DevelopmentCRC Press

Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

This book presents the latest research in the fields of computational intelligence, ubiquitous computing models, communication intelligence, communication security, machine learning, informatics, mobile computing, cloud computing and big data analytics. The best selected papers, presented at the International Conference on Innovative Data Communication Technologies and Application (ICIDCA 2020), are included in the book. The book focuses on the theory, design, analysis, implementation and applications of distributed systems and networks.

This document provides the comprehensive list of Chinese National Standards and Industry Standards (Total 17,000 standards).

The Second Edition of Security Strategies in Web Applications and Social Networking provides an in-depth look at how to secure mobile users as customer-facing information migrates from mainframe computers and application servers to Web-enabled applications. Written by an industry expert, this book provides a comprehensive explanation of the evolutionary changes that have occurred in computing, communications, and social networking and discusses how to secure systems against all the risks, threats, and vulnerabilities associated with Web-enabled applications accessible via the internet. Using examples and exercises, this book incorporates hands-on activities to prepare readers to successfully secure Web-enabled applications.

Take your apps from the small screen to the big screen and start developing for the Samsung SmartTV now! Samsung's SmartTV platform gives developers the opportunity to bring the app experience to the world of home entertainment, creating a more interactive and engaging way to reach their audience. If you're ready to expand your app development skills beyond the mobile environment, look no further than Samsung SmartTV Application Development. This unique guide shows you how to incorporate SmartTV features like Smart Interaction, gesture and voice recognition, and personalized recommendations into your app designs and take advantage of movie, video game, web, and other smart content available on the latest SmartTV offerings. Shows how to build a new SmartTV application – from planning the app design to creating a compelling user interface, adding features, and taking the app to market Walks you through the development environment, key platform capabilities, the SmartTV toolset, and testing emulator Includes helpful source code examples to use as inspiration for your own app design and instruction on using video-on-demand, gaming, multi-screen, and Smart Interaction features in your app Written by a team of experts from Handstudio, a global smart media application and solution developer whose clients include Samsung, Humax, and LG, who share their real-world insights and experience developing for the Samsung SmartTV platform Make the smart move and get Samsung SmartTV Application Development today!

In Offshore Software Development: Making It Work, hands-on managers of Offshore solutions help you answer these questions: What is Offshore and why is it an IT imperative? What do you need to do to successfully evaluate an Offshore solution? How do you avoid common pitfalls? How do you confront security and geopolitical risk? How do you handle issues related to displaced workers? The author applies her considerable experience in the analysis of such Offshore issues as the financial growth of the Offshore industry, keys to success in initiating a program, choosing and managing vendors, risk mitigation, and employee impacts. A detailed program checklist outlines the steps for successful Offshore execution, providing real-world exposure and guidance to a movement that has become a fixture in the IT realm. About the Author Tandy Gold is a 20-year veteran of the technology industry who is focused on entrepreneurial consulting and innovation. As part of her responsibilities in implementing the first Offshore initiative for a large financial institution, she created a monthly Offshore interest group. Comprised of Offshore program managers from Fortune 100 firms, together they represent more than 40 years of experience in Offshore.

This book constitutes the refereed proceedings of the 8th International Conference on Software Business, ICSOB 2017, held in Essen, Germany, in June 2017. The 11 full papers and 5 short papers presented in this volume were carefully reviewed and selected from 30 submissions. They were organized in topical sections named: software startups and platform governance; software business development; software ecosystems and App stores. Security Strategies in Web Applications and Social Networking provides a unique, in-depth look at how to secure mobile users as customer-facing information migrates from mainframe computers and application servers to Web-enabled applications. Written by an industry expert, this book provides a comprehensive explanation of the evolutionary changes that have occurred in computing, communications, and social networking and discusses how to secure systems against all the risks, threats, and vulnerabilities associated with Web-enabled applications accessible via the Internet. Using examples and exercises, this book incorporates hands-on activities to prepare readers to successfully secure Web-enabled applications. The Jones & Bartlett Learning: Information Systems Security & Assurance Series delivers fundamental IT security principles packed with real-world applications and examples for IT Security, Cybersecurity, Information Assurance, and Information Systems Security programs. Authored by Certified Information Systems Security Professionals (CISSPs), and reviewed by leading technical experts in the field, these books are current, forward-thinking resources that enable readers to solve the cybersecurity challenges of today and tomorrow. This book presents the most interesting talks given at ISSE 2012 - the forum for the inter-disciplinary discussion of how to adequately secure electronic business processes. The topics include: - Information Security Strategy; Enterprise and Cloud Computing Security - Security and Privacy Impact of Green Energy; Human Factors of IT Security - Solutions for Mobile Applications; Identity & Access Management - Trustworthy Infrastructures; Separation & Isolation - EU Digital Agenda; Cyber Security: Hackers & Threats Adequate information security is one of the basic requirements of all electronic business processes. It is crucial for effective solutions that the possibilities offered by security technology can be integrated with the commercial requirements of the applications. The reader may expect state-of-the-art: best papers of the Conference ISSE 2012. Content Information Security Strategy - Enterprise and Cloud Computing Security - Security and Privacy - Impact of Green Energy - Human Factors of IT Security - Solutions for Mobile Applications - Identity & Access Management - Trustworthy Infrastructures - Separation & Isolation - EU Digital Agenda - Cyber Security - Hackers & Threats Target Group Developers of Electronic Business Processes IT Managers IT Security Experts Researchers The Editors Norbert Pohlmann: Professor for Distributed

System and Information Security at Westfälische Hochschule Gelsenkirchen Helmut Reimer: Senior Consultant, TeleTrusT Wolfgang Schneider: Senior Adviser, Fraunhofer Institute SIT

This document provides the comprehensive list of Chinese Industry Standards - Category: YD; YD/T; YDT.

Develop the advanced cybersecurity knowledge and skills for success on the latest CompTIA Cybersecurity Analyst certification exam (CySA+ CS0-002) with Ciampa's COMPTIA CYSA+ GUIDE TO CYBERSECURITY ANALYST (CS0-002), 2nd Edition. Updated, stair-stepped content builds on material you've previously mastered as you learn to analyze and interpret threat intelligence data, identify and address both external and internal vulnerabilities and respond effectively to cyber incidents. Each module opens with an actual, recent cybersecurity event that provides context for the information that follows. Quick review questions help test your understanding as you progress through content that completely maps to the latest CySA+ CS0-002 certification. New case projects and updates illustrate actual on-the-job tasks and procedures, including controls, monitoring, incident response and compliance, to further prepare you to meet the challenges in cybersecurity today. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Although many software books highlight open problems in secure software development, few provide easily actionable, ground-level solutions. Breaking the mold, Secure and Resilient Software Development teaches you how to apply best practices and standards for consistent and secure software development. It details specific quality software developmen

Web-Application have been widely accepted by the organization be it in private, public or government sector and form the main part of any e-commerce business on the internet. However with the widespread of web-application, the threats related to the web-application have also emerged. Web-application transmit substantial amount of critical data such as password or credit card information etc. and this data should be protected from an attacker. There has been huge number of attacks on the web-application such as ‘SQL Injection’, ‘Cross-Site Scripting’, ‘Http Response Splitting’ in recent years and it is one of the main concerns in both the software developer and security professional community.This projects aims to explore how security can be incorporated by using security pattern in web-application and how effective it is in addressing the security problems of web-application.

Cyber-attacks continue to rise as more individuals rely on storing personal information on networks. Even though these networks are continuously checked and secured, cybercriminals find new strategies to break through these protections. Thus, advanced security systems, rather than simple security patches, need to be designed and developed. Exploring Security in Software Architecture and Design is an essential reference source that discusses the development of security-aware software systems that are built into every phase of the software architecture. Featuring research on topics such as migration techniques, service-based software, and building security, this book is ideally designed for computer and software engineers, ICT specialists, researchers, academicians, and field experts.

Learn application security from the very start, with this comprehensive and approachable guide! Alice and Bob Learn Application Security is an accessible and thorough resource for anyone seeking to incorporate, from the beginning of the System Development Life Cycle, best security practices in software development. This book covers all the basic subjects such as threat modeling and security testing, but also dives deep into more complex and advanced topics for securing modern software systems and architectures. Throughout, the book offers analogies, stories of the characters Alice and Bob, real-life examples, technical explanations and diagrams to ensure maximum clarity of the many abstract and complicated subjects. Topics include: · Secure requirements, design, coding, and deployment · Security Testing (all forms) · Common Pitfalls · Application Security Programs · Securing Modern Applications · Software Developer Security Hygiene Alice and Bob Learn Application Security is perfect for aspiring application security engineers and practicing software developers, as well as software project managers, penetration testers, and chief information security officers who seek to build or improve their application security programs. Alice and Bob Learn Application Security illustrates all the included concepts with easy-to-understand examples and concrete practical applications, furthering the reader’s ability to grasp and retain the foundational and advanced topics contained within.

This book constitutes the refereed proceedings of the Fifth International Conference on Service-Oriented Computing, ICSOC 2007. The 30 revised full papers and 14 short papers are organized in topical sections on service deployment, business process design, service discovery, quality of service support, testing and validation, service assembly, service properties, service modeling, SOA composition/experience/runtime/governance and QoS and composite service support.

A step-by-step book and eBook guide for web application development and quick tips to enhance applications using Lotus Domino.

Reengineering MIS: Aligning Information Technology and Business Operations provides the background and foundation that will allow the radical change necessary for MIS to contribute to the success of the organization. It provides detailed understanding of reengineering initiatives in business.

Pro .NET Best Practices is a practical reference to the best practices that you can apply to your .NET projects today. You will learn standards, techniques, and conventions that are sharply focused, realistic and helpful for achieving results, steering clear of unproven, idealistic, and impractical recommendations. Pro .NET Best Practices covers a broad range of practices and principles that development experts agree are the right ways to develop software, which includes continuous integration, automated testing, automated deployment, and code analysis. Whether the solution is from a free and open source or a commercial offering, you will learn how to get a continuous integration server running and executing builds every time code changes. You will write clearer and more maintainable automated testing code that focuses on prevention and helping your .NET project succeed. By learning and following the .NET best practices in this book, you will avoid making the same mistakes once. With this book at your side, you'll get: Real-world, no-nonsense approaches to continuous integration, automated testing, automated deployment, and code analysis Tips and tricks you'll need to clear hurdles that keep others from putting these common sense ideas into common practice Guidance from the minimal, essential approach all the way to what's necessary to deliver at the highest levels of quality and effectiveness Benefit immediately, even before finishing it, from the knowledge, workable advice, and experience found in Pro .NET Best Practices.

Client side JavaScript for enterprise Oracle applications. About This Book Develop resilient and robust client-side applications Explore the power of popular JavaScript libraries such as jQuery, RequireJS, and custom Oracle JavaScript libraries Integrate JavaScript for Oracle developers Easily debug and secure your cloud interfaces Who This Book Is For If you are a web components developer looking to create client-side apps that are resilient and robust using Oracle JET, then this book is the right choice for you. What You Will Learn Use Yeoman or npm to start a new Oracle JET-based project Implement real-world use cases using Oracle JET components Get to know the best practices for Oracle JET web applications Explore Knockout.js, the framework behind Oracle JET Implement a multi-platform app with OJ and Cordova In Detail This book will give you a complete practical understanding of the Oracle JavaScript Extension Toolkit (JET) and how you can use it to develop efficient client-side applications with ease. It will tell you how to get your own customized Oracle JET set up. You'll start with individual libraries, such as jQuery, Cordova, and Require.js. You'll also get to work with the JavaScript libraries created by Oracle, especially for cloud developers. You'll use these tools to create a working backend application with these libraries. Using the latest Oracle Alta UI, you'll develop a state-of-the-art backend for your cloud applications. You'll learn how to develop and integrate the different cloud services required for your application and use other third-party libraries to get more features from your cloud applications. Toward the end of the book, you'll learn how to manage and secure your cloud applications, and test them to ensure seamless deployment. Style and approach This book will have a practical step by step approach where every step of application development will be explained in detail with code samples.

Threats to application security continue to evolve just as quickly as the systems that protect against cyber-threats. In many instances, traditional firewalls and other conventional controls can no longer get the job done. The latest line of defense is to build security features into software as it is being developed. Drawing from the author’s extensive experience as a developer, Secure Software Development: Assessing and Managing Security Risks illustrates how software application security can be best, and most cost-effectively, achieved when developers monitor and regulate risks early on, integrating assessment and management into the development life cycle. This book identifies the two primary reasons for inadequate security safeguards: Development teams are not sufficiently trained to identify risks; and developers falsely believe that pre-existing perimeter security controls are adequate to protect newer software. Examining current trends, as well as problems that have plagued software security for more than a decade, this useful guide: Outlines and compares various techniques to assess, identify, and manage security risks and vulnerabilities, with step-by-step instruction on how to execute each approach Explains the fundamental terms related to the security process Elaborates on the pros and cons of each method, phase by phase, to help readers select the one that best suits their needs Despite decades of extraordinary growth in software development, many open-source, government, regulatory, and industry organizations have been slow to adopt new application safety controls, hesitant to take on the added expense. This book improves understanding of the security environment and the need for safety measures. It shows readers how to analyze relevant threats to their applications and then implement time- and money-saving techniques to safeguard them.

Application Security in the ISO 27001:2013 Environment explains how organisations can implement and maintain effective security practices to protect their web applications – and the servers on which they reside – as part of a wider information security management system by following the guidance set out in the international standard for information security management, ISO 27001. The book describes the methods used by criminal hackers to attack organisations via their web applications and provides a detailed explanation of how you can combat such attacks by employing the guidance and controls set out in ISO 27001. Product overviewSecond edition, updated to reflect ISO 27001:2013 as well as best practices relating to cryptography, including the PCI SSC’s denigration of SSL in favour of TLS.Provides a full introduction to ISO 27001 and information security management systems, including implementation guidance.Describes risk assessment, management and treatment approaches.Examines common types of web app security attack, including injection attacks, cross-site scripting, and attacks on authentication and session management, explaining how each can compromise ISO 27001 control objectives and showing how to test for each attack type.Discusses the ISO 27001 controls relevant to application security.Lists useful web app security metrics and their relevance to ISO 27001 controls.Provides a four-step approach to threat profiling, and describes application security review and testing approaches.Sets out guidelines and the ISO 27001 controls relevant to them, covering:input validationauthenticationauthorisationsensitive data handling and the use of TLS rather than SSLsession managementerror handling and loggingDescribes the importance of security as part of the web app development process

Many organizations critically depend on very large information systems. In the authors' experience these organizations often struggle to find the right strategy to sustainably develop their systems. Based on their own experience at a major bank, over more than a decade, the authors have developed a successful strategy to deal with these challenges, including: - A thorough analysis of the challenges associated with very large information systems - An assessment of possible strategies for the development of these systems, resulting in managed evolution as the preferred strategy - Describing key system aspects for the success of managed evolution, such as architecture management, integration architecture and infrastructure - Developing the necessary organizational, cultural, governance and controlling mechanisms for successful execution

This best-selling guide provides a complete, practical, and thoroughly up-to-date introduction to network and computer security. COMPTIA SECURITY+ GUIDE TO NETWORK SECURITY FUNDAMENTALS, Seventh Edition, maps to the new CompTIA Security+ SY0-601 Certification Exam, providing comprehensive coverage of all domain objectives to help readers prepare for professional certification and career success. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

IT securiteers - The human and technical dimension working for the organisation. Current corporate governance regulations and international standards lead many organisations, big and small, to the creation of an information technology (IT) security function in their organisational chart or to the acquisition of services from the IT security industry. More often than desired, these teams are only useful for companies' executives to tick the corresponding box in a certification process, be it ISO, ITIL, PCI, etc. Many IT security teams do not provide business value to their company. They fail to really protect the organisation from the increasing number of threats targeting its information systems. IT Security Management provides an insight into how to create and grow a team of passionate IT security professionals. We will call them "securiteers". They will add value to the business, improving the information security stance of organisations.

Polyolefins, such as polyethylene and polypropylene, are among the most widely used commercial polymers. These versatile fibers are durable, chemically resistant, lightweight, economical, and functional. This book provides researchers in materials, as well as product development specialists in industry and biomedical engineering with a comprehensive resource that will assist them with material improvement and product development. The first chapters discuss the structural and chemical properties of different types of polyolefins, as well as production methods. Other chapters delve into functionality improvement and address how polyolefins can be incorporated into specific industrial, medical, and automotive products.

This book constitutes the thoroughly refereed proceedings of the 6th International Conference on Data Management Technologies and Applications, DATA 2017, held in Madrid, Spain, in July 2017. The 13 revised full papers were carefully reviewed and selected from 66 submissions. The papers deal with the following topics: databases, big data, data mining, data management, data security, and other aspects of information systems and technology involving advanced applications of data.

This book constitutes the refereed proceedings of the Third International Conference on Trust and Privacy in Digital Business, TrustBus 2006, held in Krakow, Poland in September 2006 in conjunction with DEXA 2006. The 24 revised full papers presented were carefully reviewed and selected from 70 submissions. The papers are organized in topical sections on privacy and identity management, security and risk management, security requirements and development, privacy enhancing technologies and privacy management, access control models, trust and reputation, security protocols, and security and privacy in mobile environments.

Application Security Recipes for JAVA/JEE: A Problem-Solution Approach teaches how to build a highly secure and hack-resistant system using JAVA technology. This book provides end-to-end application security secrets and solutions. It provides a simplified and easy to follow approach to implement core security requirements (confidentiality, integrity, availability, authentication, authorization and accountability). When you start a new application development cycle or are working on existing legacy applications for the security aspects of the process, you can use the book as a catalog of 'Security Best Practices'. The book content is organized in such a way that you feel you are working on system security at every phase of a software development life cycle (SDLC) in keeping with business requirements. This book starts its presentation with risk management terminology because without a fundamental understanding of risk you may fail to define a secure system; then the presentation moves towards the following topics in the process: identify and capture security requirements, transform all the identified requirements to a secure design phase, and then validate the design with threat model concepts. Thereafter we give a detailed presentation of the 'Java built-in Security Model', secure coding guidelines for Java, a presentation of various input injection attacks and web attacks, control injection attacks with input sanitization and output encoding, a detailed presentation of web services (SOAP/REST) security, validation and verification of all the security controls with 'white-box' and 'black-box' testing. Then, how to apply cryptosystem best-practices for application development, a presentation of cloud security and Android security, an introduction to the OWASP TOP 10 Risks for 2014 and the OWASP TOP 10 Mobile Risks for 2014 and finally a discussion of Spring framework's built-in security module is explored. The highlights of the book are: * Input injection attacks & Web injection attack * Threat modeling * SOAP and RESTful web services security * OAuth and SAML protocols * Android Security & Cloud Security This book guides you step-by-step through topics using complete and real-world code examples. Instead of theoretical descriptions on complex concepts, you will find live examples in this book. When you start a new project, you can follow the recipes to define end-to-end security aspects of a system.

This book covers the most critical 24 NFRs that are applicable to IT applications and systems. About This Book Explains three stages of nonfunctional requirements, that is, analysis, architecture, and assessment In-depth knowledge of NFR framework and taxonomy that provides guidance around the modelling phase for the NFRs Coverage of 24 critical and pivotal NFRs, including the analysis, architecture, and assessment. Who This Book Is For The primary audience for this title are the gamut of roles starting from IT consultant to chief architects who are responsible to deliver strategic, tactical, and operational engagements for fortune 100 customers worldwide. Nonfunctional requirements are the key to any software / IT program. They cannot be overlooked or ignored. The book provides a comprehensive approach from analysis, architecture, and measurement of nonfunctional requirements. The book includes considerations for bespoke (Java, .Net, and COTS applications). These are applicable to IT applications from various domains. The book outlines the methodology for capturing the NFRs and also describes a framework that can be leveraged by analysts and architects for tackling NFRs for various engagements. The audience for this book include business analysts, enterprise architects, business architects, solution architects, technical architects/designers, domain/security/integration architects, software developers, support engineers and test engineers, technical project managers, project leads/technical leads/technical project managers, and students from the computer science/IT stream What You Will Learn Learn techniques related to the analysis, architecture, and monitoring of NFRs Understand the various tools, techniques, and processes in order to improve the overall quality of the desired outcomes Embrace the best practices of architecting, metrics, and success factors for NFRs Identify the common pitfalls to be avoided and the patterns to leverage Understand taxonomy and framework for NFRs Learn the design guidelines for architecting applications and systems relating to NFRs Abstract different methodologies to analyze and gather NFRs In Detail Non-functional Requirements are key to any software/IT program and cannot be overlooked or ignored. This book provides a comprehensive approach to the analysis, architecture, and measurement of NFRs. It includes considerations for bespoke Java, .NET, and COTS applications that are applicable to IT applications/systems in different domains. The book outlines the methodology for capturing the NFRs and also describes a framework that can be leveraged by analysts and architects for tackling NFRs for various engagements. This book starts off by explaining the various KPIs, taxonomies, and methods for identifying NFRs.

Learn the design guidelines for architecting applications and systems relating to NFRs and design principles to achieve the desired outcome. We will then move on to various key tiers/layers and patterns pertaining to the business, database, and integrating tiers. After this, we will dive deep into the topics pertaining to techniques related to monitoring and measurement of NFRs, such as sizing, analytical modeling, and quality assurance. Lastly, we end the book by describing some pivotal NFRs and checklists for the software quality attributes related to the business, application, data, and infrastructure domains. Style and approach The book takes a pragmatic approach, describing various techniques related to the analysis of NFRs, the architecture of NFRs, and assessment of NFRs.

Although organizations that store, process, or transmit cardholder information are required to comply with payment card industry standards, most find it extremely challenging to comply with and meet the requirements of these technically rigorous standards. PCI Compliance: The Definitive Guide explains the ins and outs of the payment card industry (PCI) security standards in a manner that is easy to understand. This step-by-step guidebook delves into PCI standards from an implementation standpoint. It begins with a basic introduction to PCI compliance, including its history and evolution. It then thoroughly and methodically examines the specific requirements of PCI compliance. PCI requirements are presented along with notes and assessment techniques for auditors and assessors. The text outlines application development and implementation strategies for Payment Application Data Security Standard (PA-DSS) implementation and validation. Explaining the PCI standards from an implementation standpoint, it clarifies the intent of the standards on key issues and challenges that entities must overcome in their quest to meet compliance requirements.

The book goes beyond detailing the requirements of the PCI standards to delve into the multiple implementation strategies available for achieving PCI compliance. The book includes a special appendix on the recently released PCI-DSS v 3.0. It also contains case studies from a variety of industries undergoing compliance, including banking, retail, outsourcing, software development, and processors. Outlining solutions extracted from successful real-world PCI implementations, the book ends with a discussion of PA-DSS standards and validation requirements.

The world is becoming increasingly mobile. Smartphones and tablets have become more powerful and popular, with many of these devices now containing confidential business, financial, and personal information. This has led to a greater focus on mobile software security. Establishing mobile software security should be of primary concern to every mobile application developer. This book explains how you can create mobile social applications that incorporate security throughout the development process. Although there are many books that address security issues, most do not explain how to incorporate security into the building process. Secure Development for Mobile Apps does exactly that. Its step-by-step guidance shows you how to integrate security measures into social apps running on mobile platforms. Youll learn how to design and code apps with security as part of the process and not an afterthought. The author outlines best practices to help you build better, more secure software. This book provides a comprehensive guide to techniques for secure development practices. It covers PHP security practices and tools, project layout templates, PHP and PDO, PHP encryption, and guidelines for secure session management, form validation, and file uploading. The book also demonstrates how to develop secure mobile apps using the APIs for Google Maps, YouTube, jQuery Mobile, Twitter, and Facebook. While this is not a beginners guide to programming, you should have no problem following along if youve spent some time developing with PHP and MySQL.

Servers are frequently targeted by attackers because of the value of their data and services. For example, a server might contain personally identifiable info. that could be used to perform identity theft. This document is intended to assist organizations in installing, configuring, and maintaining secure servers. More specifically, it describes, in detail, the following practices to apply: (1) Securing, installing, and configuring the underlying operating system; (2) Securing, installing, and configuring server software; (3) Maintaining the secure configuration through application of appropriate patches and upgrades, security testing, monitoring of logs, and backups of data and operating system files. Illus.

Cloud Computing: Implementation, Management, and Security provides an understanding of what cloud computing really means, explores how disruptive it may become in the future, and examines its advantages and disadvantages. It gives business executives the knowledge necessary to make informed, educated decisions regarding cloud initiatives. The authors first discuss the evolution of computing from a historical perspective, focusing primarily on advances that led to the development of cloud computing. They then survey some of the critical components that are necessary to make the cloud computing paradigm feasible. They also present various standards based on the use and implementation issues surrounding cloud computing and describe the infrastructure management that is maintained by cloud computing service providers. After addressing significant legal and philosophical issues, the book concludes with a hard look at successful cloud computing vendors. Helping to overcome the lack of understanding currently preventing even faster adoption of cloud computing, this book arms readers with guidance essential to make smart, strategic decisions on cloud initiatives.

Cell phones and Personal Digital Assistants (PDAs) have become indispensable tools for today¿s highly mobile workforce. Small and relatively inexpensive, these devices can be used not only for voice calls, simple text messages, and Personal Information Management (PIM), but also for many functions done at a desktop computer. While these devices provide productivity benefits, they also pose new risks. This document is intended to assist organizations in securing cell phones and PDAs. More specifically, this document describes in detail the threats faced by organizations that employ handheld devices and the measures that can be taken to counter those threats.

This book constitutes the proceedings of the 4th Asia Pacific Requirements Engineering Symposium, APRES 2017, held in Melaka, Malaysia, in November 2017. The 11 full papers presented together with four short papers were carefully reviewed and selected from 45 submissions. The papers are organized in topical sections on big data, cyber security, crowd-sourcing, requirements challenges, automation.