[EPUB] Application Security For The Data Center Fortinet

If you ally dependence such a referred **application security for the data center fortinet** book that will allow you worth, get the categorically best seller from us currently from several preferred authors. If you desire to hilarious books, lots of novels, tale, jokes, and more fictions collections are along with launched, from best seller to one of the most current released.

You may not be perplexed to enjoy every book collections application security for the data center fortinet that we will very offer. It is not almost the costs. Its nearly what you habit currently. This application security for the data center fortinet, as one of the most enthusiastic sellers here will categorically be in the middle of the best options to review.

Data and Application Security-B. Thuraisingham 2006-04-11 New technology is always evolving and companies must have appropriate security for their businesses to be able to keep up to date with the changes. With the rapid growth of the internet and the world wide web, data and applications security will always be a key topic in industry as well as in the public sector, and has implications for the whole of society. Data and Applications Security covers issues related to security and privacy of information in a wide range of applications, including: Electronic Commerce, XML and Web Security; Workflow Security and Role-based Access Control; Distributed Objects and Component Security; Inference Problem, Data Mining and Intrusion Detection; Language and SQL Security; Security Architectures and Frameworks; Federated and Distributed Systems Security; Encryption, Authentication and Security Policies. This book contains papers and panel discussions from the Fourteenth Annual Working Conference on Database Security, which is part of the Database Security: Status and Prospects conference series sponsored by the International Federation for Information Processing (IFIP). The conference was held in Schoorl, The Netherlands in August 2000.

Database and Applications Security-Bhavani Thuraisingham 2005-05-26 This is the first book to provide an in-depth coverage of all the developments, issues and challenges in secure databases and applications. It provides directions for data and application security, including securing emerging applications such as bioinformatics, stream information processing and peer-to-peer computing. Divided into eight sections,

Data and Applications Security XIX-Sushil Jajodia 2005-07-20 This book constitutes the refereed proceedings of the 19th Annual Working Conference on Data and Applications Security held in Storrs, CT, USA, in August 2005. The 24 revised full papers presented together with an invited lecture were thoroughly reviewed and selected from 54 submissions. The papers present theory, technique, applications, and practical experience of data and application security with topics like cryptography, privacy, security planning and administration, secure information integration, secure semantic Web technologies and applications, access control, integrity maintenance, knowledge discovery and privacy, concurrency control, fault-tolerance and recovery methods.

Data and Applications Security and Privacy XXXIII-Simon N. Foley 2019-08-02 This book constitutes the refereed proceedings of the 33rd Annual IFIP WG 11.3 Conference on Data and Applications Security and Privacy, DBSec 2019, held in Charleston, SC, USA, in July 2018. The 21 full papers presented were carefully reviewed and selected from 52 submissions. The papers present high-quality original research from academia, industry, and government on theoretical and practical aspects of information security. They are organized in topical sections on attacks, mobile and Web security, privacy, security protocol practices, distributed systems, source code security, and malware.

Application Security for the Android Platform-Jeff Six 2011-12-01 With the Android platform fast becoming a target of malicious hackers, application security is crucial. This concise book provides the knowledge you need to design and implement robust, rugged, and secure apps for any Android device. You'll learn how to identify and manage the risks inherent in your design, and work to minimize a hacker's opportunity to compromise your app and steal user data. How is the Android platform structured to handle security? What services and tools are available to help you protect data? Up until now, no single resource has provided this vital information. With this guide, you'll learn how to address real threats to your app, whether or not you have previous experience with security issues. Examine Android's architecture and security model, and how it isolates the filesystem and database Learn how to use Android permissions and restricted system APIs Explore Android component types, and learn how to secure communications in a multi-tier app Use cryptographic tools to protect data stored on an Android device Secure the data transmitted from the device to other parties, including the servers that interact with your app

Network and Application Security-Debashis Ganguly 2011-11-11 To deal with security issues effectively, knowledge of theories alone is not sufficient. Practical experience is essential. Helpful for beginners and industry practitioners, this book develops a concrete outlook, providing readers with basic concepts and an awareness of industry standards and best practices. Chapters address cryptography and network security, system-level security, and applications for network security. The book also examines application level attacks, practical software security, and securing application-specific networks. Ganguly Debashis speaks about Network and Application Security

Oracle Database Application Security-Osama Mustafa 2019-10-31 Focus on the security aspects of designing, building, and maintaining a secure Oracle Database application. Starting with data encryption, you will learn to work with transparent data, back-up, and networks. You will then go through the key principles of audits, where you will get to know more about identity preservation, policies and fine-grained audits. Moving on to virtual private databases, you'll set up and configure a VPD to work in concert with other security features in Oracle, followed by tips on managing configuration drift, profiles, and default users. Shifting focus to coding, you will take a look at secure coding standards, multi-schema database models, code-based access control, and SQL injection. Finally, you'll cover single sign-on (SSO), and will be introduced to Oracle Internet Directory (OID), Oracle Access Manager (OAM), and Oracle Identity Management (OIM) by installing and configuring them to meet your needs. Oracle databases hold the majority of the world's relational data, and are attractive targets for attackers seeking high-value targets for data theft. Compromise of a single Oracle Database can result in tens of millions of breached records costing millions in breach-mitigation activity. This book gets you ready to avoid that nightmare scenario. What You Will Learn Work with Oracle Internet Directory using the command-line and the console Integrate Oracle Access Manager with different applications Work with the Oracle Identity Manager console and connectors, while creating your own custom one Troubleshooting issues with OID, OAM, and OID Dive deep into file system and network security concepts Who This Book Is For Oracle DBAs and developers. Readers will need a basic understanding of Oracle RDBMS and Oracle Application Server to take complete advantage of this book.

Alice and Bob Learn Application Security-Tanya Janca 2020-11-10 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.

Cloud Security and Privacy-Tim Mather 2009-09-04 You may regard cloud computing as an ideal way for your company to control IT costs, but do you know how private and secure this service really is? Not many people do. With Cloud Security and Privacy, you'll learn what's at stake when you trust your data to the cloud, and what you can do to keep your virtual infrastructure and web applications secure. Ideal for IT staffers, information security and privacy practitioners, business managers, service providers, and investors alike, this book offers you sound advice from three well-known authorities in the tech security world. You'll learn detailed information on cloud computing security that-until now-has been sorely lacking. Review the current state of data security and storage in the cloud, including confidentiality, integrity, and availability Learn about the identity and access management (IAM) practice for authentication, authorization, and auditing of the users accessing cloud services Discover which security management frameworks and standards are relevant for the cloud Understand the privacy aspects you need to consider in the cloud, including how they compare with traditional computing models Learn the importance of audit and compliance functions within the cloud, and the various standards and frameworks to consider Examine security delivered as a service-a different facet of cloud security

Application of Big Data for National Security-Babak Akhgar 2015-02-19 Application of Big Data for National Security provides users with state-of-the-art concepts, methods, and technologies for Big Data analytics in the fight against terrorism and crime, including a wide range of case studies and application scenarios. This book combines expertise from an international team of experts in law enforcement, national security, and law, as well as computer sciences, criminology, linguistics, and psychology, creating a unique cross-disciplinary collection of knowledge and insights into this increasingly global issue. The strategic frameworks and critical factors presented in Application of Big Data for National Security consider technical, legal, ethical, and societal impacts, but also practical considerations of Big Data system design and deployment, illustrating how data and security concerns intersect. In identifying current and future technical and operational challenges it supports law enforcement and government agencies in their operational, tactical and strategic decisions when employing Big Data for national security Contextualizes the Big Data concept and how it relates to national security and crime detection and prevention Presents strategic approaches for the design, adoption, and deployment of Big Data technologies in preventing terrorism and reducing crime Includes a series of case studies and scenarios to demonstrate the application of Big Data in a national security context Indicates future directions for Big Data as an enabler of advanced crime prevention and detection

Data and Applications Security and Privacy XXVIII-Vijay Atluri 2014-07-24 This book constitutes the refereed proceedings of the 28th IFIP WG 11.3 International Working Conference on Data and Applications Security and Privacy, DBSec 2014, held in Vienna, Austria, in July 2014. The 22 revised full papers and 4 short papers presented were carefully reviewed and selected from 63 submissions. The papers are organized in topical sections on access control, privacy, networked and mobile environments, data access, cloud databases, and private retrieval.

iOS Application Security-David Thiel 2016-02-16 "The most thorough and thoughtful treatment of iOS security that you can find today." —Alex Stamos, Chief Security Officer at Facebook "David Thiel is the most skilled and knowledgeable iOS security researcher that I've worked with. Countless times David has identified iOS platform 'gotchas' and steered us toward more robust security patterns. David's advice for developing secure iOS applications has been indispensable to my organization." —Brandon Sterne, Director of Security Engineering, Workday, Inc. Eliminating security holes in iOS apps is critical for any developer who wants to protect their users from the bad guys. In iOS Application Security, mobile security expert David Thiel reveals common iOS coding mistakes that create serious security problems and shows you how to find and fix them. After a crash course on iOS application structure and Objective-C design patterns, you'll move on to spotting bad code and plugging the holes. You'll learn about: *The iOS security model and the limits of its built-in protections *The myriad ways sensitive data can leak into places it shouldn't, such as through the pasteboard *How to implement encryption with the Keychain, the Data Protection API, and CommonCrypto *Legacy flaws from C that still cause problems in modern iOS applications *Privacy issues related to gathering user data and how to mitigate potential pitfalls Don't let your app's security leak become another headline. Whether you're looking to bolster your app's defenses or hunting bugs in other people's code, iOS Application Security will help you get the job done well.

Developer's Guide to Web Application Security-Michael Cross 2011-04-18 Over 75% of network attacks are targeted at the web application layer. This book provides explicit hacks, tutorials, penetration tests, and step-by-step demonstrations for security professionals and Web application developers to defend their most vulnerable applications. This book defines Web application security, why it should be addressed earlier in the lifecycle in development and quality assurance, and how it differs from other types of Internet security. Additionally, the book examines the procedures and technologies that are essential to developing, penetration testing and releasing a secure Web application. Through a review of recent Web application breaches, the book will expose the prolific methods hackers use to execute Web attacks using common vulnerabilities such as SQL Injection, Cross-Site Scripting and Buffer Overflows in the application layer. By taking an in-depth look at the techniques hackers use to exploit Web applications, readers will be better equipped to protect confidential. The Yankee Group estimates the market for Web application-security products and services will grow to $1.74 billion by 2007 from $140 million in 2002 Author Michael Cross is a highly sought after speaker who regularly delivers Web Application presentations at leading conferences including: Black Hat, TechnoSecurity, CanSec West, Shmoo Con, Information Security, RSA Conferences, and more

Web Application Security-Andrew Hoffman 2020-03-02 While many resources for network and IT security are available, detailed knowledge regarding modern web application security has been lacking—until now. This practical guide provides both offensive and defensive security concepts that software engineers can easily learn and apply. Andrew Hoffman, a senior security engineer at Salesforce, introduces three pillars of web application security: recon, offense, and defense. You'll learn methods for effectively researching and analyzing modern web applications—including those you don't have direct access to. You'll also learn how to break into web applications using the latest hacking techniques. Finally, you'll learn how to develop mitigations for use in your own web applications to protect against hackers. Explore common vulnerabilities plaguing today's web applications Learn essential hacking techniques attackers use to exploit applications Map and document web applications for which you don't have direct access Develop and deploy customized exploits that can bypass common defenses Develop and deploy mitigations to protect your applications against hackers Integrate secure coding best practices into your development lifecycle Get practical tips to help you improve the overall security of your web applications

Android Application Security Essentials-Pragati Ogal Rai 2013-01-01 Android Application Security Essentials is packed with examples, screenshots, illustrations, and real world use cases to secure your apps the right way.If you are looking for guidance and detailed instructions on how to secure app data, then this book is for you. Developers, architects, managers, and technologists who wish to enhance their knowledge of Android security will find this book interesting. Some prior knowledge of development on the Android stack is desirable but not required.

Identity and Data Security for Web Development-Jonathan LeBlanc 2016-06-06 Developers, designers, engineers, and creators can no longer afford to pass responsibility for identity and data security onto others. Web developers who don't understand how to obscure data in transmission, for instance, can open security flaws on a site without realizing it. With this practical guide, you'll learn how and why everyone working on a system needs to ensure that users and data are protected. Authors Jonathan LeBlanc and Tim Messerschmidt provide a deep dive into the concepts, technology, and programming methodologies necessary to build a secure interface for data and identity—without compromising usability. You'll learn how to plug holes in existing systems, protect against viable attack vectors, and work in environments that sometimes are naturally insecure. Understand the state of web and application security today Design security password encryption, and combat password attack vectors Create digital fingerprints to identify users through browser, device, and paired device detection Build secure data transmission systems through OAuth and OpenID Connect Use alternate methods of identification for a second factor of authentication Harden your web applications against attack Create a secure data transmission system using SSL/TLS, and synchronous and asynchronous cryptography

The Manager's Guide to Web Application Security-Ron Lepofsky 2014-12-26 The Manager's Guide to Web Application Security is a concise, information-packed guide to application security risks every organization faces, written in plain language, with guidance on how to deal with those issues quickly and effectively. Often, security vulnerabilities are difficult to understand and quantify because they are the result of intricate programming deficiencies and highly technical issues. Author and noted industry expert Ron Lepofsky breaks down the technical barrier and identifies many real-world examples of security vulnerabilities commonly found by IT security auditors, translates them into business risks with identifiable consequences, and provides practical

guidance about mitigating them. The Manager's Guide to Web Application Security describes how to fix and prevent these vulnerabilities in easy-to-understand discussions of vulnerability classes and their remediation. For easy reference, the information is also presented schematically in Excel spreadsheets available to readers for free download from the publisher’s digital annex. The book is current, concise, and to the point—which is to help managers cut through the technical jargon and make the business decisions required to find, fix, and prevent serious vulnerabilities.

Big Data Analytics: Systems, Algorithms, Applications-C.S.R. Prabhu 2019-10-14 This book provides a comprehensive survey of techniques, technologies and applications of Big Data and its analysis. The Big Data phenomenon is increasingly impacting all sectors of business and industry, producing an emerging new information ecosystem. On the applications front, the book offers detailed descriptions of various application areas for Big Data Analytics in the important domains of Social Semantic Web Mining, Banking and Financial Services, Capital Markets, Insurance, Advertisement, Recommendation Systems, Bio-Informatics, the IoT and Fog Computing, before delving into issues of security and privacy. With regard to machine learning techniques, the book presents all the standard algorithms for learning – including supervised, semi-supervised and unsupervised techniques such as clustering and reinforcement learning techniques to perform collective Deep Learning. Multi-layered and nonlinear learning for Big Data are also covered. In turn, the book highlights real-life case studies on successful implementations of Big Data Analytics at large IT companies such as Google, Facebook, LinkedIn and Microsoft. Multi-sectorial case studies on domain-based companies such as Deutsche Bank, the power provider Opower, Delta Airlines and a Chinese City Transportation application represent a valuable addition. Given its comprehensive coverage of Big Data Analytics, the book offers a unique resource for undergraduate and graduate students, researchers, educators and IT professionals alike.

Information Technology. Security Techniques. Application Security. Protocols and Application Security Controls Data Structure-British Standards Institute Staff 1917-10-24 Information systems, Organizations, Data processing, Computer networks, Data storage protection, Data security, Computer applications, Computer technology, Computers, Management

Advances in Security in Computing and Communications-Jaydip Sen 2017-07-19 In the era of Internet of Things (IoT) and with the explosive worldwide growth of electronic data volume, and associated need of processing, analysis, and storage of such humongous volume of data, several new challenges are faced in protecting privacy of sensitive data and securing systems by designing novel schemes for secure authentication, integrity protection, encryption, and non-repudiation. Lightweight symmetric key cryptography and adaptive network security algorithms are in demand for mitigating these challenges. This book presents some of the state-of-the-art research work in the field of cryptography and security in computing and communications. It is a valuable source of knowledge for researchers, engineers, practitioners, graduates, and doctoral students who are working in the field of cryptography, network security, and security and privacy issues in the Internet of Things (IoT). It will also be useful for faculty members of graduate schools and universities.

Web Application Security-Ibrahim Haji 2014-10-09 Essay from the year 2011 in the subject Information Management, grade: B, The University of Chicago, language: English, abstract: As the world continues to enjoy the reliability of web-based applications, security of such applications is becoming an increasingly vital concern. Currently, virtually all sectors are implementing some form of internet-based programs. The World Wide Web has significantly led to desirable expansion in business, healthcare, government and social services (Lee, Shieh & Tygar, 2005, p.184). However, the number of internet attacks has equally increased in the recent past. Hackers have become more adept in writing malicious codes to counter the conventional software codes developed by software vendors. The emergence of various types of vulnerabilities and generation of malicious codes on the internet platform has affected service provision in many sectors. The healthcare field is a particularly sensitive area where privacy and confidentiality of information are immensely important. Storage, transmission and implementation of health-related data and information are some of the processes which require secure online platforms. As such, it is very important to provide security in web applications used in the health sector. This paper explores the impacts of web application security in e-health. Provision of integral healthcare in the modern medical profession has taken a new direction with regards to storage of clinical data and patients' records (Chryssanthou & Apostolakis & Varlamis, 2010, p.3). In order to achieve a shared healthcare paradigm, implementation of web-based applications has become inevitable. Electronic health records (EHRs) have become a common buzzword in healthcare issues and facilities. The advent of EHRs has reliably replaced paperwork in medical informatics (Chryssanthou & Apostolakis & Varlamis, 2010, p.3). The EHR can be designed as an online-hosted platform in which medical information, patients' health records and clini

Android Application Security-Mu Zhang 2016-11-16 This SpringerBrief explains the emerging cyber threats that undermine Android application security. It further explores the opportunity to leverage the cutting-edge semantics and context–aware techniques to defend against such threats, including zero-day Android malware, deep software vulnerabilities, privacy breach and insufficient security warnings in app descriptions. The authors begin by introducing the background of the field, explaining the general operating system, programming features, and security mechanisms. The authors capture the semantic-level behavior of mobile applications and use it to reliably detect malware variants and zero-day malware. Next, they propose an automatic patch generation technique to detect and block dangerous information flow. A bytecode rewriting technique is used to confine privacy leakage. User-awareness, a key factor of security risks, is addressed by automatically translating security-related program semantics into natural language descriptions. Frequent behavior mining is used to discover and compress common semantics. As a result, the produced descriptions are security-sensitive, human-understandable and concise.By covering the background, current threats, and future work in this field, the brief is suitable for both professionals in industry and advanced-level students working in mobile security and applications. It is valuable for researchers, as well.

Security for Web Developers-John Paul Mueller 2015-11-10 As a web developer, you may not want to spend time making your web app secure, but it definitely comes with the territory. This practical guide provides you with the latest information on how to thwart security threats at several levels, including new areas such as microservices. You’ll learn how to help protect your app no matter where it runs, from the latest smartphone to an older desktop, and everything in between. Author John Paul Mueller delivers specific advice as well as several security programming examples for developers with a good knowledge of CSS3, HTML5, and JavaScript. In five separate sections, this book shows you how to protect against viruses, DDoS attacks, security breaches, and other nasty intrusions. Create a security plan for your organization that takes the latest devices and user needs into account Develop secure interfaces, and safely incorporate third-party code from libraries, APIs, and microservices Use sandboxing techniques, in-house and third-party testing techniques, and learn to think like a hacker Implement a maintenance cycle by determining when and how to update your application software Learn techniques for efficiently tracking security threats as well as training requirements that your organization can use

Android Apps Security-Sheran Gunasekera 2012-12-03 Android Apps Security provides guiding principles for how to best design and develop Android apps with security in mind. It explores concepts that can be used to secure apps and how developers can use and incorporate these security features into their apps. This book will provide developers with the information they need to design useful, high-performing, and secure apps that expose end-users to as little risk as possible. Overview of Android OS versions, features, architecture and security. Detailed examination of areas where attacks on applications can take place and what controls should be implemented to protect private user data In-depth guide to data encryption, authentication techniques, enterprise security and applied real-world examples of these concepts

LSC (GLOBE UNIVERSITY) SD256: VS ePub for Mobile Application Security-Himanshu Dwivedi 2010-02-18 Secure today's mobile devices and applications Implement a systematic approach to security in your mobile application development with help from this practical guide. Featuring case studies, code examples, and best practices, Mobile Application Security details how to protect against vulnerabilities in the latest smartphone and PDA platforms. Maximize isolation, lockdown internal and removable storage, work with sandboxing and signing, and encrypt sensitive user information. Safeguards against viruses, worms, malware, and buffer overflow exploits are also covered in this comprehensive resource. Design highly isolated, secure, and authenticated mobile applications Use the Google Android emulator, debugger, and third-party security tools Configure Apple iPhone APIs to prevent overflow and SQL injection attacks Employ private and public key cryptography on Windows Mobile devices Enforce fine-grained security policies using the BlackBerry Enterprise Server Plug holes in Java Mobile Edition, SymbianOS, and WebOS applications Test for XSS, CSRF, HTTP redirects, and phishing attacks on WAP/Mobile HTML applications Identify and eliminate threats from Bluetooth, SMS, and GPS services Himanshu Dwivedi is a co-founder of iSEC Partners (www.isecpartners.com), an information security firm specializing in application security. Chris Clark is a principal security consultant with iSEC Partners. David Thiel is a principal security consultant with iSEC Partners.

Network Security Assessment-Chris McNab 2004-03-19 There are hundreds--if not thousands--of techniques used to compromise both Windows and Unix-based systems. Malicious code and new exploit scripts are released on a daily basis, and each evolution becomes more and more sophisticated. Keeping up with the myriad of systems used by hackers in the wild is a formidable task, and scrambling to patch each potential vulnerability or address each new attack one-by-one is a bit like emptying the Atlantic with paper cup.If you're a network administrator, the pressure is on you to defend your systems from attack. But short of devoting your life to becoming a security expert, what can you do to ensure the safety of your mission critical systems? Where do you start?Using the steps laid out by professional security analysts and consultants to identify and assess risks, Network Security Assessment offers an efficient testing model that an administrator can adopt, refine, and reuse to create proactive defensive strategies to protect their systems from the threats that are out there, as well as those still being developed.This thorough and insightful guide covers offensive technologies by grouping and analyzing them at a higher level--from both an offensive and defensive standpoint--helping administrators design and deploy networks that are immune to offensive exploits, tools, and scripts. Network administrators who need to develop and implement a security assessment program will find everything they're looking for--a proven, expert-tested methodology on which to base their own comprehensive program--in this time-saving new book.

Data Hiding Fundamentals and Applications-Husrev T. Sencar 2004-09-09 Multimedia technologies are becoming more sophisticated, enabling the Internet to accommodate a rapidly growing audience with a full range of services and efficient delivery methods. Although the Internet now puts communication, education, commerce and socialization at our finger tips, its rapid growth has raised some weighty security concerns with respect to multimedia content. The owners of this content face enormous challenges in safeguarding their intellectual property, while still exploiting the Internet as an important resource for commerce. Data Hiding Fundamentals and Applications focuses on the theory and state-of-the-art applications of content security and data hiding in digital multimedia. One of the pillars of content security solutions is the imperceptible insertion of information into multimedia data for security purposes; the idea is that this inserted information will allow detection of unauthorized usage. Provides a theoretical framework for data hiding, in a signal processing context Realistic applications in secure, multimedia delivery Compression robust data hiding Data hiding for proof of ownership--WATERMARKING Data hiding algorithms for image and video watermarking

Professional Cocoa Application Security-Graham J. Lee 2010-05-13

Securing Ajax Applications-Christopher Wells 2007-07-11 Ajax applications should be open yet secure. Far too often security is added as an afterthought. Potential flaws need to be identified and addressed right away. This book explores Ajax and web application security with an eye for dangerous gaps and offers ways that you can plug them before they become a problem. By making security part of the process from the start, you will learn how to build secure Ajax applications and discover how to respond quickly when attacks occur. Securing Ajax Applications succinctly explains that the same back-and-forth communications that make Ajax so responsive also gives invaders new opportunities to gather data, make creative new requests of your server, and interfere with the communications between you and your customers. This book presents basic security techniques and examines vulnerabilities with JavaScript, XML, JSON, Flash, and other technologies -- vital information that will ultimately save you time and money. Topics include: An overview of the evolving web platform, including APIs, feeds, web services and asynchronous messaging Web security basics, including common vulnerabilities, common cures, state management and session management How to secure web technologies, such as Ajax, JavaScript, Java applets, Active X controls, plug-ins, Flash and Flex How to protect your server, including front-line defense, dealing with application servers, PHP and scripting Vulnerabilities among web standards such as HTTP, XML, JSON, RSS, ATOM, REST, and XDOS How to secure web services, build secure APIs, and make open mashups secure Securing Ajax Applications takes on the challenges created by this new generation of web development, and demonstrates why web security isn't just for administrators and back-end programmers any more. It's also for web developers who accept the responsibility that comes with using the new wonders of the Web.

Research Directions in Data and Applications Security XVIII-Csilla Farkas 2006-04-11 As Information Technology becomes a vital part of our everyday activities, ranging from personal use to government and defense applications, the need to develop high-assurance systems increases. Data and applications security and privacy are crucial elements in developing such systems. Research Directions in Data and Applications Security XVIII presents original unpublished research results, practical experiences, and innovative ideas in the field of data and applications security and privacy. Topics presented in this volume include: -Database theory; -Inference control; -Data protection techniques; -Distributed systems; -Access control models; -Security policy; -Design and management; -Privacy; -Network security. This book is the eighteenth volume in the series produced by the International Federation for Information Processing (IFIP) Working Group 11.3 on Data and Applications Security. It contains twenty-three papers and two invited talks that were presented at the Eighteenth Annual IFIP WG 11.3 Conference on Data and Applications Security, which was sponsored by IFIP and held in Sitges, Catalonia, Spain in July 2004. Research Directions in Data and Applications Security XVIII is a high-quality reference volume that addresses several aspects of information protection, and is aimed at researchers, educators, students, and developers.

Web Application Security-Carlos Serrao 2010-10-19 IBWAS 2009, the Iberic Conference on Web Applications Security, was the first international conference organized by both the OWASP Portuguese and Spanish ch- ters in order to join the international Web application security academic and industry communities to present and discuss the major aspects of Web applications security. There is currently a change in the information systems development paradigm. The emergence of Web 2. 0 technologies led to the extensive deployment and use of W-based applications and Web services as a way to develop new and flexible information systems. Such systems are easy to develop, deploy and maintain and they demonstrate impressive features for users, resulting in their current wide use. The “social” features of these technologies create the necessary “massification” effects that make millions of users share their own personal information and content over large web-based int- active platforms. Corporations, businesses and governments all over the world are also developing and deploying more and more applications to interact with their bu- nesses, customers, suppliers and citizens to enable stronger and tighter relations with all of them. Moreover, legacy non-Web systems are being ported to this new intrin- cally connected environment. IBWAS 2009 brought together application security experts, researchers, educators and practitioners from industry, academia and international communities such as OWASP, in order to discuss open problems and new solutions in application security. In the context of this track, academic researchers were able to combine interesting results with the experience of practitioners and software engineers.

Security and Privacy for Big Data, Cloud Computing and Applications-Wei Ren 2019-09 This book examines various topics and approaches related to the security and privacy in big data and cloud computing, where authors share their expertise in their respective chapters on a broad range of security and privacy challenges and state of the art solutions.

Cryptography for Internet and Database Applications-Nick Galbreath 2003-02-03

Application security in the ISO27001:2013 Environment-Vinod Vasudevan 2015-10-15 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

CODASPY 16 6th ACM Conference on Data and Application Security and Privacy-CODASPY 16 Conference Committee 2016-07-18

Web Application Security is a Stack-Lori Mac Vittie 2015-02-17 This book is intended for application developers, system administrators and operators, as well as networking professionals who need a comprehensive top-level view of web application security in order to better defend and protect both the ‘web’ and the ‘application’ against potential attacks. This book examines the most common, fundamental attack vectors and shows readers the defence techniques used to combat them.

Advances in Data Science, Cyber Security and IT Applications-Auhood Alfaries 2019-12-21 This book constitutes the refereed proceedings of the First International Conference on Intelligent Cloud Computing, ICC 2019, held in Riyadh, Saudi Arabia, in December 2019. The two-volume set presents 53 full papers, which were carefully reviewed and selected from 174 submissions. The papers are organized in topical sections on Cyber Security; Data Science; Information Technology and Applications; Network and IoT.

Information Technology. Application Security. Application Security Management Process-British Standards Institute Staff 1918-05-29 Data security, Data processing, Computer technology, Computer applications, Computer networks, Data storage protection, Security, Management

Application of Big Data for National Security-Babak Akhgar 2015-02-17 Application of Big Data for National Security provides users with state-of-the-art concepts, methods, and technologies for Big Data analytics in the fight against terrorism and crime, including a wide range of case studies and application scenarios. This book combines expertise from an international team of experts in law enforcement, national security, and law, as well as computer sciences, criminology, linguistics, and psychology, creating a unique cross-disciplinary collection of knowledge and insights into this increasingly global issue. The strategic frameworks and critical factors presented in Application of Big Data for National Security consider technical, legal, ethical, and societal impacts, but also practical considerations of Big Data system design and deployment, illustrating how data and security concerns intersect. In identifying current and future technical and operational challenges it supports law enforcement and government agencies in their operational, tactical and strategic decisions when employing Big Data for national security Contextualizes the Big Data concept and how it relates to national security and crime detection and prevention Presents strategic approaches for the design, adoption, and deployment of Big Data technologies in preventing terrorism and reducing crime Includes a series of case studies and scenarios to demonstrate the application of Big Data in a national security context Indicates future directions for Big Data as an enabler of advanced crime prevention and detection

Information Security and Ethics: Concepts, Methodologies, Tools, and Applications-Nemati, Hamid 2007-09-30 Presents theories and models associated with information privacy and safeguard practices to help anchor and guide the development of technologies, standards, and best practices. Provides recent, comprehensive coverage of all issues related to information security and ethics, as well as the opportunities, future challenges, and emerging trends related to this subject.