# Detection And Prevention Of Sql Injection Attacks

This two volume set LNCS 7016 and LNCS 7017 constitutes the refereed proceedings of the 11th International Conference on Algorithms and Architectures for Parallel Processing, ICA3PP 2011, held in Melbourne, Australia, in October 2011. The second volume includes 37 papers from one symposium and three workshops held together with ICA3PP 2011 main conference. These are 16 papers from the 2011 International Symposium on Advances of Distributed Computing and Networking (ADCN 2011), 10 papers of the 4th IEEE International Workshop on Internet and Distributed Computing Systems (IDCS 2011), 7 papers belonging to the III International Workshop on Multicore and Multithreaded Architectures and Algorithms (M2A2 2011), as well as 4 papers of the 1st IEEE International Workshop on Parallel Architectures for Bioinformatics Systems (HardBio 2011).

"Creating channels with application programming interfaces"--Cover.

This book presents the proceedings of the 5th International Conference on Advanced Intelligent Systems and Informatics 2019 (AISI2019), which took place in Cairo, Egypt, from October 26 to 28,

2019. This international and interdisciplinary conference, which highlighted essential research and developments in the fields of informatics and intelligent systems, was organized by the Scientific Research Group in Egypt (SRGE). The book is divided into several sections, covering the following topics: machine learning and applications, swarm optimization and applications, robotic and control systems, sentiment analysis, e-learning and social media education, machine and deep learning algorithms, recognition and image processing, intelligent systems and applications, mobile computing and networking, cyber-physical systems and security, smart grids and renewable energy, and micro-grid and power systems.

Provides modern enterprises with the tools to create a robust digital platform utilizing proven best practices, practical models, and time-tested techniques Contemporary business organizations can either embrace the digital revolution or be left behind. Enterprise Content and Search Management for Building Digital Platforms provides modern enterprises with the necessary tools to create a robust digital platform utilizing proven best practices, practical models, and time-tested techniques to compete in today's digital world. Features include: Comprehensive discussions on content strategy, content key performance indicators (KPIs), mobile-¬first strategy, content assessment models,

various practical techniques and methodologies successfully used in real-world digital programs, relevant case studies, and more. Initial chapters cover core concepts of a content management system (CMS), including content strategy, CMS architecture, templates, work flow, reference architectures, information architecture, taxonomy, and content metadata. Advanced CMS topics are then covered with chapters on integration, content standards, digital asset management (DAM), document management, content migration, evaluation, validation, maintenance, analytics, search engine optimization (SEO), security, infrastructure, and performance. The basics of enterprise search technologies are explored next, including enterprise search features, advanced search methods, and other enterprise search concepts. An accompanying book support website provides additional material such as various content templates, checklists, and content case studies; along with an illuminating end-to-end digital program case study. Enterprise Content and Search Management for Building Digital Platforms: Offers a comprehensive guide to understanding and learning new methodologies, techniques, and models for the creation of an end-to-end digital system Addresses a wide variety of proven best practices, reference architecture, and deployed techniques in content management and enterprise search space which can

be readily used for digital programs Covers the latest digital trends such as mobile-first strategy, responsive design, adaptive content design, micro services architecture, and semantic search; and also utilizes sample reference architecture for implementing solutions Features numerous case studies to enhance comprehension, including a complete end-to-end digital program case study Provides readily usable content management checklists and reusable templates for defining content strategy, CMS evaluation, search evaluation, and DAM evaluation that can be found on the book support website Comprehensive and cutting-edge, this book is an invaluable reference resource for creating an optimal enterprise digital eco-system to meet the challenges of today's hyper-connected world.

The two-volume set CCIS 827 and 828 constitutes the thoroughly refereed proceedings of the Third International Conference on Next Generation Computing Technologies, NGCT 2017, held in Dehradun, India, in October 2017. The 135 full papers presented were carefully reviewed and selected from 948 submissions. There were organized in topical sections named: Smart and Innovative Trends in Communication Protocols and Standards; Smart and Innovative Trends in Computational Intelligence and Data Science; Smart and Innovative Trends in Image Processing and

Machine Vision; Smart Innovative Trends in Natural Language Processing for Indian Languages; Smart Innovative Trends in Security and Privacy.

Web sites are dynamic, static, and most of the time a combination of both. Web sites needs to protect their databases to assure security. An SQL injection attacks interactive web applications that provide database services. These applications take user inputs and use them to create an SQL query at run time. In an SQL injection attack, an attacker might insert a malicious crafted SQL query as input to perform an unauthorized database operation. Using SQL injection attacks, an attacker can retrieve, modify or can delete confidential sensitive information from the database. It may jeopardize the confidentiality, trust and security of Web sites which totally depends on databases. This report presents a "code reengineering" that implicitly protects the web applications from SQL injection attacks. It uses an original approach that combines static as well as dynamic analysis. In this report, I mentioned an automated technique for moving out SQL injection vulnerabilities from Java code by converting plain text inputs received from users into prepared statements.

This two volume set LNCS 10602 and LNCS 10603 constitutes the thoroughly refereed post-conference proceedings of the Third International Conference on Cloud Computing and Security, ICCCS 2017, held in

Nanjing, China, in June 2017. The 116 full papers and 11 short papers of these volumes were carefully reviewed and selected from 391 submissions. The papers are organized in topical sections such as: information hiding; cloud computing; IOT applications; information security; multimedia applications; optimization and classification.

This book captures the state of the art research in the area of malicious code detection, prevention and mitigation. It contains cutting-edge behavior-based techniques to analyze and detect obfuscated malware. The book analyzes current trends in malware activity online, including botnets and malicious code for profit, and it proposes effective models for detection and prevention of attacks using. Furthermore, the book introduces novel techniques for creating services that protect their own integrity and safety, plus the data they manage.

A lot of research has gone into eliminating SQL Injection attacks over the past decade and yet it is one of the most prevalent web based attacked harming commerce as well as privacy today. This is a clear indicator that we need to look deeper than just the network and application layer to consolidate security recommendations and practices into the core of any application - its data layer.

This Short Cut introduces you to how SQL injection vulnerabilities work, what makes applications vulnerable, and how to protect them. It helps you find your vulnerabilities with analysis and testing tools and describes simple approaches for fixing them in the most popular web-programming languages. This Short Cut also helps you protect your live applications by describing how to monitor for and block attacks before your data is stolen. Hacking is an increasingly

criminal enterprise, and web applications are an attractive path to identity theft. If the applications you build, manage, or guard are a path to sensitive data, you must protect your applications and their users from this growing threat. Supplying a comprehensive introduction to next-generation networks, Building Next-Generation Converged Networks: Theory and Practice strikes a balance between how and why things work and how to make them work. It compiles recent advancements along with basic issues from the wide range of fields related to next generation networks. Containing the co These proceedings represent the work of researchers participating in the 15th European Conference on Cyber Warfare and Security (ECCWS 2016) which is being hosted this year by the Universitat der Bundeswehr, Munich, Germany on the 7-8 July 2016. ECCWS is a recognised event on the International research conferences calendar and provides a valuable plat-form for individuals to present their research findings, display their work in progress and discuss conceptual and empirical advances in the area of Cyberwar and Cyber Security. It provides an important opportunity for researchers and managers to come together with peers to share their experiences of using the varied and ex-panding range of Cyberwar and Cyber Security research available to them. With an initial submission of 110 abstracts, after the double blind, peer review process there are 37 Academic research papers and 11 PhD research papers, 1 Master's research paper, 2 Work In Progress papers and 2 non-academic papers published in these Conference Proceedings. These papers come from many different countries including Austria, Belgium, Canada, Czech Republic, Finland, France, Germany, Greece, Hungary, Ireland, Kenya, Luxembourg, Netherlands, Norway, Portugal, Romania, Russia, Slovenia, South Africa, Sweden, Turkey, UK and USA. This is not only highlighting the international character

of the conference, but is also promising very interesting discussions based on the broad treasure trove of experience of our community and partici-pants."

This volume contains 73 papers presented at CSI 2014: Emerging ICT for Bridging the Future: Proceedings of the 49th Annual Convention of Computer Society of India. The convention was held during 12-14, December, 2014 at Hyderabad, Telangana, India. This volume contains papers mainly focused on Fuzzy Systems, Image Processing, Software Engineering, Cyber Security and Digital Forensic, E-Commerce, Big Data, Cloud Computing and ICT applications.

This book constitutes the refereed proceedings of the 6th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, DIMVA 2009, held in Milan, Italy, in July 2009. The 10 revised full papers presented together with three extended abstracts were carefully selected from 44 initial submissions. The papers are organized in topical sections on malware and SPAM, emulation-based detection, software diversity, harnessing context, and anomaly detection.

This volume constitutes the refereed proceedings of the 4th International Conference on Information Systems, Technology and Management, ICISTM 2010, held in Bangkok, Thailand, in March 2010. The 28 revised full papers presented together with 3 keynote lectures, 9 short papers, and 2 tutorial papers were carefully reviewed and selected from 86 submissions. The papers are organized in topical sections on information systems, information technology, information management, and applications.

This book discusses reliability applications for power systems, renewable energy and smart grids and

highlights trends in reliable communication, fault-tolerant systems, VLSI system design and embedded systems. Further, it includes chapters on software reliability and other computer engineering and software management-related disciplines, and also examines areas such as big data analytics and ubiquitous computing. Outlining novel, innovative concepts in applied areas of reliability in electrical, electronics and computer engineering disciplines, it is a valuable resource for researchers and practitioners of reliability theory in circuit-based engineering domains.

Web applications have become increasingly popular in recent years. They are widely used in security-critical areas, such as financial, medical, and military systems. Meanwhile, the number and sophistication of attacks against web applications have increased rapidly. It is important for organizations and companies to add security functions to existing web application servers in order to maintain the confidentiality of critical information. One common approach to protect web systems is to build an Intrusion Detection and Prevention System (IDPS). In this thesis, we propose an IDPS framework to detect and prevent web attacks by employing Aspect-Oriented Programming (AOP) and Autonomic Computing (AC) technologies. This framework can also be used to discover whether a web application under protection has abilities to prevent certain web attacks itself. We developed a prototyping tool to implement the functionality of this framework partially. We evaluated this tool on two Java web applications to detect and prevent Cross Scripting Site (XSS) and Structured Query

Language (SQL) Injection, which are two of the most common web attacks. The experimental results show that the prototyping tool based on AOP and AC technologies can be applied to detect and prevent the two common web attacks effectively.

This book constitutes the refereed proceedings of the 5th International Conference on Information Processing, ICIP 2011, held in Bangalore, India, in August 2011. The 86 revised full papers presented were carefully reviewed and selected from 514 submissions. The papers are organized in topical sections on data mining; Web mining; artificial intelligence; soft computing; software engineering; computer communication networks; wireless networks; distributed systems and storage networks; signal processing; image processing and pattern recognition.

Basics of SQL Injection Analysis, Detection and PreventionWeb SecurityLAP Lambert Academic Publishing

This all new book covering the brand new Snort version 2.6 from members of the Snort developers team. This fully integrated book and Web toolkit covers everything from packet inspection to optimizing Snort for speed to using the most advanced features of Snort to defend even the largest and most congested enterprise networks. Leading Snort experts Brian Caswell, Andrew Baker, and Jay Beale analyze traffic from real attacks to demonstrate the best practices for implementing the most powerful Snort features. The book will begin with a discussion of packet inspection and the progression from intrusion detection to intrusion prevention. The authors

provide examples of packet inspection methods including: protocol standards compliance, protocol anomaly detection, application control, and signature matching. In addition, application-level vulnerabilities including Binary Code in HTTP headers, HTTP/HTTPS Tunneling, URL Directory Traversal, Cross-Site Scripting, and SQL Injection will also be analyzed. Next, a brief chapter on installing and configuring Snort will highlight various methods for fine tuning your installation to optimize Snort performance including hardware/OS selection, finding and eliminating bottlenecks, and benchmarking and testing your deployment. A special chapter also details how to use Barnyard to improve the overall performance of Snort. Next, best practices will be presented allowing readers to enhance the performance of Snort for even the largest and most complex networks. The next chapter reveals the inner workings of Snort by analyzing the source code. The next several chapters will detail how to write, modify, and fine-tune basic to advanced rules and pre-processors. Detailed analysis of real packet captures will be provided both in the book and the companion material. Several examples for optimizing output plugins will then be discussed including a comparison of MySQL and PostrgreSQL. Best practices for monitoring Snort sensors and analyzing intrusion data follow with examples of real world attacks using: ACID, BASE, SGUIL, SnortSnarf, Snort_stat.pl, Swatch, and more. The last part of the book contains several chapters on active response, intrusion prevention, and using Snort's most advanced capabilities for everything from forensics and incident

handling to building and analyzing honey pots. This fully integrated book and Web toolkit covers everything all in one convenient package It is authored by members of the Snort team and it is packed full of their experience and expertise Includes full coverage of the brand new Snort version 2.6, packed full of all the latest information This book presents high-quality papers from the Third International Conference on Smart Computing and Informatics (SCI 2018?19), organized by the School of Computer Engineering and School of Computer Application, Kalinga Institute of Industrial Technology Deemed to be University, Bhubaneswar, from 21 to 22 December 2018. It includes advanced and multi-disciplinary research on the design of smart computing and informatics, focusing on innovation paradigms in system knowledge, intelligence and sustainability that have the potential to provide realistic solutions to various problems in society, the environment and industry. The papers featured provide a valuable contribution to the deployment of emerging computational and knowledge transfer approaches, optimizing solutions in varied disciplines of science, technology and health care.

This book includes high-quality, peer-reviewed papers from the International Conference on Recent Advancement in Computer, Communication and Computational Sciences (RACCCS-2018), held at Aryabhatta College of Engineering & Research Center, Ajmer, India on August 10–11, 2018, presenting the latest developments and technical solutions in computational sciences. Networking and communication are the backbone of data science, data- and knowledge engineering, which have a wide scope for implementation in engineering sciences. This book offers insights that reflect the

advances in these fields from upcoming researchers and leading academicians across the globe. Covering a variety of topics, such as intelligent hardware and software design, advanced communications, intelligent computing technologies, advanced software engineering, the web and informatics, and intelligent image processing, it helps those in the computer industry and academia use the advances in next-generation communication and computational technology to shape real-world applications.

In today's world, SQL Injection is a serious security threat over the Internet for the various dynamic web applications residing over the internet. These Web applications conduct many vital processes in various web-based businesses. As the use of internet for various online services is rising, so is the security threats present in the web increasing. There is a universal need present for all dynamic web applications and this universal need is the need to store, retrieve or manipulate information from a database. Most of systems which manage the databases and its requirements such as MySQL Server and PostgreSQL use SQL as their language. Flexibility of SQL makes it a powerful language. It allows its users to ask what he/she wants without leaking any information about how the data will be fetched. However the vast use of SQL based databases has made it the center of attention of hackers. They take advantage of the poorly coded Web applications to attack the databases. They introduce an apparent SQL query, through an unauthorized user input, into the legitimate query statement. In this paper, we have tried to present a comprehensive review of all the different types of SQL injection attacks present, as well as detection of such attacks and preventive measure used. We have highlighted their individual strengths and weaknesses. Such a classification would help other researchers to choose the right technique for further studies.

This book constitutes the refereed proceedings of the 14th International Conference on Advanced Data Mining and Applications, ADMA 2018, held in Nanjing, China in November 2018. The 23 full and 22 short papers presented in this volume were carefully reviewed and selected from 104 submissions. The papers were organized in topical sections named: Data Mining Foundations; Big Data; Text and Multimedia Mining; Miscellaneous Topics.

Injection attacks top the list of Open Web Application Security Project's Top 10 Application Security Risks almost every year. SQL Injection is one such attack that presents the adversaries an opportunity to access Personally Identifiable Information (PII) and commit identity theft, putting breach victims at risk. Any data that could potentially be utilized to identify a particular person could be classified as PII. Passport number, social security number, bank account number, driver's license number, and email address are all good examples of PII. Intrusion detection and prevention system is a system or software application that continuously monitors a network for possible malicious activity or policy violations. The alerts and logs generated are typically reviewed by the administrator or SIEM. A signature-based IDS relies on predefined signatures to detect an attack. The signatures used are usually released periodically by the company who owns the IDS software or by the admin herself. Writing these signatures manually or waiting on the releases of new rules can take up significant time, effort and knowledge. In this thesis, a system is developed that monitors traffic in real time, performs deep packet inspection on each incoming packet and looks for possible SQLI patterns to form rules in Snort (IDS) database. Once the system finds a possible SQLI pattern, it saves the attacker's IP to a blacklist for the admin to review later. If the attacker continues to pass such attack patterns, the IP is blacklisted and the access to

that specific user is blocked. Our proposed system, ScorPi increases the baseline intrusion detection performance by 4.7x, with only 23% of the resources required by the baseline, while performing in the order of a few milliseconds, suitable for real-time edge networks.

This book is an introduction and deep-dive into the many uses of dynamic SQL in Microsoft SQL Server. Dynamic SQL is key to large-scale searching based upon user-entered criteria. It's also useful in generating value-lists, in dynamic pivoting of data for business intelligence reporting, and for customizing database objects and querying their structure. Executing dynamic SQL is at the heart of applications such as business intelligence dashboards that need to be fluid and respond instantly to changing user needs as those users explore their data and view the results. Yet dynamic SQL is feared by many due to concerns over SQL injection attacks. Reading Dynamic SQL: Applications, Performance, and Security is your opportunity to learn and master an often misunderstood feature, including security and SQL injection. All aspects of security relevant to dynamic SQL are discussed in this book. You will learn many ways to save time and develop code more efficiently, and you will practice directly with security scenarios that threaten companies around the world every day. Dynamic SQL: Applications, Performance, and Security helps you bring the productivity and user-satisfaction of flexible and responsive applications to your organization safely and securely. Your organization's increased ability to respond to rapidly changing business scenarios will build competitive advantage in an increasingly crowded and competitive global marketplace. Discusses many applications of dynamic SQL, both simple and complex. Explains each example with demos that can be run at home and on your laptop. Helps you to identify when dynamic SQL can offer superior performance. Pays attention to security and

best practices to ensure safety of your data. What You Will Learn Build flexible applications that respond fast to changing business needs. Take advantage of unconventional but productive uses of dynamic SQL. Protect your data from attack through best-practices in your implementations. Know about SQL Injection and be confident in your defenses against it Run at high performance by optimizing dynamic SQL in your applications. Troubleshoot and debug dynamic SQL to ensure correct results. Who This Book is For Dynamic SQL: Applications, Performance, and Security is for developers and database administrators looking to hone and build their T-SQL coding skills. The book is ideal for advanced users wanting to plumb the depths of application flexibility and troubleshoot performance issues involving dynamic SQL. The book is also ideal for beginners wanting to learn what dynamic SQL is about and how it can help them deliver competitive advantage to their organizations.

SpringerBriefs present concise summaries of cutting-edge research and practical applications across a wide spectrum of fields. Featuring compact volumes of 50 to 100 pages (approximately 20,000- 40,000 words), the series covers a range of content from professional to academic. Briefs allow authors to present their ideas and readers to absorb them with minimal time investment. As part of Springer's eBook collection, SpringBriefs are published to millions of users worldwide. Information/Data Leakage poses a serious threat to companies and organizations, as the number of leakage incidents and the cost they inflict continues to increase. Whether caused by malicious intent, or an inadvertent mistake, data loss can diminish a company's brand, reduce shareholder value, and damage the company's goodwill and reputation. This book aims to provide a structural and comprehensive overview of the practical solutions and current research in the DLP domain. This is the first comprehensive

book that is dedicated entirely to the field of data leakage and covers all important challenges and techniques to mitigate them. Its informative, factual pages will provide researchers, students and practitioners in the industry with a comprehensive, yet concise and convenient reference source to this fascinating field. We have grouped existing solutions into different categories based on a described taxonomy. The presented taxonomy characterizes DLP solutions according to various aspects such as: leakage source, data state, leakage channel, deployment scheme, preventive/detective approaches, and the action upon leakage. In the commercial part we review solutions of the leading DLP market players based on professional research reports and material obtained from the websites of the vendors. In the academic part we cluster the academic work according to the nature of the leakage and protection into various categories. Finally, we describe main data leakage scenarios and present for each scenario the most relevant and applicable solution or approach that will mitigate and reduce the likelihood and/or impact of the leakage scenario.

The volume contains 75 papers presented at International Conference on Communication and Networks (COMNET 2015) held during February 19–20, 2016 at Ahmedabad Management Association (AMA), Ahmedabad, India and organized by Computer Society of India (CSI), Ahmedabad Chapter, Division IV and Association of Computing Machinery (ACM), Ahmedabad Chapter. The book aims to provide a forum to researchers to propose theory and technology on the networks and services, share their experience in IT and telecommunications industries and to discuss future management solutions for communication systems, networks and services. It comprises of original contributions from researchers describing their original, unpublished, research contribution. The papers are mainly from 4 areas – Security,

Management and Control, Protocol and Deployment, and Applications. The topics covered in the book are newly emerging algorithms, communication systems, network standards, services, and applications.

This book is intended to present the state of the art in research on machine learning and big data analytics. The accepted chapters covered many themes including artificial intelligence and data mining applications, machine learning and applications, deep learning technology for big data analytics, and modeling, simulation, and security with big data. It is a valuable resource for researchers in the area of big data analytics and its applications.

This book includes high-quality research papers presented at the Third International Conference on Innovative Computing and Communication (ICICC 2020), which is held at the Shaheed Sukhdev College of Business Studies, University of Delhi, Delhi, India, on 21-23 February, 2020. Introducing the innovative works of scientists, professors, research scholars, students and industrial experts in the field of computing and communication, the book promotes the transformation of fundamental research into institutional and industrialized research and the conversion of applied exploration into real-time applications.

This book constitutes the refereed proceedings of the International Symposium on Security in Computing and Communications, SSCC 2014, held in Delhi, India, in September 2013. The 36 revised full papers presented together with 12 work-in-progress papers were carefully reviewed and selected from 132 submissions. The papers are organized in topical sections on security and privacy in networked systems; authentication and access control systems; encryption and cryptography; system and network security; work-in-progress.

This book presents the outcomes of the 2017 International

Conference on Applications and Techniques in Cyber Security and Intelligence, which focused on all aspects of techniques and applications in cyber and electronic security and intelligence research. The conference provides a forum for presenting and discussing innovative ideas, cutting-edge research findings, and novel techniques, methods and applications on all aspects of cyber and electronic security and intelligence.

The 4-volume set LNCS 11632 until LNCS 11635 constitutes the refereed proceedings of the 5th International Conference on Artificial Intelligence and Security, ICAIS 2019, which was held in New York, USA, in July 2019. The conference was formerly called “International Conference on Cloud Computing and Security” with the acronym ICCCS. The total of 230 full papers presented in this 4-volume proceedings was carefully reviewed and selected from 1529 submissions. The papers were organized in topical sections as follows: Part I: cloud computing; Part II: artificial intelligence; big data; and cloud computing and security; Part III: cloud computing and security; information hiding; IoT security; multimedia forensics; and encryption and cybersecurity; Part IV: encryption and cybersecurity.

This book reviews the latest developments in nature-inspired computation, with a focus on the cross-disciplinary applications in data mining and machine learning. Data mining, machine learning and nature-inspired computation are current hot research topics due to their importance in both theory and practical applications. Adopting an application-focused approach, each chapter introduces a specific topic, with detailed descriptions of relevant algorithms, extensive literature reviews and implementation details. Covering topics such as nature-inspired algorithms, swarm intelligence, classification, clustering, feature selection, cybersecurity, learning algorithms over cloud, extreme learning machines,

object categorization, particle swarm optimization, flower pollination and firefly algorithms, and neural networks, it also presents case studies and applications, including classifications of crisis-related tweets, extraction of named entities in the Tamil language, performance-based prediction of diseases, and healthcare services. This book is both a valuable a reference resource and a practical guide for students, researchers and professionals in computer science, data and management sciences, artificial intelligence and machine learning.