Advances in Computing and Communications, Part IISmart and Sustainable Intelligent SystemsSQL in a NutshellTrust, Privacy and Security in Digital BusinessComputer Networks and Intelligent ComputingWriting Secure CodeSQL Injection Attacksevaluation of emerging computational and knowledge transfer approaches, optimizing solutions in varied potential to provide realistic solutions to various problems in society, the environment and industry. The papers featured provide a of smart computing and informatics, focusing on innovation paradigms in system knowledge, intelligence and sustainability that have the Deemed to be University, Bhubaneswar, from 21 to 22 December 2018. It includes advanced and multi-disciplinary research on the design and implementation of system knowledge and information services focusing on innovation paradigms in computing and info. 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 

Most modern web applications rely on retrieving updated data from a database. In response to a request from a web page, the application will generate a SQL query, and often incorporate portions of the user input into the query. SQL injection refers to injecting crafted malicious SQL query segments to change the intended effect of a SQL query. The hacker could access unauthorized data, or even gain complete control over the web server or back-end database system. SQL injection attack has become one of the top web application vulnerabilities. In this project, I surveyed different types of SQL injection attacks and the corresponding countermeasure strategies proposed by other researchers. A new technique to detect and prevent SQL injection attacks is presented; the basic idea is to insert a validation process between the generation of SQL query and the query execution. The technique consists of both static analysis of web application code and runtime validation check of dynamically generated SQL query. Following four steps are involved: Identify hotspot; analyze SQL query; initialization; and runtime validation check. The project was implemented using JAVA. Performance evaluation was also conducted.

The world is experiencing an unprecedented period of change and growth through all the electronic and technological developments and everyone on the planet has been impacted. What was once ‘science fiction’, today it is a reality. This book explores the world of many of once unthinkable advancements by explaining current technologies in detail. Each chapter focuses on a different aspect - Machine Vision, Data Analysis and Fusion, Computational Intelligence and Decision Analysis - Advanced Trends in Computational Intelligence, Cyber Security, and Communication Technologies - Disruptive Technologies for Future Sustainability. The chapters include the list of topics that spans all the areas of smart intelligent systems and computing such as: Data Mining with Soft Computing, Evolutionary Computing, Quantum Computing, Expert Systems, Next Generation Communication, Blockchain and Trust Management, Intelligent Biometrics, Multi-Valued Logical Systems, Cloud Computing and security etc. An extensive list of bibliographic references at the end of each chapter guides the reader to probe further into application area of interest to him/her.

SQL injection attacks occur when a user submits maliciously formatted data to a web application that results in the application behaving in an unintended fashion. This allows attackers to access, modify, or destroy data that they would otherwise be unable to. This thesis presents a novel approach to detecting injection attacks by identifying characteristics of injection attacks and using a Bayesian model to determine the likelihood that a given query is malicious. This approach is implemented in a proxy that sits between a web application and a database and prevents suspected malicious queries from being executed. This requires no modification of existing application code and is capable of identifying unknown attacks. In tests, this approach was able to identify over 99% of common attacks while having no false positives.

The technological and industrial revolution brought by the Complex Cyber Physical Systems (CCPSs) comes with new threats and attacks that exploit their inherent complexity and heterogeneity Those attacks affect the operation of various services that are vital for the society functioning, like energy, transport, communications, and so on. A system under attack, should exhibit robustness and the ability to degrade and or survive and fast recovery of the functionality in order to avoid potentially uncontrolled cascade effects To this end, the emerging field of Cyber Resilience can be understood as a mix of strategies, methods and techniques to support CCPS adaptive capacity during cyber attacks The conference focuses on both the theoretical & practical aspects of the security, privacy, trust and resilience of networks, devices, applications, and services as well as novel ways of dealing with their vulnerabilities and mitigating sophisticated cyber attacks

The six volumes LNCS 11619-11624 constitute the refereed proceedings of the 19th International Conference on Computational Science and Its Applications, ICCSA 2019, held in Saint Petersburg, Russia, in July 2019. The 64 full papers, 10 short papers and 259 workshop papers presented were carefully reviewed and selected from numerous submissions. The 64 full papers are organized in the following five general tracks: computational methods, algorithms and scientific applications; high performance computing and networks; geometric modeling, graphics and visualization; advanced and emerging applications; and information systems and technologies. The 259 workshop papers were presented at 33 workshops in various areas of computational sciences, ranging from computational science technologies to specific areas of computational sciences, such as software engineering, security, artificial intelligence and blockchain technologies.

What is SQL injection? -- Testing for SQL injection -- Reviewing code for SQL injection -- Exploiting SQL injection -- Blind SQL injection exploitation -- Exploiting the operating system -- Advanced topics -- Code-level defenses -- Platform level defenses -- Confirming and recovering from SQL injection attacks -- References. This book presents high-quality papers from the Third International Conference on Smart Computing and Informatics (SCI 2018 | 2019), 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 and information, focusing on innovation paradigms in computing and info. 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
Read Free Detecting SQL Injection Attacks Using Short Ids

The increasing use of web applications to provide reliable online services, such as banking, shopping, etc., and to store sensitive user data has made them vulnerable to attacks that target them. In particular, SQL injection, which allows attackers to gain unauthorized access to the database by injecting specially crafted input strings, is one of the most serious threats to web applications. Although researchers and practitioners have proposed various methods to address the SQL injection problem, organizations continue to be its victim, as attackers are successfully able to circumvent the employed techniques. In this research, we develop a Runtime Monitoring Framework to detect and prevent SQL Injection Attacks on web applications. At its core, the framework leverages the knowledge gained from emerging areas of research on library services, new emerging technologies, and the advancements made to libraries during this global health crisis. The Handbook of Research on Library Response to the COVID-19 Pandemic consists of chapters that contain essential library services and emerging research and technology that evolved and/or has continued during the COVID-19 pandemic, as well as the challenges and opportunities that have been undertaken as a result. The chapters provide in-depth research, surveys, and information on areas such as remote working, machine learning, data management, and the role of information during COVID-19. This book is a valuable reference tool for practitioners, stakeholders, researchers, and students who are interested in the current state of libraries during a pandemic and the future outlook.

This volume is the second part of a four-volume set (CGIS 190, CGIS 191, CGIS 192, CGIS 193), which constitutes the refereed proceedings of the First International Conference on Computing and Communications, ACC, held in Kochi, India, in July 2011. The 72 revised full papers presented in this volume were carefully reviewed and selected from a large number of submissions. The papers are organized in topical sections on database and information systems; distributed software development; human computer interaction and interface; ICT; internet and Web computing; mobile computing; multi agent systems; multimedia and video systems; parallel and distributed algorithms; security, trust and privacy.

This book helps people find sensitive information on the Web. Google is one of the 5 most popular sites on the internet with more than 380 million unique users per month (Nielsen/NetRatings 8/05). But, Google’s search capabilities are so powerful, they sometimes discover content that no one ever intended to be publicly available on the Web including: social security numbers, credit card numbers, tools for illegal downloading, and lists of illegal drugs and weapons. Google is used by security professionals and system administrators to find this sensitive information and “self-police their own organizations. Readers will learn how Google Maps and Google Earth provide pinpoint military accuracy, see how bad guys can manipulate Google to create super worms, and see how they can “mash up” Google with MySpace, LinkedIn, and more for passive reconnaissance. - Learn Google Hacking to Find Secret Data on the Web - Learn how to search for secret data using Google. - Leverage Advanced Google Queries - Combine advanced operators and learn about colliding operators and bad search-tul. - Learn the Ways of the Google Hacker - How to use caches for anonymity and review directory listings and traversal techniques. - Review Document Gridding and Database Digging - See the ways to use Google to locate documents and then search within the documents to locate information. - Understand Google’s Part in an Information Collection Federation - Learn the principles of automating searches and the applications of data mining. - Leverage Google as your Search Platform - Learn how to use Google as a search platform to locate exploit code and find vulnerable targets. - Leverage Security Searches - Learn a few searches that give good results just about every time and are good for a security assessment. - Track Down Web Servers - Locate and profile web servers, login portals, network hardware and utilities. - See How Bad Guys Troll for Data - Find ways to search for usernames, passwords, credit card numbers, social security numbers, and other juicy information. - Hack Google Services - Learn more about the AJAX Search API, Calendar, Blogger, Blog Search, and more.

Over 120 recipes to perform advanced penetration testing with Kali Linux About This Book Practical recipes to conduct effective vulnerability testing using the powerful Kali Linux - Leverage tools like Metasploit, Wireshark, Nmap, and many more to detect vulnerabilities with ease - Confidently perform networking and application attacks using task-oriented recipes - Who This Book Is For This book is aimed at IT security professionals, pen testers, and security analysts who have basic knowledge of Kali Linux and want to conduct advanced penetration testing techniques. What You Will Learn Installing, setting up and customizing Kali for pentesting on multiple platforms - Pentesting routers and embedded devices - Bug hunting 2017 Pwning and escalating through corporate network - Buffer overflows 101 Auditing wireless networks - Fiddling around with software-defined radio Hacking on the run with NetHunter Writing good quality reports In Detail - With the current rate of hacking, it is very important to pentest your environment in order to ensure advanced level security. This book is packed with practical recipes that will quickly get you started with Kali Linux (version 2016.2) according to your needs, and move on to core functionalities. This book will start with the installation and configuration of Kali Linux so that you can perform your tests. You will learn how to plan attack strategies and perform web application exploitation using tools such as Burp, and Jexboss. You will also learn how to perform network exploitation using Metasploit, Sparta, and Wireshark. Next, you will perform wireless and payload attacks using tools such as Patator, John the Ripper, and airoscript-ng. Lastly, you will learn how to create an optimum quality pentest report! By the end of this book, you will know how to conduct advanced penetration testing thanks to the book's crisp and task-oriented recipes. Style and approach This is a recipe-based book that allows you to venture into some of the most cutting-edge practices and techniques to perform penetration testing with Kali Linux.

The volume comprises best selected papers presented at International Conference on Wireless Communication (ICWiCOM) which is organized by Department of Electronics and Telecommunication Engineering of D J Sanghvi College of Engineering. The volume focuses on narrowed topics of wireless communication like signal and image processing applicable to wireless domain, networking, microwave and antenna designs, tele-medicine systems, etc. The papers are divided into three main domains like, networking, antenna designs and embedded systems applicable to the communication domain. The content will be helpful for Post-Graduate and Doctoral students in their research.

The increasing use of web applications to provide reliable online services, such as banking, shopping, etc., and to store sensitive user data has made them vulnerable to attacks that target them. In particular, SQL injection, which allows attackers to gain unauthorized access to the database by injecting specially crafted input strings, is one of the most serious threats to web applications. Although researchers and practitioners have proposed various methods to address the SQL injection problem, organizations continue to be its victim, as attackers are successfully able to circumvent the employed techniques. In this research, we develop a Runtime Monitoring Framework to detect and prevent SQL Injection Attacks on web applications. At its core, the framework leverages the knowledge gained from pre-deployment testing of web applications to identify legal/valid execution paths. Monitors are then developed and instrumented to observe the application’s behavior and check it for compliance with the valid/legal execution paths obtained; any deviation in the application’s behavior is identified as a possible SQL Injection Attack. We conducted an extensive evaluation of the framework by targeting subject applications with a large number of both legitimate and malicious inputs, and assessed its ability to detect and prevent SQL Injection Attacks. The framework successfully allowed all the legitimate inputs to access the database without generating any false positives, and was able to effectively detect attacks without generating false negative. Moreover, the framework imposed a low runtime overhead on the subject applications compared to other techniques.
Read Free Detecting Sql Injection Attacks Using Snort Ids

Multimedia Mining; Miscellaneous Topics.

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 losing 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 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; software engineering; computer communication networks; wireless networks; distributed systems and storage networks; signal processing; image processing and pattern recognition.

This book constitutes the proceedings of the 20th International Conference on Logic for Programming, Artificial Intelligence, and Reasoning, LPAR-20, held in November 2015, in Suva, Fiji. The 43 regular papers presented together with 1 invited talk included in this volume were carefully reviewed and selected from 92 submissions. The series of International Conferences on Logic for Programming, Artificial Intelligence and Reasoning, LPAR, is a forum where, year after year, some of the most renowned researchers in the areas of logic, automated reasoning, computational logic, programming languages and their applications come to present cutting-edge results, to discuss advances in these fields, and to exchange ideas in a scientifically emerging part of the world.

This book constitutes the refereed proceedings of the 13th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, DIMVA 2016, held in San Sebastián, Spain, in July 2016. The 19 revised full papers and 2 extended abstracts presented were carefully reviewed and selected from 66 submissions. They present the state of the art in intrusion detection, malware analysis, and vulnerability assessment, dealing with novel ideas, techniques, and applications in important areas of computer security including vulnerability detection, attack prevention, web security, malware detection and classification, authentication, data leakage prevention, and countering evasive techniques such as obfuscation.

Technology provides numerous opportunities for positive developments in modern society; however, these venues inevitably increase vulnerability to threats in online environments. Addressing issues of security in the cyber realm is increasingly relevant and critical to society. Threat Mitigation and Detection of Cyber Warfare and Terrorism Activities is a comprehensive reference source for the latest scholarly perspectives on countermeasures and related methods to enhance security and protection against criminal activities online. Highlighting a range of topics relevant to secure computing, such as parameter tampering, surveillance and control, and digital protests, this book is ideally designed for academics, researchers, graduate students, professionals, and practitioners actively involved in the expanding field of cyber security.

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 book concentrates on a wide range of advances related to IT cybersecurity management. The topics covered in this book include, among others, management techniques in security, IT risk management, the impact of technologies and techniques on security management, regulatory techniques and issues, surveillance technologies, security policies, security for protocol management, location management, GOS management, resource management, channel management, and mobility management. The authors also discuss digital contents copyright protection, system security management, network security management, security management in network equipment, storage area networks (SAN) management, information security management, government security policy, web penetration testing, security operations, and vulnerabilities management. The authors introduce the concepts, techniques, methods, approaches and trends needed by cybersecurity management specialists and educators for keeping current their cybersecurity management knowledge.

Further, they provide a glimpse of future directions where cybersecurity management techniques, policies, applications, and theories are headed. The book is a rich collection of carefully selected and reviewed manuscripts written by diverse cybersecurity management experts in the listed fields and edited by prominent cybersecurity management researchers and specialists.

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.

The SQL Injection Attack is very large safety measure risk in the present scenario. That manages conscious and secret records and put the injurious SQL query put to modify the expected function. This book introduces a latest framework to protecting web based application from the SQL Injection Attack. This book is authored by Ms Rashmi Gupta and Ms. Ruchi Kamra working as assistant professor in Amity University Haryana.

This book presents recent advances in the field of distributed computing and machine learning, along with cutting-edge research in the field of Internet of Things (IoT) and blockchain in distributed environments. It features selected high-quality research papers from the First International Conference on Advances in Distributed Computing and Machine Learning (ICADCML 2020), organized by the School of Information Technology and Engineering, VIT, Vellore, India, and held on 30–31 January 2020.

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

A big novel about a small town When Barry Fairbrother dies in his early forties, the town of Pagford is left in shock. Pagford is, seemingly, an English idyll, with a cobbled market square and an ancient abbey, but what lies behind the pretty façade is a town at war. Rich at war with poor, teenagers at war with their parents, wives at war with their husbands, teachers at war with their pupils.Pagford is not what it first seems. And the empty seat left by Barry on the parish council soon becomes the catalyst for the biggest war the town has yet seen. Who will triumph in an election fraught with passion, duplicity, and unexpected revelations? A big novel about a small town, The Casual Vacancy is J.K. Rowling’s first novel for adults. It is the work of a storyteller like no other.

This book constitutes the proceedings of the 17th International Symposium on Research in Attacks, Intrusions and Defenses, RAID 2014, held in Gothenburg, Sweden, in September 2014. The 22 full papers were carefully reviewed and selected from 113 submissions, and are presented together with 10 poster abstracts. The papers address all current topics in computer security, including network security, authentication, malware, intrusion detection, browser security, web application security, wireless security, vulnerability analysis.

This book constitutes revised selected papers from the International Conference on Advanced Computing, Networking and Security, ADCONS 2011, held in Surathkal, India, in December 2011. The 73 papers included in this book were carefully reviewed and selected from 289 submissions. The papers are organized in topical sections on distributed computing, image processing, pattern recognition, applied algorithms, wireless networking, sensor networks, network infrastructure, cryptography, Web security, and application security.

This volume features the refereed proceedings of the 4th International Conference on Trust and Privacy in Digital Business. The 28 papers were all carefully reviewed. They cover 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.

This two volume set LNCS 16062 and LNCS 16063 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 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.

Learn to exploit vulnerable database applications using SQL injection tools and techniques, while understanding how to effectively prevent attacks. Key Features Understand SQL injection and its effects on websites and other systems. Get hands-on with SQL injection using both manual and automated tools. Explore practical tips for various attack and defense strategies relating to SQL injection. Book Description SQL injection (SQLi) is probably the most infamous attack that can be unleashed against applications on the internet. SQL Injection Strategies is an end-to-end guide for beginners looking to learn how to perform SQL injection and test the security of web applications, websites, or databases, using both manual and automated techniques. The book serves as both a theoretical and practical guide to take you through the important aspects of SQL injection, both from an attack and a defense perspective. You’ll start with a thorough introduction to SQL injection and its impact on websites and systems. Later, the book features steps to configure a virtual environment, so you can try SQL injection techniques safely on your own computer. These tests can be performed not only on web applications but also on web services and mobile applications that can be used for managing IoT environments. Tools such as sqlmap and others are then covered, helping you understand how to use them effectively to perform SQL injection attacks. By the end of this book, you will be well-versed with SQL injection, from both the attack and defense perspective. What you will learn Focus on how to defend against SQL injection attacks Understand web application security Get up and running with a variety of SQL injection concepts Become well-versed with different SQL injection scenarios Discover SQL injection manual attack techniques Delve into SQL injection automation Who this book is for This book is ideal for penetration testers, ethical hackers, or anyone who wants to learn about SQL injection and the various attack and defense strategies against this web security vulnerability. No prior knowledge of SQL injection is needed to get started with this book.

Covers topics such as the importance of secure systems, threat modeling, canonical representation issues, solving database input, denial-of-service attacks, and security code reviews and checklists.

Seven Deadliest Web Application Attacks highlights the vagaries of web security by discussing the seven deadliest vulnerabilities exploited by attackers. This book pinpoints the most dangerous hacks and exploits specific to web applications, laying out the anatomy of these attacks including how to make your system more secure. You will discover the best ways to defend against these vicious hacks with step-by-step instruction and learn techniques to make your computer and network impenetrable. Each chapter presents examples of different attacks conducted against web sites. The methodology behind the attack is explored, showing its potential impact. The chapter then moves on to address possible countermeasures for different aspects of the attack. The book consists of seven chapters that cover the seven most pervasive vulnerabilities in web sites and web browsers: Structured Query Language (SQL) injection attacks; mistakes of server administrators that expose the web site to attack; brute force attacks; and logic attacks. The ways in which malicious software malware has been growing as a threat on the Web are also considered. This book is ideal for security professionals of all levels, as well as application developers and recreational hackers. Knowledge is power, find out about the most dominant attacks currently waging war on computers and networks globally. Discover the best ways to defend against these vicious attacks with step-by-step instruction shows you how to mitigate countermeasures, don’t be caught defenseless again, and learn techniques to make your computer and network impenetrable.

This volume is the second part of a four-volume set (CCIS 190, CCIS 191, CCIS 192, CCIS 193), which constitutes the refereed proceedings of the First International Conference on Computing and Communications, ACC 2011, held in Kochi, India, in July 2011. The 72 revised full papers presented in this volume were carefully reviewed and selected from a large number of submissions. The papers are organized in topical sections on database and information systems; distributed software development; human computer interaction and interface; ICT; internet and Web computing; mobile computing; multi agent systems; multimedia and video systems; parallel and distributed algorithms; security, trust and privacy.

This book presents refereed proceedings of the Third International Conference on Advances in Cyber Security, ACEs 2021, held in
Read Free Detecting Sql Injection Attacks Using Snort Ids

Penang, Malaysia, in August 2021. The 36 full papers were carefully reviewed and selected from 92 submissions. The papers are organized in the following topical sections: Internet of Things, Industry 4.0 and Blockchain, and Cryptology; Digital Forensics and Surveillance, Botnet and Malware, DDoS, and Intrusion Detection/Prevention; Ambient Cloud and Edge Computing, SDN, Wireless and Cellular Communication; Governance, Social Media, Mobile and Web, Data Privacy, Data Policy and Fake News.

SQL in a Nutshell applies the eminently useful “Nutshell” format to Structured Query Language (SQL), the elegant--but complex--descriptive language that is used to create and manipulate large stores of data. For SQL programmers, analysts, and database administrators, the new second edition of SQL in a Nutshell is the essential date language reference for the world’s top SQL database products. SQL in a Nutshell is a lean, focused, and thoroughly comprehensive reference for those who live in a deadline-driven world. This invaluable desktop quick reference drills down and documents every SQL command and how to use it in both commercial (Oracle, DB2, and Microsoft SQL Server) and open source implementations (PostgreSQL, and MySQL). It describes every command and reference and includes the command syntax (by vendor, if the syntax differs across implementations), a clear description, and practical examples that illustrate important concepts and uses. And it also explains how the leading commercial and open sources database product implement SQL. This wealth of information is packed into a succinct, comprehensive, and extraordinarily easy-to-use format that covers the SQL syntax of no less than 4 different databases. When you need fast, accurate, detailed, and up-to-date SQL information, SQL in a Nutshell, Second Edition will be the quick reference you’ll reach for every time. SQL in a Nutshell is small enough to keep by your keyboard, and concise (as well as clearly organized) enough that you can look up the syntax you need quickly without having to wade through a lot of useless fluff. You won’t want to work on a project involving SQL without it.

This book constitutes the thoroughly refereed proceedings of eight international workshops held in Valencia, Spain, in conjunction with the 25th International Conference on Advanced Information Systems Engineering, CAiSE 2013, in June 2013. The 36 full and 12 short papers have undertaken a high-quality and selective acceptance policy, resulting in acceptance rates of up to 50% for full research papers. The eight workshops were Approaches for Enterprise Engineering Research (AppEER), International Workshop on BUSiness/IT ALignment and Interoperability (BUSITAL), International Workshop on Cognitive Aspects of Information Systems Engineering (COGNISE), Workshop on Human-Centric Information Systems (HC-IS), Next Generation Enterprise and Business Innovation Systems (NGEBIS), International Workshop on Ontologies and Conceptual Modeling (OntoCom), International Workshop on Variability Support in Information Systems (VarIS), International Workshop on Information Systems Security Engineering (WISSE).

SQL injection has become a predominant type of attacks that target web applications. It allows attackers to obtain unauthorized access to the back-end database by submitting malicious SQL query segments to change the intended application-generated SQL queries. Researchers have proposed various solutions to address SQL injection problems. However, many of them have limitations and often cannot address all kinds of injection problems. What's more, new types of SQL injection attacks have arisen over the years. To better counter these attacks, identifying and understanding the types of SQL injections and existing countermeasures are very important. This book presents a review of different types of SQL injections and illustrated how to use them to perform attacks. It also surveys existing techniques against SQL injection attacks and analyzed their advantages and disadvantages. In addition, it identifies techniques for building secure systems and applied them to my applications and database system, and illustrated how they were performed and the effect of them.

Copyright code: 2bb4ece9650bd88cd7bf6856b67b12c5