Detecting Sql Injection Attacks Using Snort Ids

YULIANA ALIJAH

Research in Attacks, Intrusions and Defenses John Wiley & Sons
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.
The Casual Vacancy Pearson Education
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.
Security in Computing and Communications Springer
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.
Smart and Sustainable Intelligent Systems Springer
The security of an organizational information system with the invention of next-generation technologies is a prime focus these days. The industries and institutions in the field of computing and communication, especially in internet of things, cloud computing, mobile networks, next-generation networks, the energy market, banking sector, government sector, and many more, are primarily focused on these security and privacy issues. Blockchain is a new technology that has changed the scenario when it comes to addressing security concerns and resolving traditional safety issues. These industries have started developing applications based on the blockchain underlying platform to tap into this unlimited potential. Blockchain technologies have a great future, but there are still many challenges and issues to resolve for optimal design and utilization of the technology. Revolutionary Applications of Blockchain-Enabled Privacy and Access Control focuses on the recent challenges, design, and issues in the field of blockchain technologies-enabled privacy and advanced security practices in computing and communication. This book provides the latest research findings, solutions, and relevant theoretical frameworks in blockchain technologies, information security, and privacy in computing and communication. While highlighting the technology itself along with its applications and future outlook, this book is ideal for IT specialists, security analysts, cybersecurity professionals, researchers, academicians, students, scientists, and IT sector industry practitioners looking for research exposure and new ideas in the field of blockchain.
End-to-end penetration testing solutions Springer Nature
Basics of SQL Injection Analysis, Detection and PreventionWeb SecurityLAP Lambert Academic Publishing
CRC Press
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, whihc 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 practioners have proposed various menthods 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 execuiton 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.
A 360-degree Approach IGI Global
Injection attacks, including SQL injection, cross-site scripting, and operating system command injection, rank the top two entries in the MITRE Common Vulnerability Enumeration (CVE) [1]. Under this attack model, an application (e.g., a web application) uses some untrusted input to produce an output program (e.g., a SQL query). Applications may be vulnerable to injection attacks because the untrusted input may alter the output program in malicious ways. Recent work has established a rigorous definition of injection attacks. Injections are benign iff they obey the NIE property, which states that injected symbols strictly insert or expand noncode tokens in the output program. Noncode symbols are strictly those that are either removed by the tokenizer (e.g., insignificant whitespace) or span closed values in the output program language, and code symbols are all other symbols. This thesis demonstrates that such attacks are possible on applications for android--a mobile device operating system--and Bash--a common Linux shell--and shows by construction that these attacks can be detected precisely. Specifically, this thesis examines the recent Shellshock attacks on Bash and shows how it widely differs from ordinary attacks, but can still be precisely detected by instrumenting the output program's runtime. The paper closes with a discussion of the lessons learned from this study and how best to overcome the practical challenges to precisely preventing these attacks in practice.
Sql Injection Attack and Countermeasures Springer
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, trade secrets, and federally classified documents. Google Hacking for Penetration Testers Volume 2 shows the art of manipulating Google 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 reconaissance. • Learn Google Searching Basics Explore Google’s Web-based Interface, build Google queries, and work with Google URLs. • Use Advanced Operators to Perform Advanced Queries Combine advanced operators and learn about colliding operators and bad search-fu. • Learn the Ways of the Google Hacker See how to use caches for anonymity and review directory listings and traversal techniques. • Review Document Grinding 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 Framework Learn the principles of automating searches and the applications of data mining. • Locate Exploits and Finding Targets Locate exploit code and then vulnerable targets. • See Ten Simple 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.

Writing Secure Code IGI Global

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.

Real-time Traffic Monitoring and SQL Injection Attack Detection for Edge Networks LAP Lambert Academic Publishing

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.

Cloud Computing and Security LAP Lambert Academic Publishing

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.

2020 IEEE Conference on Computer Applications(ICCA) Elsevier

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.

Web Security smashwords.inc

ICISC 2018 conference will provide an outstanding international forum for students, professors and tech enthusiast from all over the world to share ideas and achievements in the theory and practice of all areas of machines, systems and control Presentations should highlight inventive systems as a concept that combines theoretical research and applications in the field of machines, systems and control Papers from all areas of Engineering and Technology are invited

5th International Conference on Information Processing, ICIP 2011, Bangalore, India, August 5-7, 2011. Proceedings Springer Nature

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.

First International Conference, ACC 2011, Kochi, India, July 22-24, 2011. Proceedings, Part II Little, Brown

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.

Runtime Monitoring Technique to Detect and Prevent SQL Injection Attacks Springer

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.

Proceedings of International Conference on Wireless Communication Springer

The world is experiencing an unprecedented period of change and growth through all the electronic and technilogical 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 great detail. Each chapter focuses on a different aspect - Machine Vision, Pattern Analysis and Image Processing - Advanced Trends in Computational Intelligence and Data Analytics - Futuristic 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.

Proceedings of ICADCML 2020 Springer

Big Data Systems encompass massive challenges related to data diversity, storage mechanisms, and requirements of massive computational power. Further, capabilities of big data systems also vary with respect to type of problems. For instance, distributed memory systems are not recommended for iterative algorithms. Similarly, variations in big data systems also exist related to consistency and fault tolerance. The purpose of this book is to provide a detailed explanation of big data systems. The book covers various topics including Networking, Security, Privacy, Storage, Computation, Cloud Computing, NoSQL and NewSQL systems, High Performance Computing, and Deep Learning. An illustrative and practical approach has been adopted in which theoretical topics have been aided by well-explained programming and illustrative examples. Key Features: Introduces concepts and evolution of Big Data technology. Illustrates examples for thorough understanding. Contains programming examples for hands on development. Explains a variety of topics including NoSQL Systems, NewSQL systems, Security, Privacy, Networking, Cloud, High Performance Computing, and Deep Learning. Exemplifies widely used big data technologies such as Hadoop and Spark. Includes discussion on case studies and open issues. Provides end of chapter questions for enhanced learning.

CAiSE 2013 International Workshops, Valencia, Spain, June 17-21, 2013, Proceedings "O'Reilly Media, Inc."

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 focusses 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.

Revolutionary Applications of Blockchain-Enabled Privacy and Access Control Packt Publishing Ltd

Over 120 recipes to perform advanced penetration testing with Kali Linux About This Book Practical recipes to conduct effective penetration 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, pentesters, 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-defned 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 password 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.