Detecting Sql Injection Attacks Using Snort Ids

COLLINS KOLE

Advances in Distributed Computing and Machine Learning Springer Nature
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.
Third International Conference, ICCCS 2017, Nanjing, China, June 16-18, 2017, Revised Selected Papers, Part II 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.

Research in Attacks, Intrusions and Defenses "O'Reilly Media, Inc."

This book constitutes the refereed proceedings of the 17th International Conference on Applied Cryptography and Network Security, ACNS 2019, held in Bogota, Colombia in June 2019. The 29 revised full papers presented were carefully reviewed and selected from 111 submissions. The papers were organized in topical sections named: integrity and cryptanalysis; digital signature and MAC; software and systems security; blockchain and cryptocurrency; post quantum cryptography; public key and commitment; theory of cryptographic implementations; and privacy preserving techniques.

Real-time Traffic Monitoring and SQL Injection Attack Detection for Edge Networks Springer

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.

SQL Injection Attacks and Countermeasures Elsevier

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.

SQL in a Nutshell "O'Reilly Media, Inc."

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.

Proceedings of ICADCML 2020 CRC Press

Databases often store personal information such as addresses, phone numbers, bank account details, and social security numbers. SQL injection attacks can cause serious threat to applications that access this kind of information through the internet, as with this kind of attack hackers can get unrestricted access to sensitive information. Though many individuals and organizations have proposed different methods to solve this problem, they either fail to address the entire scope of the problem or are too expensive for many users to adopt. SQLiDetect is an attempt to provide a comprehensive solution to SQL injections, incorporating a detection model and a business model. The detection model uses signature-based pattern matching to check for probable SQL injections, while the business model blocks the IP address from where a hacker attempts to intrude into the system. It also provides a flexible tracking and reporting system to monitor attacks.

Precise Detection of Injection Attacks on Concrete Systems Packt Publishing Ltd

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).

Threat Mitigation and Detection of Cyber Warfare and Terrorism Activities Springer

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.

International Conference, ADCONS 2011, Surathkal, India, December 16-18, 2011, Revised Selected Papers Pearson Education

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.

Revolutionary Applications of Blockchain-Enabled Privacy and Access Control IGI Global

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.

Web Security Springer

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.

Cloud Computing and Security LAP Lambert Academic Publishing

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.

Anomaly-based Detection of SQL Injection Attacks Basics of SQL Injection Analysis, Detection and PreventionWeb Security

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.

ICWiCom 2017 Springer

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.

5th International Conference on Information Processing, ICIP 2011, Bangalore, India, August 5-7, 2011. Proceedings LAP Lambert Academic Publishing

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.

A Desktop Quick Reference Springer

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.

Proceedings of the Third International Conference on Smart Computing and Informatics, Volume 2 Springer

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 Attacks and Defense Springer

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

2020 IEEE Conference on Computer Applications(ICCA) Springer

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.