Detecting Sql Injection Attacks Using Snort Ids

This book gathers outstanding research papers presented at the 2nd International Conference on Frontiers in Computing and Systems (COMSYS 2021), organized by Department of Electronics and Communication Engineering and Department of Information Technology, North-Eastern Hill University, Shillong, Meghalaya, India held during September 29–October 1, 2021. The book presents the latest research and results in various fields of machine learning, computational intelligence, VLSI, networks and systems, computational biology, and security, making it a rich source of reference material for academia and industry alike.

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.

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.

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.

CAiSE 2013 International Workshops, Valencia, Spain, June 17-21, 2013, Proceedings

Advances in Distributed Computing and Machine Learning

2021 IEEE International Conference on Cyber Security and Resilience (CSR)

Web Security

Google Hacking for Penetration Testers

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

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.

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.

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.

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.

Python Penetration Testing Essentials

COMSYS 2021

Leverage Python scripts and libraries to overcome networking and security issues

Query Re-evaluation for Handling SQL Injection Attacks

Pinocchio, the Tale of a Puppet

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

Learn how to hack systems like black hat hackers and secure them like security experts Key Features Understand how computer systems work and their vulnerabilities Exploit weaknesses and hack into machines to test their security Learn how to secure systems from hackers Book Description This book starts with the basics of ethical hacking, how to practice hacking safely and legally, and how to install and interact with Kali Linux and the Linux terminal. You will explore network hacking, where you will see how to test the security of wired and wireless networks. You'll also learn how to crack the password for any Wi-Fi network (whether it uses WEP, WPA, or WPA2) and spy on the connected devices. Moving on, you will discover how to gain access to remote computer systems using client-side and server-side attacks. You will also get the hang of post-exploitation techniques, including remotely controlling and interacting with the systems that you compromised. Towards the end of the book, you will be able to pick up web application hacking techniques. You'll see how to discover, exploit, and prevent a number of website vulnerabilities, such as XSS and SQL injections. The attacks covered are practical techniques that work against real systems and are purely for educational purposes. At the end of each section, you will learn how to detect, prevent, and secure systems from these attacks. What you will learn Understand ethical hacking and the different fields and types of hackers Set up a penetration testing lab to practice safe and legal hacking Explore Linux basics, commands, and how to interact with the terminal Access password-protected networks and spy on connected clients Use server and client-side attacks to hack and control remote computers Control a hacked system remotely and use it to hack other systems Discover, exploit, and prevent a number of web application vulnerabilities such as XSS and SQL injections Who this book is for Learning Ethical Hacking from Scratch is for anyone interested in learning how to hack and test the security of systems like professional hackers and security experts.

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.

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

Computer application, Network Security and Cryptography, Pattern Analysis and Machine Intelligence Intelligent Databases and Information Retrieval, Image Processing, Wireless Sensor Network, Computational Biology and Bioinformatics

SQL Injection Defenses

Sql Injection Best Method For Begineers

Revolutionary Applications of Blockchain-enabled Privacy and Access Control

17th International Conference, ACNS 2019, Bogota, Colombia, June 5–7, 2019, Proceedings

Threat Mitigation and Detection of Cyber Warfare and Terrorism Activities

New Approach to Detect and Prevent SQL Injection Attacks

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.

Nowadays, configuring a network and automating security protocols are quite difficult to implement. However, using Python makes it easy to automate this whole process. This book explains the process of using Python for building networks, detecting network errors, and performing different security protocols using Python Scripting.

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.

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.

Learn Ethical Hacking from Scratch

Your stepping stone to penetration testing

Mastering Python for Networking and Security

Prevention and Detection of SQL Injection Attacks at the Database Layer

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

SQL Injection Attacks and Defense

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.

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 as energy, transport, communications, and so on A system under attack, should exhibit resilience in the form of grateful degradation and or survival 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

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.

If you are a Python programmer or a security researcher who has basic knowledge of Python programming and want to learn about penetration testing with the help of Python, this book is ideal for you. Even if you are new to the field of ethical hacking, this book can help you find the vulnerabilities in your system so that you are ready to tackle any kind of attack or intrusion.

Cloud Computing and Security

Proceedings of International Conference on Frontiers in Computing and Systems

Advances in Computing and Communications, Part II

Proceedings of Second Doctoral Symposium on Computational Intelligence

Proceedings of ICADCML 2020

Applied Cryptography and Network Security

SQL Injection Attacks and DefenseElsevier

This book includes original unpublished contributions presented at the International Conference on Data Analytics and Management (ICDAM 2021), held at Jan Wyzykowski University, Poland, during June 2021. The book covers the topics in data analytics, data management, big data, computational intelligence, and communication networks. The book presents innovative work by leading academics, researchers, and experts from industry which is useful for young researchers and students.

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 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.

Runtime Monitoring Technique to Detect and Prevent SQL Injection Attacks

Advanced Computing, Networking and Security

Sql Injection Attack and Countermeasures

Big Data Systems

Proceedings of Data Analytics and Management

Second International Symposium, SSCC 2014, Delhi, India, September 24-27, 2014. Proceedings

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.

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.

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.

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).

SQLiDetect: a Web Based Intrusion Detection System for SQL Injections

Anomaly-based Detection of SQL Injection Attacks

Tools and Techniques to Attack the Web

Writing Secure Code

Security in Computing and Communications

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

"This book provides the latest research findings, solutions and relevant theoretical frameworks in the area of blockchain technologies, information security, and privacy in computing and communication for professionals who want to improve their understanding of the recent challenges, design, and issues in these areas"--

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.

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 form 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.

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.

Emerging ICT for Bridging the Future - Proceedings of the 49th Annual Convention of the Computer Society of India (CSI) Volume 1

The Basics of Web Hacking

2018 2nd International Conference on Inventive Systems and Control (ICISC)

DoSCI 2021

Advanced Information Systems Engineering Workshops

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.

This book features high-quality research papers presented at Second Doctoral Symposium on Computational Intelligence (DoSCI-2021), organized by Institute of Engineering and Technology (IET), AKTU, Lucknow, India, on 6 March 2021. This book discusses the topics such as computational intelligence, artificial intelligence, deep learning, evolutionary algorithms, swarm intelligence, fuzzy sets and vague sets, rough set theoretic approaches, quantum-inspired computational intelligence, hybrid computational intelligence, machine learning, computer vision, soft computing, distributed computing, parallel and grid computing, cloud computing, high-performance computing, biomedical computing, decision support and decision making.

Pinocchio, The Tale of a Puppet follows the adventures of a talking wooden puppet whose nose grew longer whenever he told a lie and who wanted more than anything else to become a real boy.As carpenter Master Antonio begins to carve a block of pinewood into a leg for his table the log shouts out, "Don't strike me too hard!" Frightened by the talking log, Master Cherry does not know what to do until his neighbor Geppetto drops by looking for a piece of wood to build a marionette. Antonio gives the block to Geppetto. And thus begins the life of Pinocchio, the puppet that turns into a boy.Pinocchio, The Tale of a Puppet is a novel for children by Carlo Collodi is about the mischievous adventures of Pinocchio, an animated marionette, and his poor father and woodcarver Geppetto. It is considered a classic of children's literature and has spawned many derivative works of art. But this is not the story we've seen in film but the original version full of harrowing adventures faced by Pinnocchio. It includes 40 illustrations.

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.

2020 IEEE Conference on Computer Applications(ICCA)

Precise Detection of Injection Attacks on Concrete Systems

Computer Networks and Intelligent Computing

A 360-degree Approach

19th International Conference, Saint Petersburg, Russia, July 1–4, 2019, Proceedings, Part V

Smart and Sustainable Intelligent Systems

The Basics of Web Hacking introduces you to a tool-driven process to identify the most widespread vulnerabilities in Web applications. No prior experience is needed. Web apps are a "path of least resistance" that can be exploited to cause the most damage to a system, with the lowest hurdles to overcome. This is a perfect storm for beginning hackers. The process set forth in this book introduces not only the theory and practical information related to these vulnerabilities, but also the detailed configuration and usage of widely available tools necessary to exploit these vulnerabilities. The Basics of Web Hacking provides a simple and clean explanation of how to utilize tools such as Burp Suite, sqlmap, and Zed Attack Proxy (ZAP), as well as basic network scanning tools such as nmap, Nikto, Nessus, Metasploit, John the Ripper, web shells, netcat, and more. Dr. Josh Pauli teaches software security at Dakota State University and has presented on this topic to the U.S. Department of Homeland Security, the NSA, BlackHat Briefings, and Defcon. He will lead you through a focused, three-part approach to Web security, including hacking the server, hacking the Web app, and hacking the Web user. With Dr. Pauli's approach, you will fully understand the what/where/why/how of the most widespread Web vulnerabilities and how easily they can be exploited with the correct tools. You will learn how to set up a safe environment to conduct these attacks, including an attacker Virtual Machine (VM) with all necessary tools and several known-vulnerable Web application VMs that are widely available and maintained for this very purpose. Once you complete the entire process, not only will you be prepared to test for the most damaging Web exploits, you will also be prepared to conduct more advanced Web hacks that mandate a strong base of knowledge. Provides a simple and clean approach to Web hacking, including hands-on examples and exercises that are designed to teach you how to hack the server, hack the Web app, and hack the Web user Covers the most significant new tools such as nmap, Nikto, Nessus, Metasploit, John the Ripper, web shells, netcat, and more! Written by an author who works in the field as a penetration tester and who teaches Web security classes at Dakota State University

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.

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.

Computational Science and Its Applications – ICCSA 2019

ICDAM 2021, Volume 2

Third International Conference, ICCCS 2017, Nanjing, China, June 16-18, 2017, Revised Selected Papers, Part II

Basics of SQL Injection Analysis, Detection and Prevention