SQL Injection Attacks And Defense

Yeah, reviewing a book **SQL Injection Attacks And Defense** could amass your close links listings. This is just one of the solutions for you to be successful. As understood, expertise does not recommend that you have fantastic points.

Comprehending as well as deal even more than further will allow each success. bordering to, the message as without difficulty as keenness of this SQL Injection Attacks And Defense can be taken as without difficulty as picked to act.

Web Security for Developers - Malcolm McDonald 2020-06-19
Website security made easy. This book covers the most common ways websites get hacked and how web developers can defend themselves. The world has changed. Today, every time you make a site live, you're opening it up to attack. A first-time developer can easily be discouraged by the difficulties involved with properly securing a website. But have hope: an army of security researchers is out there discovering, documenting, and fixing security flaws. Thankfully, the tools you'll need to secure your site are freely available and generally easy to use. Web Security for Developers will teach you how your websites are vulnerable to attack and how to protect them. Each chapter breaks down a major security vulnerability and explores a real-world attack, coupled with plenty of code to show you both the vulnerability and the fix. You'll learn how to: Protect against SQL injection attacks, malicious JavaScript, and cross-site request forgery Add authentication and shape access control to protect accounts Lock down user accounts to prevent attacks that rely on guessing passwords, stealing sessions, or escalating privileges Implement encryption Manage vulnerabilities in legacy code Prevent information leaks that disclose vulnerabilities Mitigate advanced attacks like malvertising and denial-of-service As you get stronger at identifying and fixing vulnerabilities, you'll learn to deploy disciplined, secure code and become a better programmer along the way.
Cybersecurity Blue Team Toolkit - Nadean H. Tanner 2019-04-04
A practical handbook to cybersecurity for both tech and non-tech professionals As reports of major data breaches fill the headlines, it has become impossible for any business, large or small, to ignore the importance of cybersecurity. Most books on the subject, however, are either too specialized for the non-technical professional or too general for positions in the IT trenches. Thanks to author Nadean Tanner’s wide array of experience from teaching at a University to working for the Department of Defense, the Cybersecurity Blue Team Toolkit strikes the perfect balance of substantive and accessible, making it equally useful to those in IT or management positions across a variety of industries. This handy guide takes a simple and strategic look at best practices and tools available to both cybersecurity management and hands-on professionals, whether they be new to the field or looking to expand their expertise. Tanner gives comprehensive coverage to such crucial topics as security assessment and configuration, strategies for protection and defense, offensive measures, and remediation while aligning the concept with the right tool using the CIS Controls version 7 as a guide. Readers will learn why and how to use fundamental open source and free tools such as ping, tracert, PuTTY, pathping, sysinternals, NMAP, OpenVAS, Nexpose Community, OSSEC, Hamachi, InSSIDer, Nexpose Community, Wireshark, Solarwinds Kiwi Syslog Server, Metasploit, Burp, Clonezilla and many more. Up-to-date and practical cybersecurity instruction, applicable to both management and technical positions • Straightforward explanations of the theory behind cybersecurity best practices • Designed to be an easily navigated tool for daily use • Includes training appendix on Linux, how to build a virtual lab and glossary of key terms

The Cybersecurity Blue Team Toolkit is an excellent resource for anyone working in digital policy as well as IT security professionals, technical analysts, program managers, and Chief Information and Technology Officers. This is one handbook that won't gather dust on the shelf, but remain a valuable reference at any career level, from student to executive.

Security Warrior - Cyrus Peikari 2004-01-12

When it comes to network security, many users and administrators are running scared, and justifiably so. The sophistication of attacks against computer systems increases with each new Internet worm.What's the worst an attacker can do to you? You'd better find out, right? That's what Security Warrior teaches you. Based on the principle that the only way to defend yourself is to understand your attacker in depth, Security Warrior reveals how your systems can be attacked. Covering everything from reverse engineering to SQL attacks, and including topics like social engineering, antiforensics, and common attacks against UNIX and Windows systems, this book teaches you to know your enemy and how to be prepared to do battle.Security Warrior places particular emphasis on reverse engineering. RE is a fundamental skill for the administrator, who must be aware of all kinds of malware that can be installed on his machines -- trojaned binaries, "spyware" that looks innocuous but that sends private data back to its creator, and more. This is the only book to discuss reverse engineering for Linux or Windows CE. It's also the only book that shows you how SQL injection works, enabling you to inspect your database and web applications for vulnerability.Security Warrior is the most comprehensive and up-to-date book covering the art of computer war: attacks against computer systems and their defenses. It's often scary, and never comforting. If you're on the front lines, defending your site against attackers, you need this book. On your shelf--and in your hands.

Cybersecurity Ops with bash - Paul Troncone 2019-04-02

If you hope to outmaneuver threat actors, speed and efficiency need to be key components of your cybersecurity operations. Mastery of the standard command-line interface (CLI) is an invaluable skill in times of crisis because no other software application can match the CLI's availability, flexibility, and agility. This practical guide shows you how to use the CLI with the bash shell to perform tasks such as data collection and analysis, intrusion detection, reverse engineering, and administration. Authors Paul Troncone, founder of Digadel Corporation, and Carl Albing, coauthor of bash Cookbook (O'Reilly), provide insight into command-line tools and techniques to help defensive operators collect data, analyze logs, and monitor networks. Penetration testers will learn how to leverage the enormous amount of functionality built into nearly every version of Linux to enable offensive operations. In four parts, security practitioners, administrators, and students will examine: Foundations: Principles of defense and offense, command-line and bash basics, and regular expressions Defensive security operations: Data collection and analysis, real-time log monitoring, and malware analysis Penetration testing: Script obfuscation and tools for command-line fuzzing and remote access Security administration: Users, groups, and permissions; device and software inventory

Penetration Testing and Network Defense - Andrew Whitaker 2006

The practical guide to simulating, detecting, and responding to network attacks Create step-by-step testing plans Learn to perform social engineering and host reconnaissance Evaluate session hijacking methods Exploit web server vulnerabilities Detect attempts to breach database security Use password crackers to obtain access information Circumvent Intrusion Prevention Systems (IPS) and firewall protections and disrupt the service of routers and switches Scan and penetrate wireless networks Understand the inner workings of Trojan Horses, viruses, and other backdoor applications Test UNIX, Microsoft, and Novell servers for vulnerabilities Learn the root cause of buffer overflows and how to prevent them Perform and prevent Denial of Service attacks Penetration testing is a growing field but there has yet to be a definitive resource that instructs ethical hackers on how to perform a penetration test with the ethics and responsibilities of testing in mind. Penetration Testing and Network Defense offers detailed steps on how to emulate an outside attacker in order to assess

the security of a network. Unlike other books on hacking, this book is specifically geared towards penetration testing. It includes important information about liability issues and ethics as well as procedures and documentation. Using popular open-source and commercial applications, the book shows you how to perform a penetration test on an organization's network, from creating a test plan to performing social engineering and host reconnaissance to performing simulated attacks on both wired and wireless networks. Penetration Testing and Network Defense also goes a step further than other books on hacking, as it demonstrates how to detect an attack on a live network. By detailing the method of an attack and how to spot an attack on your network, this book better prepares you to guard against hackers. You will learn how to configure, record, and thwart these attacks and how to harden a system to protect it against future internal and external attacks. Full of real-world examples and step-by-step procedures, this book is both an enjoyable read and full of practical advice that will help you assess network security and develop a plan for locking down sensitive data and company resources. "This book goes to great lengths to explain the various testing approaches that are used today and gives excellent insight into how a responsible penetration testing specialist executes his trade." -Bruce Murphy, Vice President, World Wide Security Services, Cisco Systems(R)

Cybersecurity ??? Attack and Defense Strategies - Yuri Diogenes 2018-01-30

Enhance your organization’s secure posture by improving your attack and defense strategies Key Features Gain a clear understanding of the attack methods, and patterns to recognize abnormal behavior within your organization with Blue Team tactics. Learn to unique techniques to gather exploitation intelligence, identify risk and demonstrate impact with Red Team and Blue Team strategies. A practical guide that will give you hands-on experience to mitigate risks and prevent attackers from infiltrating your system. Book Description The book will start talking about the security posture before moving to Red Team tactics, where you will learn the basic syntax for the Windows and Linux tools that are commonly used to perform the necessary operations. You will also gain hands-on experience of using new Red Team techniques with powerful tools such as python and PowerShell, which will enable you to discover vulnerabilities in your system and how to exploit them. Moving on, you will learn how a system is usually compromised by adversaries, and how they hack user's identity, and the various tools used by the Red Team to find vulnerabilities in a system. In the next section, you will learn about the defense strategies followed by the Blue Team to enhance the overall security of a system. You will also learn about an in-depth strategy to ensure that there are security controls in each network layer, and how you can carry out the recovery process of a compromised system. Finally, you will learn how to create a vulnerability management strategy and the different techniques for manual log analysis. By the end of this book, you will be well-versed with Red Team and Blue Team techniques and will have learned the techniques used nowadays to attack and defend systems. What you will learn Learn the importance of having a solid foundation for your security posture Understand the attack strategy using cyber security kill chain Learn how to enhance your defense strategy by improving your security policies, hardening your network, implementing active sensors, and leveraging threat intelligence Learn how to perform an incident investigation Get an in-depth understanding of the recovery process Understand continuous security monitoring and how to implement a vulnerability management strategy Learn how to perform log analysis to identify suspicious activities Who this book is for This book aims at IT professional who want to venture the IT security domain. IT pentester, Security consultants, and ethical hackers will also find this course useful. Prior knowledge of penetration testing would be beneficial.

Real-World Bug Hunting - Peter Yaworski 2019-07-09

Learn how people break websites and how you can, too. Real-World Bug Hunting is the premier field guide to finding software bugs. Whether you're a cyber-security beginner who wants to make the internet safer or a seasoned developer who wants to write secure code, ethical hacker Peter Yaworski will show you how it's done. You'll learn about the most common types of

bugs like cross-site scripting, insecure direct object references, and server-side request forgery. Using real-life case studies of rewarded vulnerabilities from applications like Twitter, Facebook, Google, and Uber, you'll see how hackers manage to invoke race conditions while transferring money, use URL parameter to cause users to like unintended tweets, and more. Each chapter introduces a vulnerability type accompanied by a series of actual reported bug bounties. The book's collection of tales from the field will teach you how attackers trick users into giving away their sensitive information and how sites may reveal their vulnerabilities to savvy users. You'll even learn how you could turn your challenging new hobby into a successful career. You'll learn: How the internet works and basic web hacking concepts How attackers compromise websites How to identify functionality commonly associated with vulnerabilities How to find bug bounty programs and submit effective vulnerability reports Real-World Bug Hunting is a fascinating soup-to-nuts primer on web security vulnerabilities, filled with stories from the trenches and practical wisdom. With your new understanding of site security and weaknesses, you can help make the web a safer place--and profit while you're at it.

Seven Deadliest Web Application Attacks - Mike Shema 2010-02-20

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 following: the most pervasive and easily exploited 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 intended for information security professionals of all levels, as well as web 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; step-by-step instruction shows you how Institute countermeasures, don’t be caught defenseless again, and learn techniques to make your computer and network impenetrable

SQL Injection Strategies - Ettore Galluccio 2020-07-15

Learn to exploit vulnerable database applications using SQL injection tools and techniques, while understanding how to effectively prevent attacks Key FeaturesUnderstand SQL injection and its effects on websites and other systemsGet hands-on with SQL injection using both manual and automated toolsExplore practical tips for various attack and defense strategies relating to SQL injectionBook 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 learnFocus on how to defend against SQL injection attacksUnderstand web application securityGet up and running with a variety of SQL injection conceptsBecome well-versed with different SQL injection scenariosDiscover SQL injection manual attack techniquesDelve into SQL injection automated techniquesWho 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.

SEED Labs - Wenliang Du 2018-04-28
Instructor manual (for instructors only)

Mobile Malware Attacks and Defense - Ken Dunham 2008-11-12
Malware has gone mobile, and the security landscape is changing quickly with emerging attacks on cell phones, PDAs, and other mobile devices. This first book on the growing threat covers a wide range of malware targeting operating systems like Symbian and new devices like the iPhone. Examining code in past, current, and future risks, protect your banking, auctioning, and other activities performed on mobile devices. * Visual Payloads View attacks as visible to the end user, including notation of variants. * Timeline of Mobile Hoaxes and Threats Understand the history of major attacks and horizon for emerging threates. * Overview of Mobile Malware Families Identify and understand groups of mobile malicious code and their variations. * Taxonomy of Mobile Malware Bring order to known samples based on infection, distribution, and payload strategies. * Phishing, SMishing, and Vishing Attacks Detect and mitigate phone-based phishing (vishing) and SMS phishing (SMishing) techniques. * Operating System and Device Vulnerabilities Analyze unique OS security issues and examine offensive mobile device threats. * Analyze Mobile Malware Design a sandbox for dynamic software analysis and use MobileSandbox to analyze mobile malware. * Forensic Analysis of Mobile Malware Conduct forensic analysis of mobile devices and learn key differences in mobile forensics. * Debugging and Disassembling Mobile Malware Use IDA and other tools to reverse-engineer samples of malicious code for analysis. * Mobile Malware Mitigation Measures Qualify risk, understand threats to mobile assets, defend against attacks, and remediate incidents. * Understand the History and Threat Landscape of Rapidly Emerging Mobile Attacks * Analyze Mobile Device/Platform Vulnerabilities and Exploits * Mitigate Current and Future Mobile Malware Threats

Verification, Model Checking, and Abstract Interpretation - Isil Dillig 2018-01-03
This book constitutes the refereed proceedings of the 19th International Conference on Verification, Model Checking, and Abstract Interpretation, VMCAI 2018, held in Los Angeles, CA, USA, in January 2018.The 24 full papers presented together with the abstracts of 3 invited keynotes and 1 invited tutorial were carefully reviewed and selected from 43 submissions. VMCAI provides topics including: program verification, model checking, abstract interpretation, program synthesis, static analysis, type systems, deductive methods, program certification, decision procedures, theorem proving, program certification, debugging techniques, program transformation, optimization, and hybrid and cyber-physical systems.

Inside Microsoft SQL Server 2008 - Itzik Ben-Gan 2009
Provides information on the architecture of the T-SQL programming language to create scalable code.

The Web Application Hacker's Handbook: Finding And Exploiting Security Flaws, 2nd Ed - Dafydd Stuttard

The Tao of Network Security Monitoring - Richard Bejtlich 2004-07-12
"The book you are about to read will arm you with the knowledge you need to defend your network from attackers—both the obvious and the not so obvious.... If you are new to network security, don't put this book back on the shelf! This is a great book for beginners and I wish I had access to it many years ago. If you've learned the basics of TCP/IP protocols and run an open source or commercial IDS, you may be asking 'What's next?' If so, this book is for you." —Ron Gula, founder and CTO, Tenable Network

Security, from the Foreword "Richard Bejtlich has a good perspective on Internet security—one that is orderly and practical at the same time. He keeps readers grounded and addresses the fundamentals in an accessible way." —Marcus Ranum, TruSecure "This book is not about security or network monitoring: It's about both, and in reality these are two aspects of the same problem. You can easily find people who are security experts or network monitors, but this book explains how to master both topics." —Luca Deri, ntop.org "This book will enable security professionals of all skill sets to improve their understanding of what it takes to set up, maintain, and utilize a successful network intrusion detection strategy." —Kirby Kuehl, Cisco Systems Every network can be compromised. There are too many systems, offering too many services, running too many flawed applications. No amount of careful coding, patch management, or access control can keep out every attacker. If prevention eventually fails, how do you prepare for the intrusions that will eventually happen? Network security monitoring (NSM) equips security staff to deal with the inevitable consequences of too few resources and too many responsibilities. NSM collects the data needed to generate better assessment, detection, and response processes—resulting in decreased impact from unauthorized activities. In The Tao of Network Security Monitoring , Richard Bejtlich explores the products, people, and processes that implement the NSM model. By focusing on case studies and the application of open source tools, he helps you gain hands-on knowledge of how to better defend networks and how to mitigate damage from security incidents. Inside, you will find in-depth information on the following areas. The NSM operational framework and deployment considerations. How to use a variety of open-source tools—including Sguil, Argus, and Ethereal—to mine network traffic for full content, session, statistical, and alert data. Best practices for conducting emergency NSM in an incident response scenario, evaluating monitoring vendors, and deploying an NSM architecture. Developing and applying knowledge of weapons, tactics, telecommunications, system administration, scripting, and programming for NSM. The best tools for generating arbitrary packets, exploiting flaws, manipulating traffic, and conducting reconnaissance. Whether you are new to network intrusion detection and incident response, or a computer-security veteran, this book will enable you to quickly develop and apply the skills needed to detect, prevent, and respond to new and emerging threats.

Algorithms and Architectures for Parallel Processing - Sheng Wen 2020-01-21

The two-volume set LNCS 11944-11945 constitutes the proceedings of the 19th International Conference on Algorithms and Architectures for Parallel Processing, ICA3PP 2019, held in Melbourne, Australia, in December 2019. The 73 full and 29 short papers presented were carefully reviewed and selected from 251 submissions. The papers are organized in topical sections on: Parallel and Distributed Architectures, Software Systems and Programming Models, Distributed and Parallel and Network-based Computing, Big Data and its Applications, Distributed and Parallel Algorithms, Applications of Distributed and Parallel Computing, Service Dependability and Security, IoT and CPS Computing, Performance Modelling and Evaluation.

Hacking: The Next Generation - Nitesh Dhanjani 2009-08-29

With the advent of rich Internet applications, the explosion of social media, and the increased use of powerful cloud computing infrastructures, a new generation of attackers has added cunning new techniques to its arsenal. For anyone involved in defending an application or a network of systems, Hacking: The Next Generation is one of the few books to identify a variety of emerging attack vectors. You'll not only find valuable information on new hacks that attempt to exploit technical flaws, you'll also learn how attackers take advantage of individuals via social networking sites, and abuse vulnerabilities in wireless technologies and cloud infrastructures. Written by seasoned Internet security professionals, this book helps you understand the motives and psychology of hackers behind these attacks, enabling you to better prepare and defend against them. Learn how "inside out" techniques can poke holes into protected networks Understand the new wave of "blended threats" that take advantage of

multiple application vulnerabilities to steal corporate data Recognize weaknesses in today's powerful cloud infrastructures and how they can be exploited Prevent attacks against the mobile workforce and their devices containing valuable data Be aware of attacks via social networking sites to obtain confidential information from executives and their assistants Get case studies that show how several layers of vulnerabilities can be used to compromise multinational corporations

The Browser Hacker's Handbook - Wade Alcorn 2014-02-26

Hackers exploit browser vulnerabilities to attack deep withinnetworks The Browser Hacker's Handbook gives a practicalunderstanding of hacking the everyday web browser and using it as abeachhead to launch further attacks deep into corporate networks.Written by a team of highly experienced computer security experts,the handbook provides hands-on tutorials exploring a range ofcurrent attack methods. The web browser has become the most popular and widely usedcomputer "program" in the world. As the gateway to the Internet, itis part of the storefront to any business that operates online, butit is also one of the most vulnerable entry points of any system.With attacks on the rise, companies are increasingly employingbrowser-hardening techniques to protect the unique vulnerabilitiesinherent in all currently used browsers. The Browser Hacker'sHandbook thoroughly covers complex security issues and exploresrelevant topics such as: Bypassing the Same Origin Policy ARP spoofing, social engineering, and phishing to accessbrowsers DNS tunneling, attacking web applications, andproxying—all from the browser Exploiting the browser and its ecosystem (plugins andextensions) Cross-origin attacks, including Inter-protocol Communicationand Exploitation The Browser Hacker's Handbook is written with aprofessional security engagement in mind. Leveraging browsers aspivot points into a target's network should form an integralcomponent into any social engineering or red-team securityassessment. This handbook provides a complete methodology tounderstand and structure your next browser penetration test.

Securing SQL Server - Denny Cherry 2015-04-27

SQL server is the most widely-used database platform in the world, and a large percentage of these databases are not properly secured, exposing sensitive customer and business data to attack. In Securing SQL Server, Third Edition, you will learn about the potential attack vectors that can be used to break into SQL server databases as well as how to protect databases from these attacks. In this book, Denny Cherry - a Microsoft SQL MVP and one of the biggest names in SQL server - will teach you how to properly secure an SQL server database from internal and external threats using best practices as well as specific tricks that the author employs in his role as a consultant for some of the largest SQL server deployments in the world. Fully updated to cover the latest technology in SQL Server 2014, this new edition walks you through how to secure new features of the 2014 release. New topics in the book include vLANs, setting up RRAS, anti-virus installs, key management, moving from plaintext to encrypted values in an existing application, securing Analysis Services Objects, Managed Service Accounts, OS rights needed by the DBA, SQL Agent Security, Table Permissions, Views, Stored Procedures, Functions, Service Broker Objects, and much more. Presents hands-on techniques for protecting your SQL Server database from intrusion and attack Provides the most in-depth coverage of all aspects of SQL Server database security, including a wealth of new material on Microsoft SQL Server 2014. Explains how to set up your database securely, how to determine when someone tries to break in, what the intruder has accessed or damaged, and how to respond and mitigate damage if an intrusion occurs.

Metasploit - David Kennedy 2011-07-15

The Metasploit Framework makes discovering, exploiting, and sharing vulnerabilities quick and relatively painless. But while Metasploit is used by security professionals everywhere, the tool can be hard to grasp for first-time users. Metasploit: The Penetration Tester's Guide fills this gap by teaching you how to harness the Framework and interact with the vibrant community of Metasploit contributors. Once you've built your foundation for penetration testing, you'll learn the Framework's conventions, interfaces, and module system as

you launch simulated attacks. You'll move on to advanced penetration testing techniques, including network reconnaissance and enumeration, client-side attacks, wireless attacks, and targeted social-engineering attacks. Learn how to: –Find and exploit unmaintained, misconfigured, and unpatched systems –Perform reconnaissance and find valuable information about your target –Bypass anti-virus technologies and circumvent security controls –Integrate Nmap, NeXpose, and Nessus with Metasploit to automate discovery –Use the Meterpreter shell to launch further attacks from inside the network –Harness standalone Metasploit utilities, third-party tools, and plug-ins –Learn how to write your own Meterpreter post exploitation modules and scripts You'll even touch on exploit discovery for zero-day research, write a fuzzer, port existing exploits into the Framework, and learn how to cover your tracks. Whether your goal is to secure your own networks or to put someone else's to the test, Metasploit: The Penetration Tester's Guide will take you there and beyond.

Network Security Tools - Nitesh Dhanjani 2005-04-04

If you're an advanced security professional, then you know that the battle to protect online privacy continues to rage on. Security chat rooms, especially, are resounding with calls for vendors to take more responsibility to release products that are more secure. In fact, with all the information and code that is passed on a daily basis, it's a fight that may never end. Fortunately, there are a number of open source security tools that give you a leg up in the battle.Often a security tool does exactly what you want, right out of the box. More frequently, you need to customize the tool to fit the needs of your network structure. Network Security Tools shows experienced administrators how to modify, customize, and extend popular open source security tools such as Nikto, Ettercap, and Nessus.This concise, high-end guide discusses the common customizations and extensions for these tools, then shows you how to write even more specialized attack and penetration reviews that are suited to your unique network environment. It also explains how tools like port scanners, packet injectors, network sniffers, and web assessment tools function.Some of the topics covered include: Writing your own network sniffers and packet injection tools Writing plugins for Nessus, Ettercap, and Nikto Developing exploits for Metasploit Code analysis for web applications Writing kernel modules for security applications, and understanding rootkits While many books on security are either tediously academic or overly sensational, Network Security Tools takes an even-handed and accessible approach that will let you quickly review the problem and implement new, practical solutions--without reinventing the wheel. In an age when security is critical, Network Security Tools is the resource you want at your side when locking down your network.

Understanding Network Hacks - Bastian Ballmann 2015-01-19

This book explains how to see one's own network through the eyes of an attacker, to understand their techniques and effectively protect against them. Through Python code samples the reader learns to code tools on subjects such as password sniffing, ARP poisoning, DNS spoofing, SQL injection, Google harvesting and Wifi hacking. Furthermore the reader will be introduced to defense methods such as intrusion detection and prevention systems and log file analysis by diving into code.

Secure Your Node.js Web Application - Karl Duuna 2016-01-07

Cyber-criminals have your web applications in their crosshairs. They search for and exploit common security mistakes in your web application to steal user data. Learn how you can secure your Node.js applications, database and web server to avoid these security holes. Discover the primary attack vectors against web applications, and implement security best practices and effective countermeasures. Coding securely will make you a stronger web developer and analyst, and you'll protect your users. Bake security into your code from the start. See how to protect your Node.js applications at every point in the software development life cycle, from setting up the application environment to configuring the database and adding new functionality. You'll follow application security best practices and analyze common coding errors in applications as you work through the real-world scenarios in this book. Protect your

database calls from database injection attacks and learn how to securely handle user authentication within your application. Configure your servers securely and build in proper access controls to protect both the web application and all the users using the service. Defend your application from denial of service attacks. Understand how malicious actors target coding flaws and lapses in programming logic to break in to web applications to steal information and disrupt operations. Work through examples illustrating security methods in Node.js. Learn defenses to protect user data flowing in and out of the application. By the end of the book, you'll understand the world of web application security, how to avoid building web applications that attackers consider an easy target, and how to increase your value as a programmer. What You Need: In this book we will be using mainly Node.js. The book covers the basics of JavaScript and Node.js. Since most Web applications have some kind of a database backend, examples in this book work with some of the more popular databases, including MySQL, MongoDB, and Redis.

Innocent Code - Sverre H. Huseby 2004-11-19
This concise and practical book shows where code vulnerabilities lie-without delving into the specifics of each system architecture, programming or scripting language, or application-and how best to fix them Based on real-world situations taken from the author's experiences of tracking coding mistakes at major financial institutions Covers SQL injection attacks, cross-site scripting, data manipulation in order to bypass authorization, and other attacks that work because of missing pieces of code Shows developers how to change their mindset from Web site construction to Web site destruction in order to find dangerous code

Vulnerability Analysis and Defense for the Internet - Abhishek Singh 2008-01-24
Vulnerability analysis, also known as vulnerability assessment, is a process that defines, identifies, and classifies the security holes, or vulnerabilities, in a computer, network, or application. In addition, vulnerability analysis can forecast the effectiveness of proposed countermeasures and evaluate their actual effectiveness after they are put into use. Vulnerability Analysis and Defense for the Internet provides packet captures, flow charts and pseudo code, which enable a user to identify if an application/protocol is vulnerable. This edited volume also includes case studies that discuss the latest exploits.

SQL Injection Attacks and Defense - Justin Clarke-Salt 2009-06-16
SQL Injection Attacks and Defense, First Edition: Winner of the Best Book Bejtlich Read Award "SQL injection is probably the number one problem for any server-side application, and this book unequaled in its coverage." –Richard Bejtlich, Tao Security blog SQL injection represents one of the most dangerous and well-known, yet misunderstood, security vulnerabilities on the Internet, largely because there is no central repository of information available for penetration testers, IT security consultants and practitioners, and web/software developers to turn to for help. SQL Injection Attacks and Defense, Second Edition is the only book devoted exclusively to this long-established but recently growing threat. This is the definitive resource for understanding, finding, exploiting, and defending against this increasingly popular and particularly destructive type of Internet-based attack. SQL Injection Attacks and Defense, Second Edition includes all the currently known information about these attacks and significant insight from its team of SQL injection experts, who tell you about: Understanding SQL Injection – Understand what it is and how it works Find, confirm and automate SQL injection discovery Tips and tricks for finding SQL injection within code Create exploits for using SQL injection Design apps to avoid the dangers these attacks SQL injection on different databases SQL injection on different technologies SQL injection testing techniques Case Studies Securing SQL Server, Second Edition is the only book to provide a complete understanding of SQL injection, from the basics of vulnerability to discovery, exploitation, prevention, and mitigation measures. Covers unique, publicly unavailable information, by technical experts in such areas as Oracle, Microsoft SQL Server, and MySQL---including new developments for Microsoft SQL Server 2012 (Denali). Written by an established expert, author, and speaker in the field, with contributions from a team of equally renowned

creators of SQL injection tools, applications, and educational materials.

XSS Attacks - Seth Fogie 2011-04-18

A cross site scripting attack is a very specific type of attack on a web application. It is used by hackers to mimic real sites and fool people into providing personal data. XSS Attacks starts by defining the terms and laying out the ground work. It assumes that the reader is familiar with basic web programming (HTML) and JavaScript. First it discusses the concepts, methodology, and technology that makes XSS a valid concern. It then moves into the various types of XSS attacks, how they are implemented, used, and abused. After XSS is thoroughly explored, the next part provides examples of XSS malware and demonstrates real cases where XSS is a dangerous risk that exposes internet users to remote access, sensitive data theft, and monetary losses. Finally, the book closes by examining the ways developers can avoid XSS vulnerabilities in their web applications, and how users can avoid becoming a victim. The audience is web developers, security practitioners, and managers. XSS Vulnerabilities exist in 8 out of 10 Web sites The authors of this book are the undisputed industry leading authorities Contains independent, bleeding edge research, code listings and exploits that can not be found anywhere else

SQL Server Forensic Analysis - Kevvie Fowler 2009

The tools and techniques investigators need to conduct crucial forensic investigations in SQL Server. • • The database is the part of a forensic investigation that companies are the most concerned about. This book provides data and tools needed to avoid under or over reporting. • Teaches many about aspects about SQL server that are not widely known. • A complete tutorial to conducting SQL Server investigations and using that knowledge to confirm, assess, and investigate a digital intrusion. Companies today are in a terrible bind: They must report all possible data security breaches, but they don't always know if, in a given breech, data has been compromised. As a result, most companies are releasing information to the public about every system breech or attempted system breech they know about. This reporting, in turn, whips up public hysteria and makes many companies look bad. Kevvie Fowler's 'SQL Server Forensic Analysis' is an attempt to calm everyone down and focuses on a key, under-documented component of today's forensics investigations. The book will help investigators determine if a breech was attempted, if information on the database server was compromised in any way, and if any rootkits have been installed that can compromise sensitive data in the future. Readers will learn how to prioritize, acquire, and analyze database evidence using forensically sound practices and free industry tools. The final chapter will include a case study that demonstrates all the techniques from the book applied in a walk-through of a real-world investigation.

The Web Application Hacker's Handbook - Dafydd Stuttard 2011-03-16

This book is a practical guide to discovering and exploiting security flaws in web applications. The authors explain each category of vulnerability using real-world examples, screen shots and code extracts. The book is extremely practical in focus, and describes in detail the steps involved in detecting and exploiting each kind of security weakness found within a variety of applications such as online banking, e-commerce and other web applications. The topics covered include bypassing login mechanisms, injecting code, exploiting logic flaws and compromising other users. Because every web application is different, attacking them entails bringing to bear various general principles, techniques and experience in an imaginative way. The most successful hackers go beyond this, and find ways to automate their bespoke attacks. This handbook describes a proven methodology that combines the virtues of human intelligence and computerized brute force, often with devastating results. The authors are professional penetration testers who have been involved in web application security for nearly a decade. They have presented training courses at the Black Hat security conferences throughout the world. Under the alias "PortSwigger", Dafydd developed the popular Burp Suite of web application hack tools.

Moving Target Defense - Sushil Jajodia 2011-08-26

Moving Target Defense: Creating Asymmetric

Uncertainty for Cyber Threats was developed by a group of leading researchers. It describes the fundamental challenges facing the research community and identifies new promising solution paths. Moving Target Defense which is motivated by the asymmetric costs borne by cyber defenders takes an advantage afforded to attackers and reverses it to advantage defenders. Moving Target Defense is enabled by technical trends in recent years, including virtualization and workload migration on commodity systems, widespread and redundant network connectivity, instruction set and address space layout randomization, just-in-time compilers, among other techniques. However, many challenging research problems remain to be solved, such as the security of virtualization infrastructures, secure and resilient techniques to move systems within a virtualized environment, automatic diversification techniques, automated ways to dynamically change and manage the configurations of systems and networks, quantification of security improvement, potential degradation and more. Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats is designed for advanced -level students and researchers focused on computer science, and as a secondary text book or reference. Professionals working in this field will also find this book valuable.

Understanding Network Hacks - Bastian Ballmann 2021-02-02

This book explains how to see one's own network through the eyes of an attacker, to understand their techniques and effectively protect against them. Through Python code samples the reader learns to code tools on subjects such as password sniffing, ARP poisoning, DNS spoofing, SQL injection, Google harvesting, Bluetooth and Wifi hacking. Furthermore the reader will be introduced to defense methods such as intrusion detection and prevention systems and log file analysis by diving into code.

SQL Injection Attacks and Defense - Justin Clarke-Salt 2009-05-05

Winner of the Best Book Bejtlich Read in 2009 award! "SQL injection is probably the number one problem for any server-side application, and this book is unequaled in its coverage." Richard Bejtlich, http://taosecurity.blogspot.com/ SQL injection represents one of the most dangerous and well-known, yet misunderstood, security vulnerabilities on the Internet, largely because there is no central repository of information to turn to for help. This is the only book devoted exclusively to this long-established but recently growing threat. It includes all the currently known information about these attacks and significant insight from its contributing team of SQL injection experts. What is SQL injection?- Understand what it is and how it works Find, confirm, and automate SQL injection discovery Discover tips and tricks for finding SQL injection within the code Create exploits using SQL injection Design to avoid the dangers of these attacks

SQL Injection Defenses - Martin Nystrom 2007-03-22

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.

Securing SQL Server - Peter A. Carter 2018-11-14

Protect your data from attack by using SQL Server technologies to implement a defense-in-depth strategy for your database enterprise. This new edition covers threat analysis, common attacks and countermeasures, and provides an introduction to compliance that is useful for meeting regulatory requirements such as the GDPR. The multi-layered approach in this book helps ensure that a single breach does not lead to loss or compromise of confidential, or business sensitive data. Database professionals in today’s world deal increasingly with repeated data attacks against high-profile organizations and sensitive data. It is more important than ever to keep your company’s data secure.

Securing SQL Server demonstrates how developers, administrators and architects can all play their part in the protection of their company’s SQL Server enterprise. This book not only provides a comprehensive guide to implementing the security model in SQL Server, including coverage of technologies such as Always Encrypted, Dynamic Data Masking, and Row Level Security, but also looks at common forms of attack against databases, such as SQL Injection and backup theft, with clear, concise examples of how to implement countermeasures against these specific scenarios. Most importantly, this book gives practical advice and engaging examples of how to defend your data, and ultimately your job, against attack and compromise. What You'll LearnPerform threat analysis Implement access level control and data encryption Avoid non-reputability by implementing comprehensive auditing Use security metadata to ensure your security policies are enforced Mitigate the risk of credentials being stolen Put countermeasures in place against common forms of attack Who This Book Is For Database administrators who need to understand and counteract the threat of attacks against their company’s data, and useful for SQL developers and architects

Essential SQLAlchemy - Rick Copeland 2008-06-05

Essential SQLAlchemy introduces a high-level open-source code library that makes it easier for Python programmers to access relational databases such as Oracle, DB2, MySQL, PostgreSQL, and SQLite. SQLAlchemy has become increasingly popular since its release, but it still lacks good offline documentation. This practical book fills the gap, and because a developer wrote it, you get an objective look at SQLAlchemy's tools rather than an advocate's description of all the "cool" features. SQLAlchemy includes both a database server-independent SQL expression language and an object-relational mapper (ORM) that lets you map "plain old Python objects" (POPOs) to database tables without substantially changing your existing Python code. Essential SQLAlchemy demonstrates how to use the library to create a simple database application, walks you through simple queries, and explains how to use SQLAlchemy to connect to multiple databases simultaneously with the same Metadata. You also learn how to: Create custom types to be used in your schema, and when it's useful to use custom rather than built-in types Run queries, updates, and deletes with SQLAlchemy's SQL expression language Build an object mapper with SQLAlchemy, and understand the differences between this and active record patterns used in other ORMs Create objects, save them to a session, and flush them to the database Use SQLAlchemy to model object oriented inheritance Provide a declarative, active record pattern for use with SQLAlchemy using the Elixir extension Use the SQLSoup extension to provide an automatic metadata and object model based on database reflection In addition, you'll learn how and when to use other extensions to SQLAlchemy, including AssociationProxy, OrderingList, and more. Essential SQLAlchemy is the much-needed guide for every Python developer using this code library. Instead of a feature-by-feature documentation, this book takes an "essentials" approach that gives you exactly what you need to become productive with SQLAlchemy right away.

Advanced Computing, Networking and Security - P. Santhi Thilagam 2012-04-02

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.

Learn Ethical Hacking from Scratch - Zaid Sabih 2018-07-31

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.

Beginning Ethical Hacking with Kali Linux - Sanjib Sinha 2018-11-29

Get started in white-hat ethical hacking using Kali Linux. This book starts off by giving you an overview of security trends, where you will learn the OSI security architecture. This will form the foundation for the rest of Beginning Ethical Hacking with Kali Linux. With the theory out of the way, you'll move on to an introduction to VirtualBox, networking, and common Linux commands, followed by the step-by-step procedure to build your own web server and acquire the skill to be anonymous . When you have finished the examples in the first part of your book, you will have all you need to carry out safe and ethical hacking experiments. After an introduction to Kali Linux, you will carry out your first penetration tests with Python and code raw binary packets for use in those tests. You will learn how to find secret directories on a target system, use a TCP client in Python, and scan ports using NMAP. Along the way you will discover effective ways to collect important information, track email, and use important tools such as DMITRY and Maltego, as well as take a look at the five phases of penetration testing. The coverage of vulnerability analysis includes sniffing and spoofing, why ARP poisoning is a threat, how SniffJoke prevents poisoning, how to analyze protocols with Wireshark, and using sniffing packets with Scapy. The next part of the book shows you detecting SQL injection vulnerabilities, using sqlmap, and applying brute force or password attacks. Besides learning these tools, you will see how to use OpenVas, Nikto, Vega, and Burp Suite. The book will explain the information assurance model and the hacking framework Metasploit, taking you through important commands, exploit and payload basics. Moving on to hashes and passwords you will learn password testing and hacking techniques with John the Ripper and Rainbow. You will then dive into classic and modern encryption techniques where you will learn the conventional cryptosystem. In the final chapter you will acquire the skill of exploiting remote Windows and Linux systems and you will learn how to own a target completely. What You Will LearnMaster common Linux commands and networking techniques Build your own Kali web server and learn to be anonymous Carry out penetration testing using Python Detect sniffing attacks and SQL injection vulnerabilities Learn tools such as SniffJoke, Wireshark, Scapy, sqlmap, OpenVas, Nikto, and Burp Suite Use Metasploit with Kali Linux Exploit remote Windows and Linux systemsWho This Book Is For Developers new to ethical hacking with a basic understanding of Linux programming.

SQL Injection Attacks and Defense - Justin Clarke 2012-06-18

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.

The Basics of Web Hacking - Josh Pauli 2013-06-18

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