Read free Advanced web attacks and exploitation (2023)

Web Hacking Attacking and Exploiting Modern Web Applications Seven Deadliest Web Application Attacks How to Break Web Software Hacking Web Apps The Web Application Hacker's Handbook Web Application Defender's Cookbook Preventing Web Attacks with Apache The Basics of Web Hacking Cross-Site Scripting Attacks Web Application Security XSS Attacks The Web Application Hacker's Handbook Web Security for Developers Attack and Defend Computer Security Set Hacking Exposed How to Attack and Defend Your Website Web Application Obfuscation Secure Your Node.js Web Application Using Security Patterns in Web-Application Safety of Web Applications Web Security Portable Reference Primer on Client-Side Web Security Hacking Exposed Web 2.0: Web 2.0 Security Secrets and Solutions SQL injection attacks and mitigations Web Application Security, A Beginner's Guide Developer's Guide to Web Application Security Hacking Exposed Web Applications, Third Edition The Official CHFI Study Guide (Exam 312-49) Web Penetration Testing with Kali Linux Hacking Exposed Web Applications, Second Edition Web Security Web Application Vulnerabilities Mastering Modern Web Penetration Testing Alibaba Cloud□□□□□□□□□□□□□□ Understanding Network Hacks Innocent Code SQL Injection Attacks and Defense Improving Web Application Security Web Penetration Testing with Kali Linux

Web Hacking 2003 the presidentâe tm s life is in danger jimmy sniffles with the help of a new invention shrinks down to miniature size to sniff out the source of the problem

Attacking and Exploiting Modern Web Applications 2023-08-25 master the art of web exploitation with real world techniques on saml wordpress iot electronjs and ethereum smart contracts purchase of the print or kindle book includes a free pdf ebook key features learn how to detect vulnerabilities using source code dynamic analysis and decompiling binaries find and exploit vulnerabilities such as sql injection xss command injection rce and reentrancy analyze real world security incidents based on mitre att ck to understand the risk at the ciso level book descriptionattacks and exploits pose an ongoing threat to the interconnected world this comprehensive book explores the latest challenges in web application security providing you with an in depth understanding of hackers methods and the practical knowledge and skills needed to effectively understand web attacks the book starts by emphasizing the importance of mindset and toolset in conducting successful web attacks you ll then explore the methodologies and frameworks used in these attacks and learn how to configure the environment using interception proxies automate tasks with bash and python and set up a research lab as you advance through the book you ll discover how to attack the saml authentication layer attack front facing web applications by learning wordpress and sql injection and exploit vulnerabilities in iot devices such as command injection by going through three ctfs and learning about the discovery of seven cves each chapter analyzes confirmed cases of exploitation mapped with mitre att ck you ll also analyze attacks on electron javascript based applications such as xss and rce and the security challenges of auditing and exploiting ethereum smart contracts written in solidity finally you ll find out how to disclose vulnerabilities by the end of this book you ll have enhanced your ability to find and exploit web vulnerabilities what you will learn understand the mindset methodologies and toolset needed to carry out web attacks discover how saml and sso work and study their vulnerabilities get to grips with wordpress and learn how to exploit sql injection find out how iot devices work and exploit command injection familiarize yourself with electronjs applications and transform an xss to an rce discover how to audit solidity s ethereum smart contracts get the hang of decompiling debugging and instrumenting web applications who this book is for this book is for anyone whose job role involves ensuring their organization s security penetration testers and red teamers who want to deepen their knowledge of the current security challenges for web applications developers and devops professionals who want to get into the mindset of an attacker and security managers and cisos looking to truly understand the impact and risk of web iot and smart contracts basic knowledge of web technologies as well as related protocols is a must

Seven Deadliest Web Application Attacks 2010-02-20 seven deadliest 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 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

How to Break Web Software 2006-02-02 rigorously test and improve the security of all your software it s as certain as death and taxes hackers will mercilessly attack your sites applications and services if you re vulnerable you d better discover these attacks yourself before the black hats do now there s a definitive hands on guide to security testing any based software how to break software in this book two renowned experts address every category of software exploit attacks on clients servers state user inputs and more you ll master powerful attack tools and techniques as you uncover dozens of crucial widely exploited flaws in architecture and coding the authors reveal where to look for potential threats and attack vectors how to rigorously test for each of them and how to mitigate the problems you find coverage includes client vulnerabilities including attacks on client side validation state based attacks hidden fields cgi parameters cookie poisoning url jumping and session hijacking attacks on user supplied inputs cross site scripting sql injection and directory traversal language and technology based attacks buffer overflows canonicalization and null string attacks server attacks sql injection with stored procedures command injection and server fingerprinting cryptography privacy and attacks on services your software is mission critical it can t be compromised whether you re a developer tester qa specialist or it manager this book will help you protect that software systematically

Hacking Web Apps 2012-08-29 html5 html injection cross site scripting xss cross site request forgery csrf sql injection data store manipulation breaking authentication schemes abusing design deficiencies leveraging platform weaknesses browser privacy attacks

The Web Application Hacker's Handbook 2011-08-31 the highly successful security book returns with a new edition completely updated applications are the front door to most organizations exposing them to attacks that may disclose personal information execute fraudulent transactions or compromise ordinary users this practical book has been completely updated and revised to discuss the latest step by step techniques for attacking and defending the range of ever evolving web applications you ll explore the various new technologies employed in web applications that have appeared since the first edition and review the new attack techniques that have been developed particularly in relation to the client side reveals how to overcome the new technologies and techniques aimed at defending web applications against attacks that have appeared since the previous edition discusses new remoting frameworks html5 cross domain integration techniques ui redress framebusting http parameter pollution hybrid file attacks and more features a companion web site hosted by the authors that allows readers to try out the attacks described gives answers to the questions that are posed at the end of each chapter and provides a summarized methodology and checklist of tasks focusing on the areas of web application security where things have changed in recent years this book is the most current resource on the critical topic of discovering exploiting and preventing web application security flaws

Web Application Defender's Cookbook 2013-01-04 defending your web applications against hackers and attackers the top selling book application hacker s handbook showed how attackers and hackers identify and attack vulnerable live web applications this new application defender s cookbook is the perfect counterpoint to that book it shows you how to defend authored by a highly credentialed defensive security expert this new book details defensive security methods and can be used as courseware for training network security personnel web server administrators and security consultants each recipe shows you a way to detect and defend against malicious behavior and provides working code examples for the modsecurity web application firewall module topics include identifying vulnerabilities setting hacker traps defending different access points enforcing application flows and much more provides practical tactics for detecting web attacks and malicious behavior and defending against them written by a preeminent authority on web application firewall technology and web application defense tactics offers a series of recipes that include working code examples for the open source modsecurity web application firewall module find the tools techniques and expert information you need to detect and respond to web application attacks with application defender s cookbook battling hackers and protecting users

Preventing Web Attacks with Apache 2006-01-27 the only end to end guide to securing apache servers and applications apache can be hacked as companies have improved perimeter security hackers have increasingly focused on attacking apache servers and applications firewalls and ssl won t protect you you must systematically harden your application environment preventing attacks with apache brings together all the information you ll need to do that step by step guidance hands on examples and tested configuration files building on his groundbreaking sans presentations on apache security ryan c barnett reveals why your servers represent such a compelling target how significant exploits are performed and how they can be defended against exploits discussed include buffer overflows denial of service attacks on vulnerable scripts and programs credential sniffing and spoofing client parameter manipulation brute force attacks web defacements and more barnett introduces the center for internet security apache benchmarks a set of best practice apache security configuration actions and settings he helped to create he addresses issues related to it processes and your underlying os apache downloading installation and configuration application hardening monitoring and more he also presents a chapter length case study using actual attack logs and data captured in the wild for every sysadmin professional and security specialist responsible for apache or application security

The Basics of Web Hacking 2013-06-18 the basics of hacking introduces you to a tool driven process to identify the most widespread vulnerabilities in applications no prior experience is needed 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 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 security including hacking the server hacking the app and hacking the user with dr pauli s approach you will fully understand the what where why how of the most widespread 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 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

exploits you will also be prepared to conduct more advanced hacks that mandate a strong base of knowledge provides a simple and clean approach to hacking including hands on examples and exercises that are designed to teach you how to hack the server hack the app and hack the 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 security classes at dakota state university

Cross-Site Scripting Attacks 2020-02-25 social network usage has increased exponentially in recent years platforms like facebook twitter google linkedin and instagram not only facilitate sharing of personal data but also connect people professionally however development of these platforms with more enhanced features like html5 css xhtml and java script expose these sites to various vulnerabilities that may be the root cause of various threats therefore social networking sites have become an attack surface for various cyber attacks such as xss attack and sql injection numerous defensive techniques have been proposed yet with technology up gradation current scenarios demand for more efficient and robust solutions cross site scripting attacks classification attack and countermeasures is a comprehensive source which provides an overview of web based vulnerabilities and explores xss attack in detail this book provides a detailed overview of the xss attack its classification recent incidences on various web applications and impacts of the xss attack on the target victim this book addresses the main contributions of various researchers in xss domain it provides in depth analysis of these methods along with their comparative study the main focus is a novel framework which is based on clustering and context based sanitization approach to protect against xss attack on social network the implementation details conclude that it is an effective technique to thwart xss attack the open challenges and future research direction discussed in this book will help further to the academic researchers and industry specific persons in the domain of security

Web Application Security 2024-01-17 in the first edition of this critically acclaimed book andrew hoffman defined the three pillars of application security reconnaissance offense and defense in this revised and updated second edition he examines dozens of related topics from the latest types of attacks and mitigations to threat modeling the secure software development lifecycle ssdl sdlc and more hoffman senior staff security engineer at ripple also provides information regarding exploits and mitigations for several additional web application technologies such as graphql cloud based deployments content delivery networks cdn and server side rendering ssr following the curriculum from the first book this second edition is split into three distinct pillars comprising three separate skill sets pillar 1 recon learn techniques for mapping and documenting web applications remotely including procedures for working with web applications pillar 2 offense explore methods for attacking web applications using a number of highly effective exploits that have been proven by the best hackers in the world these skills are valuable when used alongside the skills from pillar 3 pillar 3 defense build on skills acquired in the first two parts to construct effective and long lived mitigations for each of the attacks described in pillar 2

XSS Attacks 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 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

The Web Application Hacker's Handbook 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

Web Security for Developers 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 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

Attack and Defend Computer Security Set 2014-03-17 defend your networks and data from attack with this unique two book security set the attack and defend computer security set is a two book set comprised of the bestselling second edition of application hacker s handbook and malware analyst s cookbook this special security bundle combines coverage of the two most crucial tactics used to defend networks applications and data from attack while giving security professionals insight into the underlying details of these attacks themselves the application hacker s handbook takes a broad look at web application security and exposes the steps a hacker can take to attack an application while providing information on how the application can defend itself fully updated for the latest security trends and threats this guide covers remoting frameworks html5 and cross domain integration techniques along with clickjacking framebusting http parameter pollution xml external entity injection hybrid file attacks and more the malware analyst s cookbook includes a book and dvd and is designed to enhance the analytical capabilities of anyone who works with malware whether you re tracking a trojan across networks performing an in depth binary analysis or inspecting a machine for potential infections the recipes in this book will help you go beyond the basic tools for tackling security challenges to cover how to extend your favorite tools or build your own from scratch using c python and perl source code the companion dvd features all the files needed to work through the recipes in the book and to complete reverse engineering challenges along the way the attack and defend computer security set gives your organization the security tools needed to sound the alarm and stand your ground against malicious threats lurking online

Hacking Exposed 2002 featuring in depth coverage of the technology platforms surrounding applications and attacks this guide has specific case studies in the popular hacking exposed format

How to Attack and Defend Your Website 2014-12-05 how to attack and defend your website is a concise introduction to web security that includes hands on web hacking tutorials the book has three primary objectives to help readers develop a deep understanding of what is happening behind the scenes in a web application with a focus on the http protocol and other underlying web technologies to teach readers how to use the industry standard in free web application vulnerability discovery and exploitation tools most notably burp suite a fully featured web application testing tool and finally to gain knowledge of finding and exploiting the most common web security vulnerabilities this book is for information security professionals and those looking to learn general penetration testing methodology and how to use the various phases of penetration testing to identify and exploit common web protocols how to attack and defend your website is be the first book to combine the methodology behind using penetration testing tools such as burp suite and damn vulnerable application dvwa with practical exercises that show readers how to and therefore how to prevent pwning with sqlmap and using stored xss to deface web pages learn the basics of penetration testing so that you can test your own website s integrity and security discover useful tools such as burp suite dvwa and sqlmap gain a deeper understanding of how your website works and how best to protect it

Web Application Obfuscation 2010-12-10 applications are used every day by millions of users which is why they are one of the most popular vectors for attackers obfuscation of code has allowed hackers to take one attack and create hundreds if not millions of variants that can evade your security measures application obfuscation takes a look at common infrastructure and security controls from an attacker s perspective allowing the reader to understand the shortcomings of their security systems find out how an attacker would bypass different types of security controls how these very security controls introduce new types of vulnerabilities and how to avoid common pitfalls in order to strengthen your defenses named a 2011 best hacking and pen testing book by infosec reviews looks at security tools like ids ips that are often the only defense in protecting sensitive data and assets evaluates application vulnerabilties from the attacker s perspective and explains how these very systems introduce new types of vulnerabilities teaches how to secure your data including info on browser quirks new attacks and syntax tricks to add to your defenses against xss sql injection and more

Secure Your Node.js Web Application 2015-12-28 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 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

Using Security Patterns in Web-Application 2014-04-01 application have been widely accepted by the organization be it in private public or government sector and form the main part of any e commerce business on the internet however with the widespread of web application the threats related to the web application have also emerged application transmit substantial amount of critical data such as password or credit card information etc and this data should be protected from an attacker there has been huge number of attacks on the web application such as sql injection cross site scripting http response splitting in recent years and it is one of the main concerns in both the software developer and security professional community this projects aims to explore how security can be incorporated by using security pattern in web application and how effective it is in addressing the security problems of web application

Safety of Web Applications 2017-04-11 safety of applications risks encryption and handling vulnerabilities with php explores many areas that can help computer science students and developers integrate security into their applications the internet is not secure but it s very friendly as a tool for storing and manipulating data customer confidence in internet software is based on it s ability to prevent damage and attacks but secure software is complicated depending on several factors including good risk estimation good code architecture cyphering web server configuration coding to prevent the most common attacks and identification and rights allocation helps computer science students and developers integrate security into their applications includes sections on risk estimate mvc modeling the cyphering certificates bi keys protocol

Web Security Portable Reference 2003 describes how hackers break into applications what function areas are vulnerable and how to guard against attacks

Primer on Client-Side Web Security 2014-11-25 this volume illustrates the continuous arms race between attackers and defenders of the ecosystem by discussing a wide variety of attacks in the first part of the book the foundation of the ecosystem is briefly recapped and discussed based on this model the assets of the ecosystem are identified and the set of capabilities an attacker may have are enumerated in the second part an overview of the web security vulnerability landscape is constructed included are selections of the most representative attack techniques reported in great detail in addition to descriptions of the most common mitigation techniques this primer also surveys the research and standardization activities related to each of the attack techniques and gives insights into the prevalence of those very attacks moreover the book provides practitioners a set of best practices to gradually improve the security of their web enabled services primer on client side security expresses insights into the future of web application security it points out the challenges of securing the platform opportunities for future research and trends toward improving security

Hacking Exposed Web 2.0: Web 2.0 Security Secrets and Solutions 2008-01-07 lock down next generation services this book concisely identifies the types of attacks which are faced daily by 2 0 sites and the authors give solid practical advice on how to identify and mitigate these threats max kelly cissp cipp cfce senior director of security facebook protect your 2 0 architecture against the latest wave of cybercrime using expert tactics from internet security professionals hacking exposed 2 0 shows how hackers perform reconnaissance choose their entry point and attack 2 0 based services and reveals detailed countermeasures and defense techniques you ll learn how to avoid injection and buffer overflow attacks fix browser and plug in flaws and secure ajax flash and xml driven applications real world case studies illustrate social networking site weaknesses cross site attack methods migration vulnerabilities and ie7 shortcomings plug security holes in 2 0 implementations the proven hacking exposed way learn how hackers target and abuse vulnerable 2 0 applications browsers plug ins online databases user inputs and html forms prevent 2 0 based sql xpath xquery ldap and command injection attacks

circumvent xxe directory traversal and buffer overflow exploits learn xss and cross site request forgery methods attackers use to bypass browser security controls fix vulnerabilities in outlook express and acrobat reader add ons use input validators and xml classes to reinforce asp and net security eliminate unintentional exposures in asp net ajax atlas direct remoting sajax and gwt applications mitigate activex security exposures using sitelock code signing and secure controls find and fix adobe flash vulnerabilities and dns rebinding attacks

SQL injection attacks and mitigations 2019-05-23 project report from the year 2018 in the subject computer science applied grade 3 91 4 language english abstract structured query language injection is one of the vulnerabilities in oswap top 10 list for web based application exploitation in this study we will be demonstrating the different methods of sql injection attacks and prevention techniques will be illustrated application are widespread as they have become the necessity for the everyday life most web based applications communicate with a database using a machine understandable language called structured query language sql sql injection is a code injection technique used to attack data driven applications in which malicious sql statements are inserted from the client of the application

Web Application Security, A Beginner's Guide 2011-12-06 security smarts for the self guided it professional get to know the hackers or plan on getting hacked sullivan and liu have created a savvy essentials based approach to web app security packed with immediately applicable tools for any information security practitioner sharpening his or her tools or just starting out ryan mcgeehan security manager facebook inc secure web applications from today s most devious hackers application security a beginner s guide helps you stock your security toolkit prevent common hacks and defend quickly against malicious attacks this practical resource includes chapters on authentication authorization and session management along with browser database and file security all supported by true stories from industry you ll also get best practices for vulnerability detection and secure development as well as a chapter that covers essential security fundamentals this book s templates checklists and examples are designed to help you get started right away application security a beginner s guide features lingo common security terms defined so that you re in the know on the job imho frank and relevant opinions based on the authors years of industry experience budget note tips for getting security technologies and processes into your organization s budget in actual practice exceptions to the rules of security explained in real world contexts your plan customizable checklists you can use on the job now into action tips on how why and when to apply new skills and techniques at work

Developer's Guide to Web Application Security 2011-04-18 over 75 of network attacks are targeted at the web application layer this book provides explicit hacks tutorials penetration tests and step by step demonstrations for security professionals and application developers to defend their most vulnerable applications this book defines application security why it should be addressed earlier in the lifecycle in development and quality assurance and how it differs from other types of internet security additionally the book examines the procedures and technologies that are essential to developing penetration testing and releasing a secure application through a review of recent application breaches the book will expose the prolific methods hackers use to execute attacks using common vulnerabilities such as sql injection cross site scripting and buffer overflows in the application layer by taking an in depth look at the techniques hackers use to exploit applications readers will be better equipped to protect confidential the yankee group estimates the market for application security products and services will grow to 1 74 billion by 2007 from 140 million in 2002 author michael cross is a highly sought after speaker who regularly delivers application presentations at leading conferences including black hat technosecurity cansec west shmoo con information security rsa conferences and more

Hacking Exposed Web Applications, Third Edition 2010-10-22 the latest app attacks and countermeasures from world renowned practitioners protect your applications from malicious attacks by mastering the weapons and thought processes of today s hacker written by recognized security practitioners and thought leaders hacking exposed applications third edition is fully updated to cover new infiltration methods and countermeasures find out how to reinforce authentication and authorization plug holes in firefox and ie reinforce against injection attacks and secure 2 0 features integrating security into the development lifecycle sdl and into the broader enterprise information security program is also covered in this comprehensive resource get full details on the hacker s footprinting scanning and profiling tools including shodan maltego and owasp dirbuster see new exploits of popular platforms like sun java system server and oracle weblogic in operation understand how attackers defeat commonly used authentication technologies see how real world session attacks leak sensitive data and how to fortify your applications learn the most devastating methods used in today s hacks including sql injection xss xsrf phishing and xml injection techniques find and fix vulnerabilities in asp net php and j2ee execution environments safety deploy xml social networking cloud computing and 2 0 services defend against ria ajax ugc and browser based client side exploits implement scalable threat modeling code review application scanning fuzzing and security testing procedures

The Official CHFI Study Guide (Exam 312-49) 2011-08-31 this is the official chfi computer hacking forensics investigator study guide for professionals studying for the forensics exams and for professionals needing the skills to identify an intruder s footprints and properly gather the necessary evidence to prosecute the ec council offers certification for ethical hacking and

computer forensics their ethical hacker exam has become very popular as an industry gauge and we expect the forensics exam to follow suit material is presented in a logical learning sequence a section builds upon previous sections and a chapter on previous chapters all concepts simple and complex are defined and explained when they appear for the first time this book includes exam objectives covered in a chapter are clearly explained in the beginning of the chapter notes and alerts highlight crucial points exam s eye view emphasizes the important points from the exam s perspective key terms present definitions of key terms used in the chapter review questions contains the questions modeled after real exam questions based on the material covered in the chapter answers to the questions are presented with explanations also included is a full practice exam modeled after the real exam the only study guide for chfi provides 100 coverage of all exam objectives chfi training runs hundreds of dollars for self tests to thousands of dollars for classroom training

Web Penetration Testing with Kali Linux 2015-11-26 build your defense against web attacks with kali linux 2 0 about this book gain a deep understanding of the flaws in web applications and exploit them in a practical manner get hands on web application hacking experience with a range of tools in kali linux 2 0 develop the practical skills required to master multiple tools in the kali linux 2 0 toolkit who this book is for if you are already working as a network penetration tester and want to expand your knowledge of web application hacking then this book tailored for you those who are interested in learning more about the kali sana tools that are used to test web applications will find this book a thoroughly useful and interesting guide what you will learn set up your lab with kali linux 2 0 identify the difference between hacking a web application and network hacking understand the different techniques used to identify the flavor of web applications expose vulnerabilities present in web servers and their applications using server side attacks use sql and cross site scripting xss attacks check for xss flaws using the burp suite proxy find out about the mitigation techniques used to negate the effects of the injection and blind sql attacks in detail kali linux 2 0 is the new generation of the industry leading backtrack linux penetration testing and security auditing linux distribution it contains several hundred tools aimed at various information security tasks such as penetration testing forensics and reverse engineering at the beginning of the book you will be introduced to the concepts of hacking and penetration testing and will get to know about the tools used in kali linux 2 0 that relate to web application hacking then you will gain a deep understanding of sql and command injection flaws and ways to exploit the flaws moving on you will get to know more about scripting and input validation flaws ajax and the security issues related to ajax at the end of the book you will use an automated technique called fuzzing to be able to identify flaws in a web application finally you will understand the web application vulnerabilities and the ways in which they can be exploited using the tools in kali linux 2 0 style and approach this step by step guide covers each topic with detailed practical examples every concept is explained with the help of illustrations using the tools available in kali linux 2 0

Hacking Exposed Web Applications, Second Edition 2006-06-05 implement bulletproof e business security the proven hacking exposed way defend against the latest based attacks by looking at your applications through the eyes of a malicious intruder fully revised and updated to cover the latest exploitation techniques hacking exposed applications second edition shows you step by step how cyber criminals target vulnerable sites gain access steal critical data and execute devastating attacks all of the cutting edge threats and vulnerabilities are covered in full detail alongside real world examples case studies and battle tested countermeasures from the authors experiences as gray hat security professionals find out how hackers use infrastructure and application profiling to perform reconnaissance and enter vulnerable systems get details on exploits evasion techniques and countermeasures for the most popular platforms including iis apache php and asp net learn the strengths and weaknesses of common authentication mechanisms including password based multifactor and single sign on mechanisms like passport see how to excise the heart of any application s access controls through advanced session analysis hijacking and fixation techniques find and fix input validation flaws including cross site scripting xss sql injection http response splitting encoding and special character abuse get an in depth presentation of the newest sql injection techniques including blind attacks advanced exploitation through subqueries oracle exploits and improved countermeasures learn about the latest xml services hacks management attacks and ddos attacks including click fraud tour firefox and ie exploits as well as the newest socially driven client attacks like phishing and adware

Web Security 2015-04-06 in late 2013 approximately 40 million customer debit and credit cards were leaked in a data breach at target this catastrophic event deemed one of the biggest data breaches ever clearly showed that many companies need to significantly improve their information security strategies security a white hat perspective presents a comprehensive guide to web security technology and explains how companies can build a highly effective and sustainable security system in this book web security expert wu hanqing reveals how hackers work and explains why companies of different scale require different security methodologies with in depth analysis of the reasons behind the choices the book covers client script security server applications security and internet company security operations it also includes coverage of browser security cross sites script attacks click jacking html5 php security injection attacks authentication session management access control web frame security ddos leaks internet transactions security

and the security development lifecycle
Web Application Vulnerabilities 2011-04-18 in this book we aim to describe how to make a computer bend to your will by finding and exploiting vulnerabilities specifically in applications we will describe common security issues in applications tell you how to find them describe how to exploit them and then tell you how to fix them we will also cover how and why some hackers the bad guys will try to exploit these vulnerabilities to achieve their own end we will also try to explain how to detect if hackers are actively trying to exploit vulnerabilities in your own applications learn to defend based applications developed with ajax soap xmlprc and more see why cross site scripting attacks can be so devastating
Mastering Modern Web Penetration Testing 2016-09-30 master the art of conducting modern pen testing attacks and techniques on your web application before the hacker does about this book this book covers the latest technologies such as advance xss xsrf sql injection evading wafs xml attack vectors oauth 2 0 security and more involved in today s web applications penetrate and secure your web application using various techniques get this comprehensive reference guide that provides advanced tricks and tools of the trade for seasoned penetration testers who this book is forthis book targets security professionals and penetration testers who want to speed up their modern web application penetrating testing it will also benefit intermediate level readers and web developers who need to be aware of the latest application hacking techniques what you will learn get to know the new and less publicized techniques such php object injection and xml based vectors work with different security tools to automate most of the redundant tasks see different kinds of newly designed security headers and see how they help to provide security exploit and detect different kinds of xss vulnerabilities protect your web application using filtering mechanisms understand old school and classic web hacking in depth using sql injection xss and csrf grasp xml related vulnerabilities and attack vectors such as xxe and dos using billon laughs quadratic blow up in detailpenetration testing is a growing fast moving and absolutely critical field in information security this book executes modern web application attacks and utilises cutting edge hacking techniques with an enhanced knowledge of web application security we will cover web hacking techniques so you can explore the attack vectors during penetration tests the book encompasses the latest technologies such as oauth 2 0 evading wafs and xml vectors used by hackers we ll explain various old school techniques in depth such as sql injection through the ever dependable sqlmap this pragmatic guide will be a great benefit and will help you prepare fully secure applications
Alibaba Cloud[illegible] 2019-09-23 [illegible] 1[illegible] 3[illegible] iaas [illegible] iot[illegible] alibaba cloud[illegible]
Understanding Network Hacks 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
Innocent Code 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 site construction to site destruction in order to find dangerous code
SQL Injection Attacks and Defense 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
Improving Web Application Security 2003 gain a solid foundation for designing building and configuring security enhanced hack resistant microsoft asp net applications this expert guide describes a systematic task based approach to security that can be applied to both new and existing applications it addresses security considerations at the network host and application layers for each physical tier server remote application server and database server detailing the security configurations and countermeasures that can help mitigate risks the information is organized into sections that correspond to both the product life cycle and the roles involved making it easy for architects designers and developers to find the answers they need all patterns practices guides are reviewed and approved by microsoft engineering teams consultants partners and customers delivering accurate real world information that s been technically validated and tested
Web Penetration Testing with Kali Linux 2018-02-28 build your defense against web attacks with kali linux including command injection flaws crypto implementation layers and web application security holes key features know how to set up your lab with kali linux discover the core concepts of web penetration testing get the tools and techniques you need with kali linux book

description penetration testing with kali linux third edition shows you how to set up a lab helps you understand the nature and mechanics of attacking websites and explains classical attacks in great depth this edition is heavily updated for the latest kali linux changes and the most recent attacks kali linux shines when it comes to client side attacks and fuzzing in particular from the start of the book you ll be given a thorough grounding in the concepts of hacking and penetration testing and you ll see the tools used in kali linux that relate to web application hacking you ll gain a deep understanding of classicalsql command injection flaws and the many ways to exploit these flaws penetration testing also needs a general overview of client side attacks which is rounded out by a long discussion of scripting and input validation flaws there is also an important chapter on cryptographic implementation flaws where we discuss the most recent problems with cryptographic layers in the networking stack the importance of these attacks cannot be overstated and defending against them is relevant to most internet users and of course penetration testers at the end of the book you ll use an automated technique called fuzzing to identify flaws in a web application finally you ll gain an understanding of web application vulnerabilities and the ways they can be exploited using the tools in kali linux what you will learn learn how to set up your lab with kali linux understand the core concepts of web penetration testing get to know the tools and techniques you need to use with kali linux identify the difference between hacking a web application and network hacking expose vulnerabilities present in web servers and their applications using server side attacks understand the different techniques used to identify the flavor of web applications see standard attacks such as exploiting cross site request forgery and cross site scripting flaws get an overview of the art of client side attacks explore automated attacks such as fuzzing web applications who this book is for since this book sets out to cover a large number of tools and security fields it can work as an introduction to practical security skills for beginners in security in addition web programmers and also system administrators would benefit from this rigorous introduction to web penetration testing basic system administration skills are necessary and the ability to read code is a must

- viper alarm 7142v manual Full PDF
- the future of identity centennial reflections on the legacy of erik erikson (Read Only)
- public relations n5 question paper memorundums (Download Only)
- a decade of extrasolar planets around normal stars proceedings of the space telescope science institute symposium held in baltimore maryland may telescope science institute symposium series (Download Only)
- image compression neural network matlab code thesis (2023)
- soal dan jawaban materi teknik komputer dan jaringan (PDF)
- root shock how tearing up city neighborhoods hurts america and what we can do about it Full PDF
- ecotechnics home [PDF]
- free kia sportage repair manual Full PDF
- philips ultramark 4a ultrasound manual .pdf
- 1962 cessna 172 owners manual [PDF]
- new english fileupper intermediate german wordlist Full PDF
- concentration and molarity phet chemistry labs answers key Full PDF
- tractor manual dongfeng [PDF]
- change management a guide to effective implementation download (PDF)
- jim stoppanis 12 week shortcut to size jim stoppani Full PDF
- cannon oakley gas cooker manual .pdf
- electrical on site guide (PDF)
- the witnesses war crimes and the promise of justice in the hague pennsylvania studies in human rights (PDF)
- cornerstone of managerial accounting solution manual Copy
- shoprider cordoba manual (Download Only)
- the healing platform build your own cure (PDF)
- lloyds law reports professional negligence 2001 Copy
- operations management sustainability and supply chain management Full PDF