The New Owasp Web Application Penetration Testing Guide

The Tangled Web
The Web Application Hacker's Handbook
Effective Python Penetration Testing
Detect, Exploit, Prevent
Exploitation and Countermeasures for Modern Web Applications
Using Security Patterns in Web-Application
Innocent Code
The Manager's Guide to Web Application Security
Discovering and Exploiting Security Flaws
OWASP Top 10: the Top 10 Most Critical Web Application Security Threats
Web Application Defender's Cookbook
Enhanced with Text Analytics and Content by PageKicker Robot Phil 73
The Web Application Hacker's Handbook
Web Application Security
Hands-on Penetration Testing for Web Applications

Cross Site Scripting Exploits and Defense
Web Application Security - Simple Steps to Win, Insights and Opportunities for Maxing Out Success
An Expert Way of Secure Web Application Deployment
A Guide to Securing Modern Web Applications
Practical techniques to secure old vulnerabilities against modern attacks
Threats and Countermeasures
Testing and Securing Web Applications
SQL Injection Strategies
Web Application Security
Iron-Clad Java
Secure Java
Building Secure Web Applications
Finding and Exploiting Security Flaws
Web Security Testing Cookbook
Application Security - Simple Steps to Win, Insights and Opportunities for Maxing Out Success
Run Web Security Testing on Modern Applications Using Nmap, Burp Suite and Wireshark (English Edition)
Hacking Exposed Web Applications, Third Edition

Web Application Security is a Stack
Learning the OWASP Top 10
XSS Attacks
Security Strategies in Web Applications and Social Networking
Risks, Encryption and Handling Vulnerabilities with PHP
Web Application Security, A Beginner's Guide
-/WAFs..Evasion..Filters//alert (/Obfuscation/)-
Security Strategies in Web Applications and Social Networking

ALICIA PAMELA

The Tangled Web McGraw Hill Professional
Covers topics such as the importance of secure systems, threat modeling, canonical representation issues, solving database input, denial-of-service attacks, and security code reviews and checklists.
The Web Application Hacker's Handbook John Wiley & Sons
tl;dr: it's a scary world out there!
Welcome to the OWASP Top 10 2013! This update broadens one of the categories from the 2010 version to be more inclusive of common, important vulnerabilities, and reorders some of the others based on changing prevalence data. It also brings component security

into the spotlight by creating a specific category for this risk, pulling it out of the obscurity of the fine print of the 2010 risk A6: Security Misconfiguration. The OWASP Top 10 for 2013 is based on 8 datasets from 7 firms that specialize in application security, including 4 consulting companies and 3 tool/SaaS vendors (1 static, 1 dynamic, and 1 with both). This data spans over 500,000 vulnerabilities across hundreds of organizations and thousands of applications. The Top 10 items are selected and prioritized according to this prevalence data, in combination with consensus estimates of exploitability, detectability, and impact estimates. The primary aim of the OWASP Top 10 is to educate developers, designers, architects, managers, and organizations about the consequences of the most important web application security weaknesses. The Top 10 provides basic techniques to protect against these high risk problem areas - and also provides guidance on where to go from here. Copyright (c) 2003 - 2013 The OWASP Foundation This document is released under the Creative Commons Attribution ShareAlike 3.0 license. For any reuse or distribution, you must make it clear to others the license terms of this wor

Effective Python Penetration Testing

Pearson Education

Proven Methods for Building Secure Java-Based Web Applications Develop, deploy, and maintain secure Java applications using the expert techniques and open source libraries described in this Oracle Press guide. Iron-Clad Java

presents the processes required to build robust and secure applications from the start and explains how to eliminate existing security bugs. Best practices for authentication, access control, data protection, attack prevention, error handling, and much more are included. Using the practical advice and real-world examples provided in this authoritative resource, you'll gain valuable secure software engineering skills. Establish secure authentication and session management processes Implement a robust access control design for multi-tenant web applications Defend against cross-site scripting, cross-site request forgery, and clickjacking Protect sensitive data while it is stored or in transit Prevent SQL injection and other injection attacks Ensure safe file I/O and upload Use effective logging, error handling, and intrusion detection methods Follow a comprehensive secure software development lifecycle "In this book, Jim Manico and August Detlefsen tackle security education from a technical perspective and bring their wealth of industry knowledge and experience to application designers. A significant amount of thought was given to include the most useful and relevant security content for designers to defend their applications. This is not a book about security theories, it’s the hard lessons learned from those who have been exploited, turned into actionable items for application designers, and condensed into print."—From the Foreword by Milton Smith, Oracle Senior Principal Security Product Manager, Java

Detect, Exploit, Prevent Springer Science & Business Media
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
Exploitation and Countermeasures for Modern Web Applications Packt Publishing Ltd
Automated Threat HandbookLulu.comWeb Application

Security, A Beginner's GuideMcGraw Hill Professional

Using Security Patterns in Web-Application diplom.de

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

Innocent Code Elsevier

The highly successful security book returns with a new edition, completely updated Web 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. Also available as a set with, CEHv8: Certified Hacker Version 8 Study Guide, Ethical Hacking and Web Hacking Set, 9781119072171.

The Manager's Guide to Web Application Security John Wiley & Sons

Pen test your system like a pro and overcome vulnerabilities by leveraging Python scripts, libraries, and tools About This Book Learn to utilize your Python scripting skills to pentest a computer system, network, and web-application Get proficient at the art of assessing vulnerabilities by conducting effective penetration testing This is the ultimate guide that teaches you how to use Python to protect your systems against sophisticated cyber attacks Who This Book Is For This book is ideal for those

who are comfortable with Python or a similar language and need no help with basic programming concepts, but want to understand the basics of penetration testing and the problems pentesters face. What You Will Learn Write Scapy scripts to investigate network traffic Get to know application fingerprinting techniques with Python Understand the attack scripting techniques Write fuzzing tools with pentesting requirements Learn basic attack scripting methods Utilize cryptographic toolkits in Python Automate pentesting with Python tools and libraries In Detail Penetration testing is a practice of testing a computer system, network, or web application to find weaknesses in security that an attacker can exploit. Effective Python Penetration Testing will help you utilize your Python scripting skills to safeguard your networks from cyberattacks. We will begin by providing you with an overview of Python scripting and penetration testing. You will learn to analyze network traffic by writing Scapy scripts and will see how to fingerprint web applications with Python libraries such as ProxMon and Spynner. Moving on, you will find out how to write basic attack scripts, and will develop debugging and reverse engineering skills with Python libraries. Toward the end of the book, you will discover how to utilize cryptography toolkits in Python and how to automate Python tools and libraries. Style and approach This is an expert's guide to Python with a practical based approach, where each chapter will help you improve your penetration testing

skills using Python to become a master pen tester.

Discovering and Exploiting Security Flaws Createspace Independent Publishing Platform

Gain a solid foundation for designing, building, and configuring security-enhanced, hack-resistant Microsoft® ASP.NET Web 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—Web 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.

OWASP Top 10: the Top 10 Most Critical Web Application Security Threats Packt Publishing Ltd

The one-stop-source powering Application Security success, jam-packed with ready to use insights for results, loaded with all the data you need to decide how to gain and move ahead. Based on extensive research, this lays out the thinking of the most successful

Application Security knowledge experts, those who are adept at continually innovating and seeing opportunities. This is the first place to go for Application Security innovation - INCLUDED are numerous real-world Application Security blueprints, presentations and templates ready for you to access and use. Also, if you are looking for answers to one or more of these questions then THIS is the title for you: How do I improve web application security? How do I do web application security testing? What are good books on web application security? Which company offers the best web application security with minimum price? What certification is most recognized for web application security? What are the top web application security scanners on the market? How do I start learning about web application security? What is the best way to learn OWASP web application security? Web Application Security: What does formkey do? What is the difference between network security and application security? Technology-Any tools available for Testing Mobile NATIVE Application Security? Web Application Security: Is there any training platform that lets you experiment with XSS, defacement, brute force, DDoS, etc. attacks? Vulnerability Assessment: Which is the best web application security scanner to buy considering the price? What are the best sources of mobile application security? Is web application security a beginner's guide book by bryan sullivan a good book, is it worth reading? Want some information regarding Web Application

Security Scanners? What would be the starting point to learn about mobile application security for both iOS and Android? ...and much more..."

Web Application Defender's Cookbook

Newnes

Test, fuzz, and break web applications and services using Burp Suite’s powerful capabilities Key Features Master the skills to perform various types of security tests on your web applications Get hands-on experience working with components like scanner, proxy, intruder and much more Discover the best-way to penetrate and test web applications Book Description Burp suite is a set of graphic tools focused towards penetration testing of web applications. Burp suite is widely used for web penetration testing by many security professionals for performing different web-level security tasks. The book starts by setting up the environment to begin an application penetration test. You will be able to configure the client and apply target whitelisting. You will also learn to setup and configure Android and IOS devices to work with Burp Suite. The book will explain how various features of Burp Suite can be used to detect various vulnerabilities as part of an application penetration test. Once detection is completed and the vulnerability is confirmed, you will be able to exploit a detected vulnerability using Burp Suite. The book will also covers advanced concepts like writing extensions and macros for Burp suite. Finally, you will discover various steps that are taken to identify the target, discover weaknesses

in the authentication mechanism, and finally break the authentication implementation to gain access to the administrative console of the application. By the end of this book, you will be able to effectively perform end-to-end penetration testing with Burp Suite. What you will learn Set up Burp Suite and its configurations for an application penetration test Proxy application traffic from browsers and mobile devices to the server Discover and identify application security issues in various scenarios Exploit discovered vulnerabilities to execute commands Exploit discovered vulnerabilities to gain access to data in various datastores Write your own Burp Suite plugin and explore the Infiltrator module Write macros to automate tasks in Burp Suite Who this book is for If you are interested in learning how to test web applications and the web part of mobile applications using Burp, then this is the book for you. It is specifically designed to meet your needs if you have basic experience in using Burp and are now aiming to become a professional Burp user.

Enhanced with Text Analytics and Content by PageKicker Robot Phil 73

Elsevier

Learn how to build an end-to-end Web application security testing framework KEY FEATURES ● Exciting coverage on vulnerabilities and security loopholes in modern web applications. ● Practical exercises and case scenarios on performing pentesting and identifying security breaches. ● Cutting-edge offerings on implementation of tools

including nmap, burp suite and wireshark. DESCRIPTION Hands-on Penetration Testing for Web Applications offers readers with knowledge and skillset to identify, exploit and control the security vulnerabilities present in commercial web applications including online banking, mobile payments and e-commerce applications. We begin with exposure to modern application vulnerabilities present in web applications. You will learn and gradually practice the core concepts of penetration testing and OWASP Top Ten vulnerabilities including injection, broken authentication and access control, security misconfigurations and cross-site scripting (XSS). You will then gain advanced skillset by exploring the methodology of security testing and how to work around security testing as a true security professional. This book also brings cutting-edge coverage on exploiting and detecting vulnerabilities such as authentication flaws, session flaws, access control flaws, input validation flaws etc. You will discover an end-to-end implementation of tools such as nmap, burp suite, and wireshark. You will then learn to practice how to execute web application intrusion testing in automated testing tools and also to analyze vulnerabilities and threats present in the source codes. By the end of this book, you will gain in-depth knowledge of web application testing framework and strong proficiency in exploring and building high secured web applications. WHAT YOU WILL LEARN ● Complete overview of concepts of web

penetration testing. ● Learn to secure against OWASP TOP 10 web vulnerabilities. ● Practice different techniques and signatures for identifying vulnerabilities in the source code of the web application. ● Discover security flaws in your web application using most popular tools like nmap and wireshark. ● Learn to respond modern automated cyber attacks with the help of expert-led tips and tricks. ● Exposure to analysis of vulnerability codes, security automation tools and common security flaws. WHO THIS BOOK IS FOR This book is for Penetration Testers, ethical hackers, and web application developers. People who are new to security testing will also find this book useful. Basic knowledge of HTML, JavaScript would be an added advantage. TABLE OF CONTENTS 1. Why Application Security? 2. Modern application Vulnerabilities 3. Web Pentesting Methodology 4. Testing Authentication 5. Testing Session Management 6. Testing Secure Channels 7. Testing Secure Access Control 8. Sensitive Data and Information disclosure 9. Testing Secure Data validation 10. Attacking Application Users: Other Techniques 11. Attacking Application Users: Other Techniques 12. Automating Custom Attacks 13. Pentesting Tools 14. Static Code Analysis 15. Mitigations and Core Defense Mechanisms

The Web Application Hacker's Handbook GRIN Verlag

The one-stop-source powering Web Application Security success, jam-packed with ready to use insights for results,

loaded with all the data you need to decide how to gain and move ahead. Based on extensive research, this lays out the thinking of the most successful Web Application Security knowledge experts, those who are adept at continually innovating and seeing opportunities. This is the first place to go for Web Application Security innovation - INCLUDED are numerous real-world Web Application Security blueprints, presentations and templates ready for you to access and use. Also, if you are looking for answers to one or more of these questions then THIS is the title for you: What are good books on web application security? How do I do web application security testing? How do I improve web application security? Which company offers the best web application security with minimum price? What certification is most recognized for web application security? What are the top web application security scanners on the market? How do I start learning about web application security? What is the best way to learn OWASP web application security? Web Application Security: What does formkey do? Web Application Security: Is there any training platform that lets you experiment with XSS, defacement, brute force, DDoS, etc. attacks? Vulnerability Assessment: Which is the best web application security scanner to buy considering the price? Is web application security a beginner's guide book by bryan sullivan a good book, is it worth reading? Want some information regarding Web Application Security

Scanners? Open Web Application Security Project (OWASP): Do OWASPs have any Android apps? Where can I get the list of companies who provide web application security? Can web application security solutions create the proficient enterprise structure? Kindly let me know the carrier scope of open web application security project? ...and much more..."

Web Application Security No Starch Press

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.

Hands-on Penetration Testing for Web Applications Packt Publishing Ltd

Learn to exploit vulnerable database applications using SQL injection tools and techniques, while understanding how to effectively prevent attacks Key Features Understand SQL injection and its effects on websites and other systems Get hands-on with SQL injection using both manual and automated tools Explore practical tips for various attack and defense strategies relating to SQL injection Book 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 learn Focus on how to defend against SQL injection attacks Understand web application security Get up and running with a variety of SQL injection concepts Become well-versed with different SQL injection scenarios Discover SQL injection manual attack techniques Delve into SQL injection automated techniques Who 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.
Cross Site Scripting Exploits and Defense

Complete Publishing
Introduction -- HTML -- JavaScript and VBScript -- Nonalphanumeric JavaScript -- CSS -- PHP -- SQL -- Web application firewalls and client-side filters -- Mitigating bypasses and attacks -- Future developments.

Web Application Security - Simple Steps to Win, Insights and Opportunities for Maxing Out Success "O'Reilly Media, Inc."
Web-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. Web-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.

An Expert Way of Secure Web Application Deployment Jones & Bartlett Publishers
Safety of Web 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, https protocol)

A Guide to Securing Modern Web Applications CRC Press

Modern web applications are built on a tangle of technologies that have been developed over time and then haphazardly pieced together. Every piece of the web application stack, from HTTP requests to browser-side scripts, comes with important yet subtle security consequences. To keep users safe, it is essential for developers to confidently navigate this landscape. In The Tangled Web, Michal Zalewski, one of the world’s top browser security experts, offers a compelling narrative that explains exactly how browsers work and why they’re fundamentally insecure. Rather than dispense simplistic advice on vulnerabilities, Zalewski examines the entire browser security model, revealing weak points and providing crucial

information for shoring up web application security. You'll learn how to: –Perform common but surprisingly complex tasks such as URL parsing and HTML sanitization –Use modern security features like Strict Transport Security, Content Security Policy, and Cross-Origin Resource Sharing –Leverage many variants of the same-origin policy to safely compartmentalize complex web applications and protect user credentials in case of XSS bugs –Build mashups and embed gadgets without getting stung by the tricky frame navigation policy –Embed or host user-supplied content without running into the trap of content sniffing For quick reference, "Security Engineering Cheat Sheets" at the end of each chapter offer ready solutions to problems you're most likely to encounter. With coverage extending as far as planned HTML5 features, The Tangled Web will help you create secure web applications that stand the test of time.

Practical techniques to secure old vulnerabilities against modern attacks Microsoft Press

In this book, we aim to describe how to make a computer bend to your will by finding and exploiting vulnerabilities specifically in Web applications. We will describe common security issues in Web 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 Web applications. Learn to defend Web-based applications developed with AJAX, SOAP, XMLPRC, and more. See why Cross Site Scripting attacks can be so devastating.