OMB No. 9873553466479

Attacking Oracle Web Applications With Metasploit

Padding Oracle Attack | Explainer Video | Secure Code Warrior I know Mag1k [medium]: HackTheBox Web Challenge (padding oracle attack) Fully Explaining the Evil of the Padding Oracle Attack with HacktheBox's \"I know Mag1k\" and \"Lazy\"! the best book to learn web hacking #shorts Protecting Your Book From Scammers HTB Academy: Attacking Web Applications With FFUF - Page Fuzzing Beginner Web Application Hacking (Full Course) Top 10: Best Books For Hackers Top Hacking Books for 2023 The Padding Oracle Attack (Part 2) - Performing the attack Identifying a Browser Attack- CompTIA Security+ Lab 24 Scan Websites for Potential Vulnerabilities Using Vega in Kali Linux [Tutorial] Ethical Hacking 101: Web App Penetration Testing - a full course for beginners Free Web Hacking Course Hacking Web Applications (2+ hours of content) Cybersecurity Books - The Web Application Hacker's Handbook Protect Against Common Database Attacks with Oracle SQL Firewall | Oracle DatabaseWorld AI Edition How a Hacker Could Attack Web Apps with Burp Suite \u0026 SQL Injection Oracle Manipulation | Web3 Security 101 Web Application Penetration Testing Book to Read Free Oracle Management Cloud SQL injection attack, querying the database type and version on Oracle SQL Injection For Beginners Attacking Web Applications with Ffuf Learn how to build a web application using JSP, JSTL and Oracle Database Burp Academy Labs - Attacking Oracle Database With Union SQL Injection

Detecting and Preventing Web Application Security Problems
Attack and Defend Computer Security Set
Certified Ethical Hacker (CEH) Cert Guide
A Hacker's Guide to Capture, Analysis, and Exploitation
Bulletproof SSL and TLS
A Practical Introduction to Modern Encryption
Information Security Applications
7th International Workshop, WISA 2006, Jeju Island, Korea, August 28-30, 2006, Revised Selected Papers
Ethical Hacking and Countermeasures: Web Applications and Data Servers
How to Break Web Software
Building Secure Apex Applications
The Database Hacker's Handbook Defending Database
Client-side Attacks and Defense
Oracle Fusion Developer Guide
Concepts, Methodologies, Tools, and Applications
The Web Application Hacker's Handbook
Functional and Security Testing of Web Applications and Web Services
Web Application Vulnerabilities
Design, deploy, and manage your APIs in Oracle’s new API Platform
Know Your Network

Attacking Oracle Web Applications With Metasploit *OMB No. 9873553466479 edited by*

HUDSON CANTRELL

Detecting and Preventing Web Application Security Problems Springer
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.
Attack and Defend Computer Security Set John Wiley & Sons

Rigorously test and improve the security of all your Web software! It’s as certain as death and taxes: hackers will mercilessly attack your Web 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 Web-based software: How to Break Web Software. In this book, two renowned experts address every category of Web 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 Web 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 Web services Your Web 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.

Certified Ethical Hacker (CEH) Cert Guide John Wiley & Sons

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.

A Hacker's Guide to Capture, Analysis, and Exploitation Pearson IT Certification

The latest Web app attacks and countermeasures from world-renowned practitioners Protect your Web 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 Web 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 Web 2.0 features. Integrating security into the Web 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 Web Server and Oracle WebLogic in operation Understand how attackers defeat commonly used Web 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 Web 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.

Bulletproof SSL and TLS Newnes

Implement bulletproof e-business security the proven Hacking Exposed way Defend against the latest Web-based attacks by looking at your Web applications through the eyes of a malicious intruder. Fully revised and updated to cover the latest Web exploitation techniques, Hacking Exposed Web 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.

A Practical Introduction to Modern Encryption McGraw Hill Professional

An example-driven approach to securing Oracle APEXapplications As a Rapid Application Development framework, Oracle ApplicationExpress (APEX) allows websites to easily be created based on datawithin an Oracle database. Using only a web browser, you candevelop and deploy professional applications that are both fast andsecure. However, as with any website, there is a security risk andthreat, and securing APEX applications requires some specificknowledge of the framework. Written by well-known securityspecialists Recx, this book shows you the correct ways to implementyour APEX applications to ensure that they are not vulnerable toattacks. Real-world examples of a variety of securityvulnerabilities demonstrate attacks and show the techniques andbest practices for making applications secure. Divides coverage into four sections, three of which cover themain classes of threat faced by web applications and the forthcovers an APEX-specific protection mechanism Addresses the security issues that can arise, demonstratingsecure application design Examines the most common class of vulnerability that allowsattackers to invoke actions on behalf of other users and accesssensitive data The lead-by-example approach featured in this critical bookteaches you basic "hacker" skills in order to show you how tovalidate and secure your APEX applications.

Information Security Applications Elsevier

Prepare for the new Certified Ethical Hacker version 8 exam with this Sybex guide Security professionals remain in high demand. The Certified Ethical Hacker is a one-of-a-kind certification designed to give the candidate a look inside the mind of a hacker. This study guide provides a concise, easy-to-follow approach that covers all of the exam objectives and includes numerous

examples and hands-on exercises. Coverage includes cryptography, footprinting and reconnaissance, scanning networks, enumeration of services, gaining access to a system, Trojans, viruses, worms, covert channels, and much more. A companion website includes additional study tools, Including practice exam and chapter review questions and electronic flashcards. Security remains the fastest growing segment of IT, and CEH certification provides unique skills The CEH also satisfies the Department of Defense's 8570 Directive, which requires all Information Assurance government positions to hold one of the approved certifications This Sybex study guide is perfect for candidates studying on their own as well as those who are taking the CEHv8 course Covers all the exam objectives with an easy-to-follow approach Companion website includes practice exam questions, flashcards, and a searchable Glossary of key terms CEHv8: Certified Ethical Hacker Version 8 Study Guide is the book you need when you're ready to tackle this challenging exam Also available as a set, Ethical Hacking and Web Hacking Set, 9781119072171 with The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, 2nd Edition.

7th International Workshop, WISA 2006, Jeju Island, Korea, August 28-30, 2006, Revised Selected Papers McGraw Hill Professional

The SANS Institute maintains a list of the "Top 10 Software Vulnerabilities." At the current time, over half of these vulnerabilities are exploitable by Buffer Overflow attacks, making this class of attack one of the most common and most dangerous weapon used by malicious attackers. This is the first book specifically aimed at detecting, exploiting, and preventing the most common and dangerous attacks. Buffer overflows make up one of the largest collections of vulnerabilities in existence; And a large percentage of possible remote exploits are of the overflow variety. Almost all of the most devastating computer attacks to hit the Internet in recent years including SQL Slammer, Blaster, and I Love You attacks. If executed properly, an overflow vulnerability will allow an attacker to run arbitrary code on the victim's machine with the equivalent rights of whichever process was overflowed. This is often used to provide a remote shell onto the victim machine, which can be used for further exploitation. A buffer overflow is an unexpected behavior that exists in certain programming languages. This book provides specific, real code examples on exploiting buffer overflow attacks from a hacker's perspective and defending against these attacks for the software developer. Over half of the "SANS TOP 10 Software Vulnerabilities" are related to buffer overflows. None of the current-best selling software security books focus exclusively on buffer overflows. This book provides specific, real code examples on exploiting buffer overflow attacks from a hacker's perspective and defending against these attacks for the software developer.

Ethical Hacking and Countermeasures: Web Applications and Data Servers John Wiley & Sons

Special Ops: Internal Network Security Guide is the solution for the impossible 24-hour IT work day. By now, most companies have hardened their perimeters and locked out the "bad guys," but what has been done on the inside? This book attacks the problem of the soft, chewy center in internal networks. We use a two-pronged approach-Tactical and Strategic-to give readers a complete guide to internal penetration testing. Content includes the newest vulnerabilities and exploits, assessment methodologies, host review guides, secure baselines and case studies to bring it all together. We have scoured the Internet and assembled some of the best to function as Technical Specialists and Strategic Specialists. This creates a diversified project removing restrictive corporate boundaries. The unique style of this book will allow it to cover an incredibly broad range of topics in unparalleled detail. Chapters within the book will be written using the same concepts behind software development. Chapters will be treated like functions within programming code, allowing the authors to call on each other's data. These functions will supplement the methodology when specific technologies are examined thus reducing the common redundancies found in other security books. This book is designed to be the "one-stop shop" for security engineers who want all their information in one place. The technical nature of this may be too much for middle management; however technical managers can use the book to help them understand the challenges faced by the engineers who support their businesses. Ø Unprecedented Team of Security Luminaries. Led by Foundstone Principal Consultant, Erik Pace Birkholz, each of the contributing authors on this book is a recognized superstar in their respective fields. All are highly visible speakers and consultants and their frequent presentations at major industry events such as the Black Hat Briefings and the 29th Annual Computer Security Institute Show in November, 2002 will provide this book with a high-profile launch. Ø The only all-encompassing book on internal network security. Windows 2000, Windows XP, Solaris, Linux and Cisco IOS and their applications are usually running simultaneously in some form on most enterprise networks. Other books deal with these components individually, but no other book provides a comprehensive solution like Special Ops. This book's unique style will give the reader the value of 10 books in 1.

How to Break Web Software

Springer

A practical handbook for network adminstrators who need to develop and implement security assessment programs, exploring a variety of offensive technologies, explaining how to design and deploy networks that are immune to offensive tools and scripts, and detailing an efficient testing model. Original. (Intermediate)

Building Secure Apex Applications

Elsevier

Master Oracle Fusion Middleware Successfully design rich enterprise web applications using the detailed information in this Oracle Press volume. Oracle Fusion Developer Guide goes beyond the predominant drag-and-drop methods in Oracle JDeveloper 11g and provides a wealth of examples that address common development scenarios when using Oracle Fusion Middleware. Work with Oracle JDeveloper 11g, define navigation rules, accept and validate user input, build page layouts and skins, and incorporate drag-and-drop functionality into web applications. This authoritative resource also explains how to secure and internationalize your applications. Understand the Oracle Application Development Framework and Oracle ADF Faces Rich Client lifestyle Construct Oracle ADF data controls, task flows, and dynamic regions Graphically represent information with Oracle ADF Faces DVT components Modularize applications using Oracle ADF libraries, Oracle ADF task flows, and other reusable components Define dynamic navigation rules in Oracle Fusion Middleware web applications Leverage Web 2.0 features using Oracle ADF Faces Rich Client components Control user access with Oracle WebLogic Server and Oracle ADF security For a complete list of Oracle Press

titles, visit www.OraclePressBooks.com
The Database Hacker's Handbook Defending Database McGraw Hill Professional
Ethical Hacking and Countermeasures: Web Applications and Data ServersCengage Learning

Client-side Attacks and Defense

McGraw Hill Professional
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 Web 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 Web 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.
Oracle Fusion Developer Guide Addison-Wesley Professional
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.

Concepts, Methodologies, Tools, and Applications

John Wiley & Sons
Expert Oracle Application Express Security covers all facets of security related to Oracle Application Express (APEX) development. From basic settings that can enhance security, to preventing SQL Injection and Cross Site Scripting attacks, Expert Oracle Application Express Security shows how to secure your APEX applictions and defend them from intrusion. Security is a process, not an event. Expert Oracle Application Express Security is written with that theme in mind. Scott Spendolini, one of the original creators of the product, offers not only examples of security best practices, but also provides step-by-step instructions on how to implement the recommendations presented. A must-read for even the most experienced APEX developer, Expert Oracle Application Express Security can help your organization ensure their APEX applications are as secure as they can be.
The Web Application Hacker's Handbook PediaPress
"This book reviews problems, issues, and presentations of the newest research in the field of cyberwarfare and cyberterrorism. While enormous efficiencies have been gained as a result of computers and telecommunications technologies, use of these systems and networks translates into a major concentration of information resources, createing a vulnerability to a host of attacks and exploitations"--Provided by publisher.
Functional and Security Testing of Web Applications and Web Services IGI Global
The latest Web app attacks and countermeasures from world-renowned practitioners Protect your Web 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 Web 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 Web 2.0 features. Integrating security into the Web 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 Web Server and Oracle WebLogic in operation Understand how attackers defeat commonly used Web 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 Web 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
Web Application Vulnerabilities Springer
The EC-Council | Press Ethical Hacking and Countermeasures Series is comprised of five books covering a broad base of topics in offensive network security, ethical hacking, and network defense and countermeasures. The content of this series is designed to immerse the reader into an interactive environment where they will be shown how to scan, test, hack and secure information systems. With the full series of books, the reader will gain in-depth knowledge and practical experience with essential security systems, and become prepared to succeed on the Certified Ethical Hacker, or C|EH, certification from EC-Council. This certification covers a plethora of offensive security topics ranging from how perimeter defenses work, to scanning and attacking simulated networks. A wide variety of tools, viruses, and malware is presented in this and the other four books, providing a complete understanding of the tactics and tools used by hackers. By gaining a thorough understanding of how hackers operate, an Ethical Hacker will be able to set up strong countermeasures and defensive systems to protect an organization's critical infrastructure and information. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Design, deploy, and manage your APIs in Oracle's new API Platform

John Wiley & Sons
Develop Robust Modern Web Applications with Oracle Application Express. Covers APEX 5.1. Easily create data-reliant web applications that are reliable, scalable, dynamic, responsive, and secure using the detailed information contained in this Oracle Press guide. Oracle Application Express (APEX): Build Powerful Data-Centric Web Apps with APEX features step-by-step application development techniques, real-world coding examples, and best practices. You will find out how to work with the App Builder and Page Designer, use APEX themes (responsive and mobile included), templates and wizards, and design and deploy custom web apps. New and updated features in APEX 5.0/5.1 are thoroughly covered and explained. • Understand APEX concepts and programming fundamentals • Plan and control the development cycle, using HLD techniques • Use APEX themes and templates, including Universal Theme • Use APEX wizards to rapidly build forms and reports on database tables • Build modern, dynamic, and interactive user interface using the Page Designer • Increase user experience using Dynamic Actions (Ajax included) • Build and utilize the new APEX 5.1 Interactive Grid • Implement App Logic with APEX computations, validations, and processes • Use (automatic) built-in and manual DML to manipulate your data • Handle security at browser, application, and database levels • Successfully deploy the developed APEX apps

Know Your Network

John Wiley & Sons
These proceedings gather outstanding research papers presented at the Second International Conference on Data Engineering 2015 (DaEng-2015) and offer a consolidated overview of the latest developments in databases, information retrieval, data mining and knowledge management. The conference brought together researchers and practitioners from academia and industry to address key challenges in these fields, discuss advanced data engineering concepts and form new collaborations. The topics covered include but are not limited to: • Data engineering • Big data • Data and knowledge visualization • Data management • Data mining and warehousing • Data privacy & security • Database theory • Heterogeneous databases • Knowledge discovery in databases • Mobile, grid and cloud computing • Knowledge management • Parallel and distributed data • Temporal data • Web data, services and information engineering • Decision support systems • E-Business engineering and management • E-commerce and e-learning • Geographical information systems • Information management • Information quality and strategy • Information retrieval, integration and visualization • Information security • Information systems and technologies