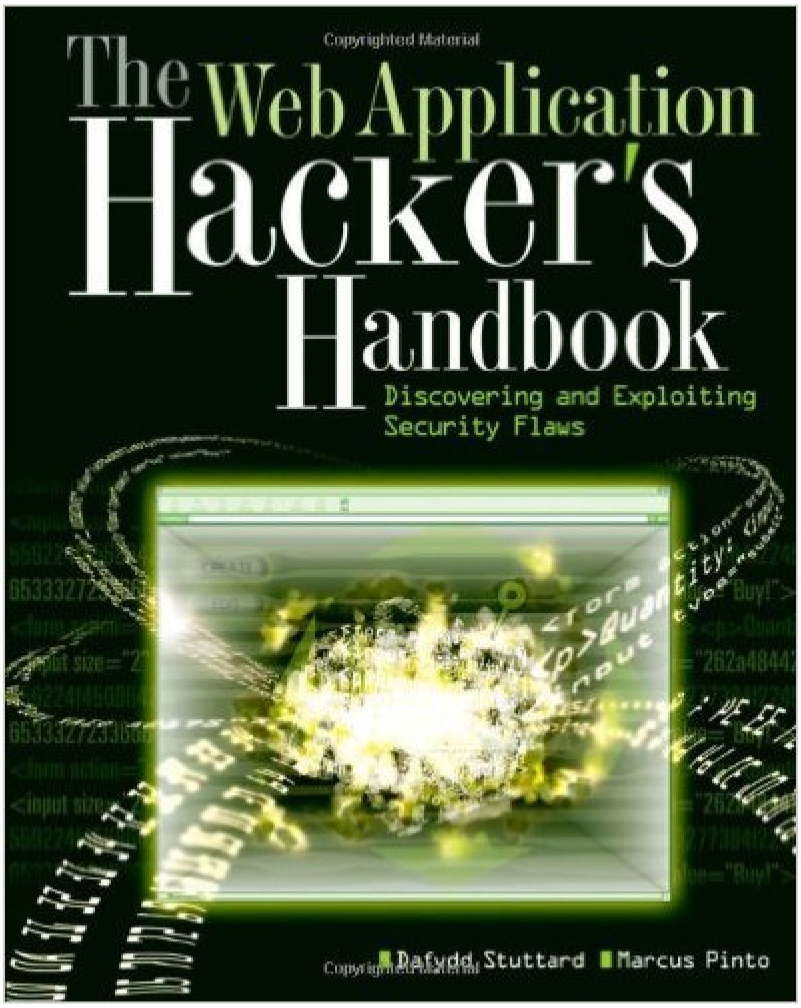
The Web Application Hacker's Handbook: Discovering And Exploiting Security Flaws


Copyrighted Material
The Web Application Hacker's Handbook
Discovering and Exploiting Security Flaws
Dafydd Stuttard
Marcus Pinto
Copyrighted Material

Synopsis

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.

Book Information

Paperback: 768 pages

Publisher: Wiley; 1 edition (October 22, 2007)

Language: English

ISBN-10: 0470170778

ISBN-13: 978-0470170779

Product Dimensions: 7.4 x 1.6 x 9.2 inches

Shipping Weight: 2.4 pounds

Average Customer Review: 4.8 out of 5 starsÂ Â See all reviewsÂ (28 customer reviews)

Best Sellers Rank: #453,698 in Books (See Top 100 in Books)   #105 inÂ Books > Computers & Technology > Certification > CompTIA   #283 inÂ Books > Computers & Technology > Security & Encryption > Privacy & Online Safety   #334 inÂ Books > Computers & Technology > Internet & Social Media > Hacking

Customer Reviews

This is the most important IT security title written in the past year or more. Why? Custom web applications offer more opportunities for exploitation than all of the publicized vulnerabilities your hear about combined. This book gives expert treatment to the subject. I found the writing to be very clear and concise in this 727 page volume. There is minimal fluff. While everything is clearly explained, this is not a beginners book. The authors assume that you can read html, JavaScript, etc... Usually with a book like this there are a few really good chapters and some so-so chapters, but that’s not the case here. Chapters 3-18 in this book rock all the way through. Another huge plus is the tools in this book are free.The first few chapters provide context and background information. Chapter 3 on Web Application Technologies provides particularly useful background info. The next 666 pages of the book are all about attacking the applications.There next five chapters cover mapping application functionality, client side controls, authentication, sessions, and access controls. The coverage is comprehensive. I’m not new to these topics, but I learned so much in every chapter. The depth of coverage is amazing.The next six chapters are the heart of this book. They cover injection, path traversal, application logic, XSS and related attacks, automating attacks, and information disclosure. You’ll find full treatment of attacks we’re all familiar with like SQL injection and cross site scripting as well as many that most of us haven’t heard of before. The danger is real and these chapters need to be read.The final next four chapters cover attacks against compiled applications, application architecture, web servers, and source code.

First off - I will come clean and admit that this review is biased on several levels. Since the public facing web application security community is small, any published work or presentation will draw the attention of others in the field and often conversations/reviews/blog comments will ensue. Why mention this? Well, Dafydd reviewed XSS Attacks on his blog - a book I co-authored along with other much bigger players in the field. I also have a bit of admiration for Burp, a program Dafydd wrote and is highlighted in most any valuable web app book. So, to say I have no connections to the authors would be misleading - to say the least.Now, for the book - just buy it, you won’t be disappointed. As I read through the book (scanning some of the familiar parts), I was overwhelmed with the fact that a full time web application penetration tester has to known A LOT - all of which this book touches on in one way or another. I really can’t think of any other book that can compete...For those new to the field, either as security professionals or as web developers, this book will most likely leave you a bit reeling. It does a good job illustrating and demonstrating the many facets of secure web app development. For the more seasoned professional, this book will no doubt serve as a resource to refresh your memory on a trick or technique you forgot about. I know it has already served this purpose for me...So, where do I start with a more detailed expose on the book? Personally, I would start by reading chapter 20 - A Web Application Hackers Methodology.

Before you even read a word, "The Web Application Hacker’s Handbook: Discovering and Exploiting Security Flaws" should catch your interest for two reasons. The first is that, by name and cover art, it is being presented by Wiley as the web security counterpart of "The Shellcoder’s Handbook", which I have already given a positive review. The second reason, which I did not realize it until the book arrived, is that one of the authors, Dafydd Stuttard, is the author of the excellent Burp Suite tools for exploring and exploiting web applications. I use the proxy features of it frequently, and I often tell people it’s the only reason I install a Java VM on my laptop. I was very excited about reading a web application security by the author of such a great set of tools, and it did not let me down.I will admit that I haven’t read any other books that focus on attacking web applications, so I do not have anything to compare it to. I can say, however, that this book has very complete and thorough coverage of the topic, from mapping the application to exploitation. While a number of common attacks are covered (such as cross-site scripting and SQL injection), the real value of the book is in the way it teaches the process of finding vulnerabilities. Armed with this, you can more effectively discover problems that involve logical errors unique to the application you’re looking at. The book reads very well cover-to-cover, with each chapter building up another step in a complete web application hacker’s methodology that the authors have put together.The topics covered encompass most of the vulnerabilities you’ll see disclosed in applications daily on the mailing lists.

Download to continue reading...

How to Break Code Wiley GAAP: Interpretation and Application of Generally Accepted Accounting Principles 2011 (Wiley GAAP: Interpretation & Application of Generally Accepted Accounting Principles) ASP.NET Core Application Development: Building an application in four sprints (Developer Reference) Girls Life Application Study Bible NLT (Kid's Life Application Bible) Sound (Discovering Science) (Discovering Science) Discovering Genesis: Content, Interpretation, Reception (Discovering Biblical Texts (DBT)) Project Management Using Microsoft Project 2013: A Training and Reference Guide for Project Managers Using Standard, Professional, Server, Web Application and Project Online

Dmca