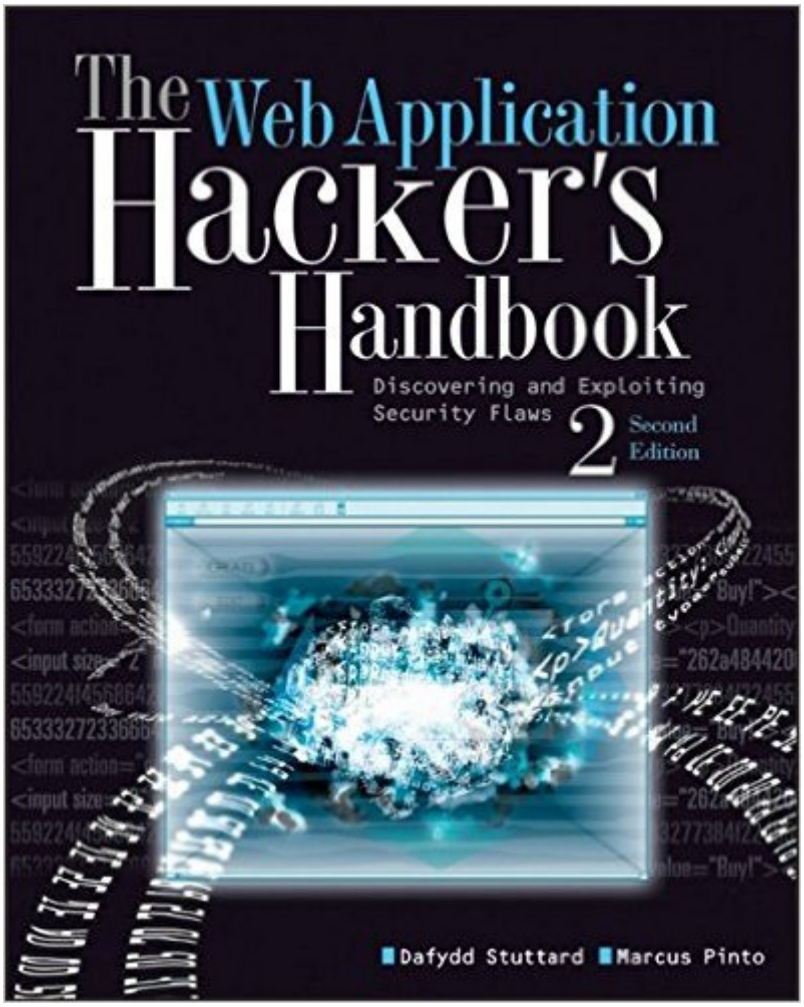
The Web Application Hacker's Handbook: Finding And Exploiting Security Flaws



Synopsis

The highly successful security book returns with a new edition, completely updatedWeb 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 editionDiscusses new remoting frameworks, HTML5, cross-domain integration techniques, UI redress, framebusting, HTTP parameter pollution, hybrid file attacks, and moreFeatures 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 tasksFocusing 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..

Book Information

Paperback: 912 pages
Publisher: Wiley; 2 edition (September 27, 2011)
Language: English
ISBN-10: 1118026470
ISBN-13: 978-1118026472
Product Dimensions: 7.4 x 1.7 x 9.3 inches
Shipping Weight: 3 pounds (View shipping rates and policies)
Average Customer Review: 4.4 out of 5 starsÂ Â See all reviewsÂ (59 customer reviews)
Best Sellers Rank: #24,854 in Books (See Top 100 in Books) #17 inÂ Books > Computers & Technology > Networking & Cloud Computing > Network Security #19 inÂ Books > Computers & Technology > Security & Encryption > Privacy & Online Safety #31 inÂ Books > Computers & Technology > Internet & Social Media > Hacking

Customer Reviews

There's a running joke we have on our assessment team about the Web Application Hackers

Handbook. Every time we see a new technology, or have to deal with a one-off situation, we start doing research online only to find it was already referenced in WAHH somewhere. We've all read this book several times too, it's like Dafydd and Marcus sneak into our houses at night and add content...Joking aside though, there is no other reference for web hacking as thorough or complete as WAHH.With WAHH2 the authors added a significant amount content and rehashed existing chapters that were already deeply technical. The bonus in WAHH2 is its associated labs. Dafydd and Marcus have been giving a live WAHH training for years and have now moved the stellar CTF like challenges to the cloud. You can buy credits ($7 for 1hr) and move right along as you read the book (MDSec.net). When I say the labs are stellar, I mean it. The labs come almost straight from the class and start trivial and then get crazy. The injection labs were by far my favorite, housing 30-40 different injection types/variants each between XSS/SQLi. The CTF in the class (which i'll mention again is where the MDSec.com labs are based from) gets ridiculous toward the end. Even seasoned web testers fall around questions 14-16. But i digress...WAHH2 is now the defacto buy for any pentest/QA/Audit team. Its usage will surpass any other book on your bookshelf if you are doing practical testing.5 stars, i'd give it 10 if I could.

Pains me to write a bad review for a book that has SO much great stuff. Really, it's full to the brim of really great info.But where they went way way wrong: they keep referencing "Try it!" modules that refer to an online site, where the have different tutorials set up on a virtual server. You're allowed to try the hack techniques against the server for a "mere 7 dollars per hour".But that's actually really really expensive (if you don't have a company paying for you, hell, even if you do). The online labs are sophisticated, but not THAT sophisticated. The author could have EASILY put them online for free, or run them cheaper. It'll take you HOURS to figure out anything on his labs, unless youre a seasoned pentest guy.it's 7 per hour, and you have to choose 1 hour increments. So I found myself listing things i wanted to try in that hour...which i never got through, because HE DIDN'T INCLUDE ANSWERS, OR A GUIDE! You're supposed to figure it out on the go, which is fine and dandy if youre just browsing a site, but not when youre paying 7 dollars an hour to be on a site.F that...could have done it better/different.

So as a book I will have to say this is a source of information, however, on the other hand it's very deceptive because in order to get the full benefit of the book you really have to:1. Buy the professional version of Burp Suite which the author wrote.It would have been nice if some sort of time trial was included.2. If you want to access any of the labs they talk about in the book you have

to subscribe to their training site which is from what I can tell $7.00 an hour...There are a great many good and free services out there, and personally I feel the this book (while having good material) was really written to support the authors sales efforts.I would have much rather seen the use of free websites and examples that didn't cost any more money.*shrug*It's ok

The first 3 chapters are a very good review of the state of Internet security in general. Then you hit chapter 4 and everything becomes C.I.P.U. (clear if previously understood) in a hurry. What is "Burp" and why do I need it? You have to jump to chapter 20 to find out, where you are told how to set up a proxy server. So now what? Use Burp to figure things out! We're going in a circle here. (And this assumes you've got your proxy even working.)The book also stresses on-line learning thru their website, for a modest fee. But just what do you get for these lessons. I don't know, because the first one doesn't occur until chapter 5. And by then I was turned off by the book.To be fair, there's a gold mine of material in this book. But it's not for the beginner. You have to put it together like a jig saw puzzle, but without benefit of any picture of what the finished puzzle should look like.If you are already beyond basic hacking, are aware of the tools available, and know the HTML standard inside out, then this is probably a good book for you. But it is way too much for the newbie. This book should come with the skill level notice of "For intermediate to advanced users."

This book improves on what I already thought was the best book on the subject.The advantage of this book (and now the new version even more so) is in the way it breaks down the topics. Many books sort of jump around with their various sections, while the WAHH takes the precise line that I think is best when building on one's understanding of this topic.The updated material is significant, and definitely worth the re-purchase. I bought both the dead-tree and the Kindle version.100% definitely recommended.

and hidden traps to hacking: Hacker, Computer, Programming, Security & Encryption Maximum Linux Security: A Hacker's Guide to Protecting Your Linux Server and Workstation Developer's Guide to Web Application Security Fatal Flaws: Navigating Destructive Relationships with People with Disorders... Brain Storm: The Flaws in the Science of Sex Differences The Negative Trait Thesaurus: A Writer's Guide to Character Flaws Exploiting Continuity: Maximum Entropy Estimation of Continuous Distribution (Series on Econometrics and Management Sciences) Beyond Counting : Exploiting Casino Games from Blackjack to Video Poker Social Security: Time for a Life of Leisure - The Guide of Secrets to Maximising Social Security Retirement Benefits and Planning Your Retirement (social ... disability, social security made simple) Pro ASP.NET Web API Security: Securing ASP.NET Web API (Expert's Voice in .NET) Python: Learn Web Scraping with Python In A DAY! - The Ultimate Crash Course to Learning the Basics of Web Scraping with Python In No Time (Web Scraping ... Python Books, Python for Beginners) The Car Hacker's Handbook: A Guide for the Penetration Tester Gray Hat Hacking The Ethical Hacker's Handbook, Fourth Edition Patent Drafting Secrets- How to write a patent application for an invention and how to draft a patent application for an invention