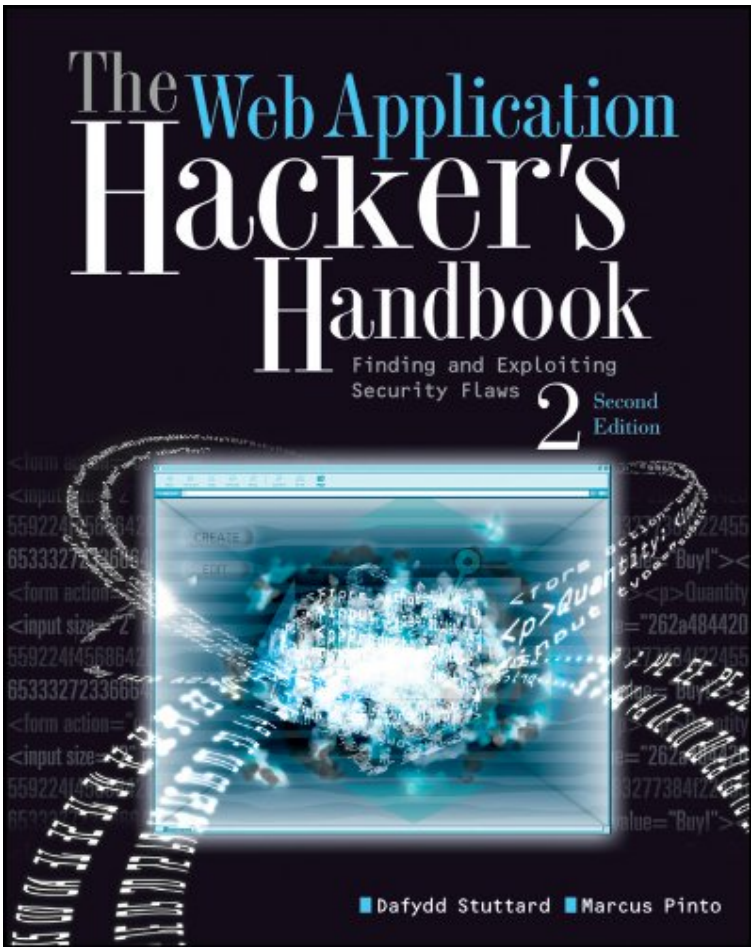
The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws

Von Dafydd Stuttard, Marcus Pinto
**Download PDF | ePub | DOC | audiobook | ebooks*



Produktinformation -Verkaufsrang: #324878 in eBooksVerffentlicht am: 2011-08-31Erscheinungsdatum: 2011-08-31File Name: B005LVQA9S | File size: 55.Mb

Von Dafydd Stuttard, Marcus Pinto : The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws before purchasing it in order to gage whether or not it would be worth my time, and all praised The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws:

KundenrezensionenHilfreichste Kundenrezensionen0 von 1 Kunden fanden die folgende Rezension hilfreich. really great bookVon LarsGreat read. Topics are well explained. It is relying on Burp for the first few chapters, but you can easily use the described Methods with other tools...32 von 38 Kunden fanden die folgende Rezension hilfreich. Well, well, well...Von LokalmatadorThere are two issues coming along with this book, which actually should be kept in mind before buying:1. The authors heavily promote BURP suite (developed by one of the authors) to be used as THE tool for web application testing. However, most of the described functionality is online available with BURP suite Pro, which can be bought for a nice 249 bucks with a single user license.2. The authors "gently" provide only labs, where

one is advised to test the various described attacks. However, as in the case with BURP suite, this does not come without additional costs...Under the bottom line, the book does not contain real insight knowledge (use Google and you will acquire the same knowledge, probably at the most in a more readable and technical manner). What it contains are numerous ads for BURP suite and attempts to get more money from you! Stay away from buying and do what a researcher does, research already available sources of knowledge, i.e., the Internet and its numerous discussion boards!@Edit: The further you get in the book, the more yackety-yak it contains. The authors try to avoid conciseness by all means. Sometimes the book acts as counting sheep. Don't buy!@@Edit: Maybe the authors also should try to get a little bit up to date and not use Windows 98 and IE 5.1 when showing a screenshot of a successful attack. This somehow makes them cockamamie...

KurzbeschreibungThe 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.
KurzbeschreibungThe 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.
BuchrckseiteNew technologies. New attack techniques. Start hacking.Web applications are everywhere, and they're insecure. Banks, retailers, and others have deployed millions of applications that are full of holes, allowing attackers to steal personal data, carry out fraud, and compromise other systems. This book shows you how they do it.This fully updated edition contains the very latest attack techniques and countermeasures, showing you how to break into today's complex and highly functional applications. Roll up your sleeves and dig in.* Discover how cloud architectures and social networking have added exploitable attack surfaces to applications* Leverage the latest HTML features to deliver powerful cross-site scripting attacks* Deliver new injection exploits, including XML external entity and HTTP parameter pollution attacks* Learn how to break encrypted session tokens and other sensitive data found in cloud services* Discover how technologies like HTML5, REST, CSS and JSON can be exploited to attack applications and compromise users* Learn new techniques for automating attacksand dealing with CAPTCHAs and cross-site request forgery tokens* Steal sensitive data across domains using seemingly harmless application functions and new browser featuresFind help and resources at http://mdsec.net/wahh* Source code for some of the scripts in the book* Links to tools and other resources* A checklist of tasks involved in most attacks* Answers to the questions posed in each chapter* Hundreds of interactive vulnerability labs