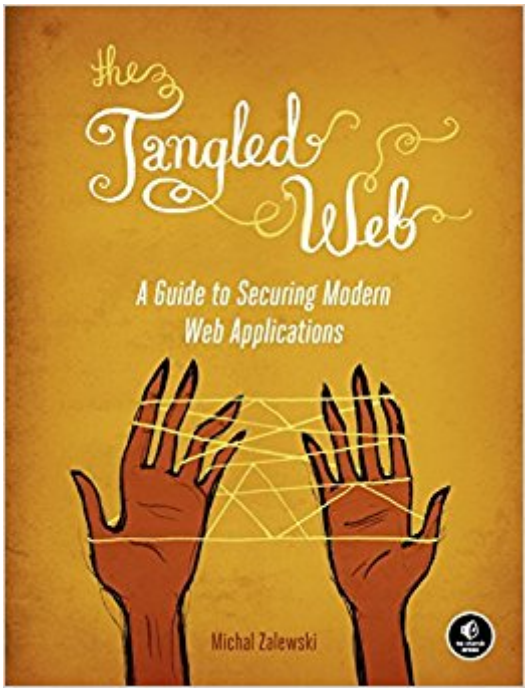
The Tangled Web: A Guide To Securing Modern Web Applications



Synopsis

"Thorough and comprehensive coverage from one of the foremost experts in browser security." --Tavis Ormandy, Google Inc.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.

Book Information

Paperback: 320 pages

Publisher: No Starch Press; 1 edition (November 26, 2011)

Language: English

ISBN-10: 1593273886

ISBN-13: 978-1593273880

Product Dimensions: 7 x 0.8 x 9.2 inches

Shipping Weight: 1.4 pounds (View shipping rates and policies)

Average Customer Review: 3.9 out of 5 stars 35 customer reviews

Best Sellers Rank: #303,805 in Books (See Top 100 in Books) #43 inÃ Â Books > Computers & Technology > Internet & Social Media > Web Browsers #76 inÃ Â Books > Computers & Technology > Security & Encryption > Viruses #96 inÃ Â Books > Computers & Technology >

Customer Reviews

Michal Zalewski is an internationally recognized information security expert with a long track record of delivering cutting-edge research. He is credited with discovering hundreds of notable security vulnerabilities and frequently appears on lists of the most influential security experts. He is the author of Silence on the Wire (No Starch Press), Google’s "Browser Security Handbook," and numerous important research papers.

The book provides systematic coverage of browser security. The first 6 pages of chapter 1 provide brilliant insight into why formal security models, risk management and taxonomies fail to deliver promised security improvements to organizations that embrace them. I used to explain the same with a lot of hand weaving, Zalewski’s approach and insight are far superior.Make no mistake, the book is focused on the browser and related technologies rather than the theory of security. The same tremendous insight, that made me nod with appreciation and wish that I had the book 5 years ago while working on security policies, illuminates browser concepts like in-browser content separation, scripting, and much more.I appreciate the authors treatment of each of the concepts in the context of the browser as a complex and still evolving technology, with it’s own history, standards, market requirements and politics.

Solid content to help one understand all the sad quirks of our Web standards! A great reference book for all security web engineers.

Did you know that every web application should have a crossdomain.xml? Check the top level of most popular sites. That is just one of the tips available in the Security Engineering Cheat Sheets in this book. Some of the content is a little dated but the guidance is very applicable.

At first i was conservative about this book because of the topics, URL, HTML, etc... However, since i’m a Zalewski’s fan, i decided to try it. When i read the first chapter, i got my mind blown. So many details where in front of me and i didn’t realize until now. It’s certainly a book for application security professionals, not for beginners.

The book is very well written and goes through modern web application vulnerabilities. The author,

as always, gives examples and very clear explanations.

Mr. Zalewski's new book is impressive and should be read by anyone working in the web space that cares about security -- whether an attacker or defender. It definitively captures the current state and how we arrived at this juncture due to the many historical browser wars. His current employer and producer of the most secure browser -- Google Chrome -- is about to capture a 40% share [1] of the browser market and leap frog Firefox, Internet Explorer, and Safari.The Tangled Web untangles the mystery of some poor design philosophies and also discusses some of the improvements that have been made along the way. A quote from the book that sums it all up is a statement that "...the status quo reflects several rounds of hastily implemented improvements and is a complex mix of browser-specific special cases..."I greatly enjoyed reading the book and jotted some notes down that may be useful to other readers. These were the topics that piqued my interest the most:* Microsoft's challenge to JavaScript, VBScript, has the potential for some exploitation, if no one has been fuzzing it much thus far.* SVG embedding vulnerabilities potential (eg. some initial research also published by Thorsten Holz [2]).* Flash cross-domain exploitation examples and crossdomain.xml "loose" policies.* Great coverage of "GIFAR" type issues.* Astute observations of trade-offs in plugin attack surface versus actual benefit to users.* XBAP security coverage.* The excellent tables of Same-Origin-Policy violations and other tests versus different client-side contexts.* In depth coverage of URI schemes [3] and potentials for abuse.* How to resolve data sharing via new mechanisms like postMessage() API.* Blind cookie-overwrite attacks (interesting examples).* Very humorous localhost.cisco.com abuse example.* Local HTML/other execution issues that break privacy segmentation.* Interesting about:neterror security weakness example.* New style HTML frame attacks.* CSS object overlay click-jacking examples and impact on user experience (eg. Firefox add-on installation).* Content sniffing and dangers such as Byte Order Marking / UTF-7; also interesting note on difference between "UTF7" and "UTF-7".* window.createPopup() example.* Abusing HSTS header injection for client-side DoS.* CSP coverage.As a final note, it was highly predictable to see slow-moving browser vendors being cited for their inability to rectify issues quickly (even those that are known), but what struck me as noteworthy was the case where Microsoft correctly challenged the CORS standard. It didn't appear that they were doing this for any political reason and in fact came up with a more technically superior solution, which the CORS team eventually drew inspiration from. That was nice for the author to throw in there and show that Microsoft still has the ability to engineer great solutions when they truly care about an initiative.I hope other readers also enjoy the book when they pick it up...[1]

[...][2] [...][3] [...]

The Tangled Web: A Guide to Securing Modern Web Applications Accessing the Deep Web & Dark Web with Tor: How to Set Up Tor, Stay Anonymous Online, Avoid NSA Spying & Access the Deep Web & Dark Web Tangled Treasures Coloring Book: 52 Intricate Tangle Drawings to Color with Pens, Markers, or Pencils - Plus: Coloring schemes and techniques (Tangled Color and Draw) Disney Tangled: The Series: Take on the World Cinestory Comic (Disney Tangled: The Series Cinestory Comic) Tangled: The Tangled Series, Book 1 Tangled (The Tangled Book 1) Tangled Dreams: Tabby's Tangled Art (Volume 1) Tangled Dreams Volume II: Tangled coloring pages to take with you. Tangled Gardens Coloring Book: 52 Intricate Tangle Drawings to Color with Pens, Markers, or Pencils (Tangled Color and Draw) Money for Art: The Tangled Web of Art and Politics in American Democracy Hollywood gothic: The tangled web of Dracula from novel to stage to screen A Tangled Web Urban Survival: The Beginners Guide to Securing your Territory, Food and Weapons (How to Survive Your First Disaster) (Urban Preppers Survival Guide, SHTF, Emergency Preparedness) Urban Survival Handbook: The Beginners Guide to Securing Your Territory, Food and Weapons (How to Survive Your First Disaster) Building Web Applications with Visual Studio 2017: Using .NET Core and Modern JavaScript Frameworks Securing the Outdoor Construction Site: Strategy, Prevention, and Mitigation How to Find Your Dream Job: Proven Strategies for Finding & Securing Your Dream Job Fast, Book 1 Home Security: Everything About Securing Your Home Qatar: Securing the Global Ambitions of a City-State Overturning Aqua Nullius: Securing Aboriginal Water Rights