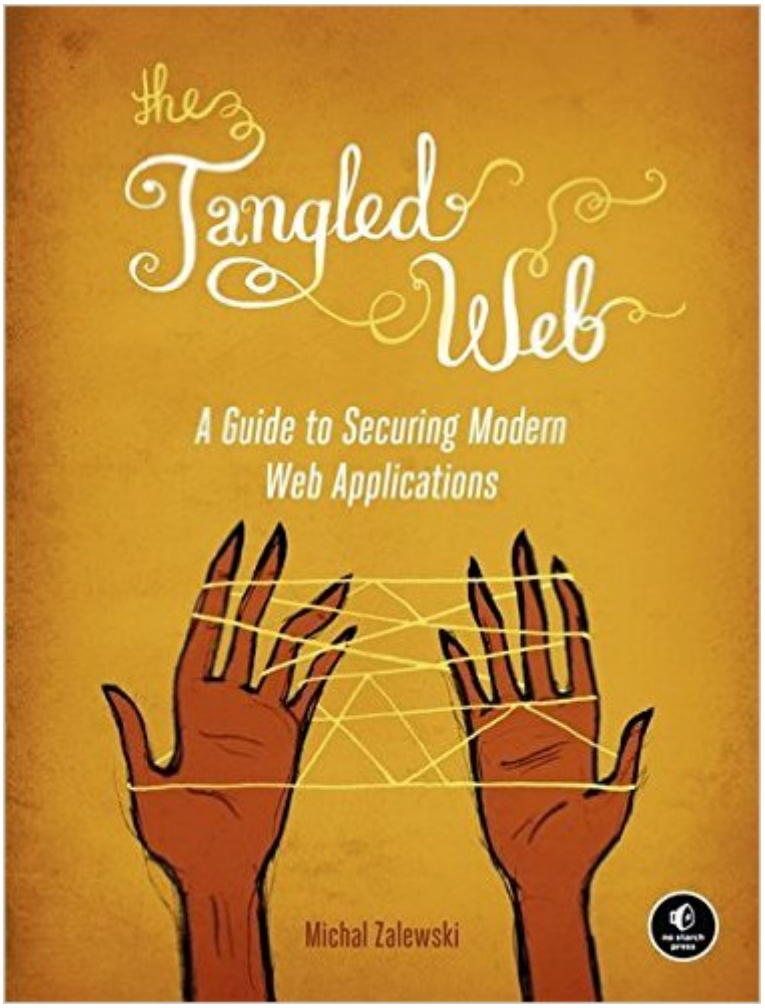
The Tangled Web: A Guide To Securing Modern Web Applications



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 29, 2011)

Language: English

ISBN-10: 1593273886

ISBN-13: 978-1593273880

Product Dimensions: 7 x 0.8 x 9 inches

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

Average Customer Review: 4.6 out of 5 starsÂ Â See all reviewsÂ (33 customer reviews)

Best Sellers Rank: #62,319 in Books (See Top 100 in Books) #10 inÂ Books > Computers & Technology > Internet & Social Media > Web Browsers #26 inÂ Books > Computers & Technology > Security & Encryption > Encryption #28 inÂ Books > Computers & Technology > Security &

Customer Reviews

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] [...]

In general, I thought this book was good. It covers a lot of material, and has nice "cheat sheets" at the end of each chapter.The reason I give the book 3 stars, however, is that the author is suffering from the curs of knowledge (or perhaps I am suffering from the curse of ignorance). While he gives some background information on how browsers work, html works, etc in the first part of the book, I did not find that it was enough to really understand the consequences of some of the vulnerabilities that he mentions. Often I was left wondering how the issue he raises is actually an issue, or how someone would exploit it.As a web developer, knowing how someone might exploit the security holes allows me to figure out how to close down those holes and make my web application more secure.Also, the book seems to be focused on what browser developers should be doing in order to close down these issues, and not what web developers should be doing.

In the classic poem Inferno, Dante passes through the gates of Hell, which has the inscription abandon all hope, ye who enter here above the entrance. After reading The Tangled Web: A Guide to Securing Modern Web Applications, one gets the feeling the writing secure web code is akin to Dante’s experience.In this incredibly good and highly technical book, author Michal Zalewski writes that modern web applications are built on a tangled mesh 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. In the book, Zalewski dissects those subtle security consequences to show what their dangers are, and how developers can take it to heart and write secure code for browsers.The Tangled Web: A Guide to Securing Modern Web Applications is written in the same style as Zalewski’s last book - Silence on the Wire: A Field Guide to Passive Reconnaissance and Indirect Attacks, which is another highly technical and dense book on the topic. This book tackles the issues surrounding insecure web browsers. Since the browser is the portal of choice for so many users; its inherent secure flaws leaves the user at a significant risk. The book details what developers can do to mitigate those risks.This book starts out with the observation that while the field of information security seems to be a mature and well-defined discipline, there is not even a rudimentary usable framework for understanding and assessing the security of modern software.In chapter 1, the book provides a brief overview of the development of the web and how so many security issues have cropped in. Zalewski writes that perhaps the most striking and nontechnical property of web

browsers is that most people who use them are overwhelmingly unskilled. And given the fact that most users simply do not know enough to use the web in a safe manner, which leads to the predicament we are in now.Zalewski then spends the remainder of the book detailing specific problems, how they are exploited, and details the manner in which they can be fixed.In chapter 2, the book details that something as elementary as how the resolution of relative URL's is done isn't a trivial exercise. The book details how misunderstandings occur between application level URL filters and the browser when handling these types of relative references can lead to security problems.For those that want a feel for the book, chapter 3 on the topic of HTTP is available here.Chapter 4 deals with HTML and the book notes that HTML is the subject of a fascinating conceptual struggle with a clash between the ideology and the reality of the on-line world. Tim Berners-Lee had the vision of a semantic web; namely a common framework that allows data to be shared and reused across applications, companies and the entire web. The notion though of a semantic web has not really caught on.Chapter 4 continues with a detailed overview of how to understand HTML parser behavior. The author writes that HTML parsers will second-guess the intent of the page developer which can leads to security problems.In chapter 12, the book deals with third-party cookies and notes that since their inception, HTTP cookies have been misunderstood as the tool that enables online advertisers to violate users privacy. Zalewski observes that the public's fixation on cookies is deeply misguided. He writes there is no doubt that some sites use cookies as a mechanism for malicious use. But that there is nothing that makes it uniquely suited for this task, as there are many other equivalent ways to sore unique identifiers on visitor's computes, such as cache-based tags.Chapter 14 details the issue of rogue scripts and how to manage them. In the chapter, the author goes slightly off-topic and asks the question if the current model of web scripting is fundamentally incompatible with the way human beings works. Which leads to the question of it if is possible for a script to consistently outsmart victims simply due to the inherent limits of human cognition.Part 3 of the book takes up the last 35 pages and is a glimpse of things to come. Zalewski optimistically writes that many of the battles being fought in today's browser war is around security, which is a good thing for everyone.Chapter 16 deals with new and upcoming security features of browsers and details many compelling security features such as security model extension frameworks and security model restriction frameworks.The chapter deals with one of the more powerful frameworks is the Content Security Policy (CSP) from Mozilla. CSP is meant to fix a large class of web application vulnerabilities, including cross site scripting, cross site request forgery and more. The book notes that as powerful as CSP is, one of its main problems is not a security one, in that it requires a webmaster to move all incline scripts on a web page to a separately requested

document. Given that many web pages have hundreds of short scripts; this can be an overwhelmingly onerous task.The chapter concludes with other developments such as in-browser HTML sanitizers, XSS filtering and more.Each chapter also concludes with a security engineering cheat sheet that details the core themes of the chapter.For anyone involved in programming web pages, The Tangled Web: A Guide to Securing Modern Web Applications should be considered required reading to ensure they write secure web code. The book takes a deep look at the core problems with various web protocols, and offers effective methods in which to mitigate those vulnerabilities.Michal Zalewski brings his extremely deep technical understanding to the book and combines it with a most readable style. The book is an invaluable resource and provides a significant amount of information needed to write secure code for browsers. There is a huge amount of really good advice in this book, and for those that are building web applications, it is hopes this is a book they read.