

Book Review: The Tangled Web

Review by Tristan Lawson, CISSP, MCSE: Security, GCIH, OSCP et al

Michal Zalewski, author of 2005's highly praised *Silence on the Wire*, is at it again with "The Tangled Web: A Guide to Securing Modern Web Applications," an incredible and highly technical book published by No Starch Press. Since the browser is the portal of choice for so many users, its inherent security flaws leave the user at a significant risk. This book details the issues surrounding insecure web browsers and what developers can do to mitigate those risks.

Mr. Zalewski writes about modern web applications which are built within a tangled mess of technologies, developed over time and then slapped together into a confusing monstrosity. This in turn leads to inconsistent operation with all kinds of vulnerabilities at several levels. The author goes into great detail taking apart every level of web applications from HTTP communication to browser and server-side scripts and dissects the subtle security consequences and the corresponding dangers of the unorganized conglomeration of web applications and browser code. The author then goes into how developers can work through the current problems and solve them down the road through new and revised code.

This book begins with the observation that the field of information security seems to be a mature and well-defined discipline, but in reality there is not even a rudimentary framework for understanding and assessing the security of modern software. So let's dive deeper into the book to see how Mr. Zalewski addresses the issues in an attempt to untangle this mess.

After the break, look for a link to a free download of Chapter 3: "Hypertext Transfer Protocol"

Discuss in Forums {mos_smf_discuss:Book Reviews}

[Click Here to Download Chapter 3: "Hypertext Transfer Protocol"](#)

The Tangled Web is written into three parts. PART I: ANATOMY OF THE WEB discusses subjects which one would think are known to everyone. Topics include URLs, HTTP and CSS. Despite them being well-known subjects, you couldn't be more wrong in that assumption. The author goes into great detail of each respective technology and explains thoroughly how vulnerabilities are in each technology due to the inadequacies of how it was originally engineered. The book provides a brief overview of the development of the web and how so many security issues have come to be.

Michal Zalewski shines light on the fact that most users of browsers are unskilled in computer technology; therefore they simply do not know enough to use the web in a safe manner. This simple fact leads to the current predicament where millions of users are easily disadvantaged. Mr. Zalewski details that something as elementary as how the parsing of relative URLs is done; it is in actuality no simple feat. The inconsistencies across browsers in parsing URLs and the misinterpretation of odd URL schemes lead to security problems and thus affect the users of the browsers.

Part II focuses on Browser Security Features. The author explores subjects such as Content Isolation, the same origin policy being the most explained, and Cross Domain Content Inclusion to name a couple. Chapters 9 through 11 cover the proper use of the same-origin policy across Flash, cookies, plug-ins, JavaScript limitations and how to shore them up or work around them. This Part represents the meat of the book and adequately covers the bulk of today's issues in an entertaining and educational manner. I won't ruin it for you by covering each aspect in detail, but let's just say the Mr. Zalewski is one sharp guy.

PART III: A GLIMPSE OF THINGS TO COME is a brief summary which delivers a vivid glimpse of the future of web applications and the web at-large. Believe it or not, he actually paints a positive picture. Since today's browser wars are centered on the battle of web browser developers to make feature distinctions with security as a selling point, it will do nothing but benefit us all in the long run. Content Security Policy (CSP), Cross Origin Resource Sharing (CORS), HTTP Strict Transport Security (HSTS), and additional tweaks to modern browsers are covered in this section. The Content Security Policy (CSP) framework from Mozilla is one of the more powerful frameworks Michal Zalewski writes about. CSP is meant to fix a large class of web application vulnerabilities, including cross-site scripting, cross-site request forgery and more. Many of these tweaks exist on some browsers but not others, and many are part of the HTML5 and CSS3 framework that is coming out but still being bickered over in development.

Michal Zalewski makes a point to discuss that while many of these security schemes are somewhat effective, it would be wise to not let your guard down and rely on these security tweaks alone. Part III ends with a chapter dedicated to a list of web application vulnerabilities which are common and is a great resource for web application penetration testers.

At the end of each chapter is a "Security Engineering" Cheat Sheet. Any penetration tester looking to expand on their

penetration testing toolkit would be wise to look over each of these cheat sheets and see if the sites and pages they are testing actually follow the notations in the cheat sheets. The cheat sheet is also very useful for those who develop and manage websites and web applications regularly. For anyone involved in the programming side of the web application scene, "The Tangled Web: A Guide to Securing Modern Web Applications" should be required reading to ensure they write secure code.

This is not a book that should read in a single sitting to absorb everything quickly. Due to the depth and abstract thinking of web security, it will make you think about aspects of web security that you probably have never considered. This book makes it clear that the state of web applications on the internet is in an alarming state, and there is cause for alarm. This book also alerts us to issues that we have likely never thought of. If you are a developer, penetration tester, or implementer of technology, it is in your best interest to read and re-read The Tangled Web to really grasp the depth of the technical problems you face.

Additional Info & Resources

Please be sure to visit Mr. Zalewski's site:

<http://lcamtuf.coredump.cx/>

Tristan Lawson, CISSP, OSCP, C|EH, E|CSA, C|HFI, GXPn, GWAPT, GCIH, GISP, GSEC, MCITP:EA, CCNA, FCT, FCNSP, JNCIA, JNCIA-FWV, MCSE Security, A+, Net+, Server+, Security+

Tristan Lawson is a Senior Information Security Consultant for Infogressive Inc. out of Lincoln, NE. He brings 10 years' experience in Information technology and is able to exercise his breadth of knowledge performing penetration testing, network security assessments, and assisting companies in deploying security technology. In addition to his passion for Information Security, Tristan also has a passion for marine biology and is actively pursuing a Master's degree in Information Assurance from University Nebraska Omaha.