To understand the vulnerabilities in web browsers and how to strengthen them, it is necessary to learn the methods of infiltrating and wreaking havoc on browsers. The complex dynamics of this particular contradiction are presented by authors Wade Alcorn, Christian Frichot and Michele Orru in their book *The Browser Hacker’s Handbook*. Web browsers are today’s *de facto* operating systems, and their vulnerabilities and exploitable flaws are not only manifold, but also unprecedented in scale and complexity. This book discusses the topic in a unique tutorial-type methodology, depicting various web attacks and exploits into the network.

This book features a review of vulnerabilities of commonly used browsers including Mozilla Firefox, Internet Explorer and Google Chrome. It enables the reader to leverage browsers as the springboard into a target network during penetration testing and assessment. It provides techniques to attain and manage controls over the target browser, yielding assets and asset control. It also facilitates understanding of exploits that expose the weaknesses of plug-ins and extensions, trapdoors into browsers, and the methods in which interprotocol communication can further exploit the internal network systems from a compromised browser.

This book delves into practical usage and application of open-source tools and diverse programming scripts, which can be used for exploiting web browsers. It provides an extensive array of illustrations on exploiting web browsers, and these are written in various computer languages. Throughout the book are screenshots of actual events describing web attacks, code writings, definition boxes, and chapter-end questions and reference notes that aid the understanding of the reader and provide the practical guidance necessary for this specialized IT area.

The book briefly covers theory, but focuses more on functions and coding scripts that readers can actually put into practice. An extensive array of methods, codes and techniques in hacking the web is treated, as is the deployment of open-source projects such as Metasploit and the Browser Exploitation Framework (BeEF), which was developed by one of this book’s authors, Wade Alcorn. These exploitation frameworks are utilized in illustrating vulnerabilities in web browsers.

The book’s focus appears mono-themed, i.e., attacks and exploits, and it could have been helpful to also discuss tactics of countering web exploits. The chapter on attacking plug-ins could also be expanded, and exploits of applications such as .jpeg files would be good to have as well. Despite these minor shortcomings, the sheer scope of web exploits and hacking methodologies covered in this book make it a must-have for anyone who needs to know what could be lurking behind their corporate and private browsing sessions.

**EDITOR’S NOTE**

*The Browser Hacker’s Handbook* is available from the ISACA® Bookstore. For information, visit www.isaca.org/bookstore, email bookstore@isaca.org or telephone +1.847.660.5650.