Preface

Have you ever wondered why all of a sudden, normal users start posting strange messages on social networks? How wireless routers can be controlled remotely? Why eBay accounts could be hijacked with a single HTTP request? Or why a news Web site suddenly shows a page from the Syrian Electronic Army? All of these incidents were possible due to attackers controlling some code within the victim's browser, a result of the current state of practice in Web security, which is less than stellar. As security researchers, we are concerned by the large gap between the state of practice and the currently available security technologies, which are often inspired by security research. In an effort to improve this situation, we have written this book, which gives a detailed view on the client-side Web security landscape. We explicitly focus on client-side security vulnerabilities, which are exploited from within a browser or explicitly target the browser, because they generally receive less attention compared to their server-side counterparts. In total, we cover 13 attacks, for which we give a detailed description, an overview of traditional mitigation techniques, and current state-of-the-art research. For each attack, we also describe the current state of practice in Web applications, and define the best practices to defend against these attacks in the modern age.

We have written this book with several target audiences in mind. It offers *students, teachers, and trainers* an introduction into the field of client-side Web security, with an extensive reference list for learning more about each topic. The best practices can be translated into teaching material for secure software development courses. The book helps *junior researchers* to quickly get up to speed in the field, and offers an overview of the current state-of-the-art for *experienced researchers*, who are looking for new opportunities to explore. Finally, *developers and security practitioners* get an overview of the current state of practice, and the upcoming state-of-the-art technologies. They should use the best practices in the book to improve the state of practice, which is beneficial for all users on the Web.

This book grew from our experience as security researchers[1] working on Web security, with a strong focus on client-side Web security topics such as cross-site request forgery, cross-site scripting, session management problems, and clickjacking. We also actively participate in European Web security projects, such as STREWS[2], WebSand[3], and NESSoS[4], and collaborate with the W3C and IETF standardization committees, further expanding our view on the current state of practice, state-of-the-art, and best practices.

We would like to explicitly acknowledge the support of the Agency for Innovation by Science and Technology (IWT), the STREWS project, where a preliminary version of this book was written as a first deliverable, and the IWT-SBO project SPION[5], which provided valuable insights in the privacy and security concerns of contemporary Web applications.

[1] Philippe De Ryck, Lieven Desmet, and Frank Piessens are affiliated with the *iMinds-DistriNet* research group at *KU Leuven University (Belgium)*, and Martin Johns is affiliated with *SAP Research (Germany)*.

[2] https://www.strews.eu/.

[3] https://www.websand.eu/.

[4] http://www.nessos-project.eu/.

[5] http://www.spion.me/.

http://www.springer.com/978-3-319-12225-0

Primer on Client-Side Web Security

De Ryck, P.; Desmet, L.; Piessens, F.; Johns, M.

2014, X, 111 p. 13 illus., 12 illus. in color., Softcover
ISBN: 978-3-319-12225-0