Data Exfiltration in the Face of CSP

Steven Van Acker, Daniel Hausknecht, Andrei Sabelfeld

Abstract

Cross-site scripting (XSS) attacks keep plaguing the Web. Supported by most modern browsers, Content Security Policy (CSP) prescribes the browser to restrict the features and communication capabilities of code on a web page, mitigating the effects of XSS. This paper puts a spotlight on the problem of data exfiltration in the face of CSP. We bring attention to the unsettling discord in the security community about the very goals of CSP when it comes to preventing data leaks. As consequences of this discord, we report on insecurities in the known protection mechanisms that are based on assumptions about CSP that turn out not to hold in practice. To illustrate the practical impact of the discord, we perform a systematic case study of data exfiltration via DNS prefetching and resource prefetching in the face of CSP. Our study of the popular browsers demonstrates that it is often possible to exfiltrate data by both resource prefetching and DNS prefetching in the face of CSP. Further, we perform a crawl of the top 10,000 Alexa domains to report on the cohabitance of CSP and prefetching in practice. Finally, we discuss directions to control data exfiltration and, for the case study, propose measures ranging from immediate fixes for the clients to prefetching-aware extensions of CSP.