Current state of research on cross-site scripting (XSS) – a systematic literature review

ABSTRACT

Context: Cross-site scripting (XSS) is a security vulnerability that affects web applications. It occurs due to improper or lack of sanitization of user inputs. The security vulnerability caused many problems for users and server applications. Objective: To conduct a systematic literature review on the studies done on XSS vulnerabilities and attacks. Method: We followed the standard guidelines for systematic literature review as documented by Barbara Kitchenham and reviewed a total of 115 studies related to cross-site scripting from various journals and conference proceedings. Results: Research on XSS is still very active with publications across many conference proceedings and journals. Attack prevention and vulnerability detection are the areas focused on by most of the studies. Dynamic analysis techniques form the majority among the solutions proposed by the various studies. The type of XSS addressed the most is reflected XSS. Conclusion: XSS still remains a big problem for web applications, despite the bulk of solutions provided so far. There is no single solution that can effectively mitigate XSS attacks. More research is needed in the area of vulnerability removal from the source code of the applications before deployment.

Keyword: Systematic literature review; Cross-site scripting; Security; Web applications