The limitations of cross-site scripting vulnerabilities detection and removal techniques

ABSTRACT

Web applications have become very important tools in our daily activities as we use them to share and get information, conduct businesses, and interact with family and friends on social media through the Internet. Despite their importance, web applications are plagued with many security vulnerabilities that enable hackers to attack them and compromise user information and privacy. Cross-site scripting vulnerabilities are a type of injection vulnerabilities existing in web applications. They can lead to attacks in web applications due to the lack of proper validation of input data in the affected web pages of an application. Many approaches and techniques have been proposed to mitigate this type of vulnerabilities. However, these solutions have some limitations and cross-site scripting vulnerabilities still remain as a major security problem for web applications. This paper explores and presents the existing techniques for detecting and for removing cross-site scripting vulnerabilities in web application. It gives an overview of cross-site scripting as a security issue in web application and its different types. The advantages as well as the limitations of each techniques are highlighted and discussed. Based on the limitations, some possible future research directions are identified, and recommendations are given as reference for researchers interested in this topic.

Keyword: Cross-site scripting; Cross-site scripting attacks; Cross-site scripting vulnerabilities; Web application security