Removing cross-site scripting vulnerabilities from web applications using the OWASP ESAPI security guidelines

ABSTRACT

Software security vulnerabilities are present in many web applications and have led to many successful attacks on a daily basis. These attacks, including cross-site scripting, have caused damages for both web site owners and users. Cross-site scripting vulnerabilities are easy to exploit but difficult to eliminate. Most solutions provided only focus on preventing attacks or detecting the vulnerabilities. Very few research works have addressed eliminating these vulnerabilities from the web applications source codes. In this paper, we propose an approach to remove cross-site scripting vulnerabilities from the source code before an application is deployed. We make use of the OWASP cross-site scripting prevention rules as guideline in our approach. The proposed approach is, so far, only implemented and validated on Java-based Web applications, although it can be implemented in other programming languages with slight modifications. Initial evaluation results have indicated promising results.

Keyword: Cross-site scripting; Software security; Vulnerability removal