Comparing web vulnerability scanners with a new method for SQL injection vulnerabilities detection and removal EPSQLiFix

ABSTRACT

Web vulnerabilities have become a major threat to the security of information and services accessible via the internet. Dynamic analysis based Web Vulnerability Scanners (WVS) have been employed to facilitate detection of vulnerabilities, though, such scanners could not remove the detected vulnerabilities. Empirical evidences show that some existing static analysis techniques targeted both detection and removal of vulnerabilities. However, these techniques are not adequately effective – they report considerably large number of false positives and do not achieve fully automatic vulnerabilities removal. Although, clear understanding of the workflow of WVSs is very essential in designing more improved scanners, current literature does not provide a comprehensive presentation on workflow of WVSs. Thus, this paper presents thorough description of generic WVS through synthesis and aggregation of knowledge. In addition, the paper presents overview of an Evolutionary Programming (EP) based static analysis method for automatic detection and removal of vulnerabilities called EPSQLiFix. Lastly, the paper compares the workflow of WVSs to that of EPSQLiFix method.

Keyword: SQL injection; Reachability analysis; Vulnerability detection and removal