

Enhanced pushdown automaton based static analysis for detection of SQL injection Hotspots in web application

ABSTRACT

SQL injection Hotspots (SQLiHs) are Application's Entry Points (AEPs) through which SQL injection is possible, subject to the application's internal sanitization or validation capabilities. Since not all AEPs are SQLiHs, one serious challenge during testing of very large web application for detection of SQL Injection Vulnerabilities (SQLiVs) is how to reliably decide which AEPs to consider for the test and which AEPs are unnecessary? In this paper, we propose a new Pushdown Automaton (PDA) based static analysis technique for detection of SQLiHs in web applications. The goal is to produce concrete information that can reliably and confidently guide both human tester/developer and SQLiVs detection tools/techniques as to which part of the source code to concentrate their efforts during detection and fixing of SQL injection flaws in an application. The proposed technique is an integral part of an on-going research on automated method for detection and removal of SQLiVs in web application. Experimental evaluation of the method is in progress. However, preliminary results show that the proposed technique is both feasible and effective.

Keyword: Context free grammar; Data flow path; Sensitive sink; Vulnerabilities