Defining fitness function for search based assessment of grammar reachability

ABSTRACT

Certain generalized graph nodes reachability problems, such as data dependency flow, have been reformulated as Context Free Grammar (CFG) nonterminals reachability problems, and addressed using grammar reachability analysis. The reformulation efforts could be extended by reformulating such problems as Search Based CFG reachability problems, addressable using search algorithms, such as Evolutionary Programming (EP). However, this calls for the need of fitness function that can assess reachability attained by candidates during search process. This paper defines set of fitness functions that can be applied for search based assessment of reachability between non terminal symbols of CFG. Further, the paper highlights how the set of fitness functions support reformulation of data dependency flow for detection of SQL Injection Vulnerabilities as an EP search problem.

Keyword: SQL injection; Static analysis; Vulnerabilities detection; Web application