SYNTACTIC ANALYSIS TO COMPARE THE BEHAVIOR OF JAVA AND PHP TOWARD SQL INJECTION

Alvin Sulendra 1100060846

Abstract

The aim of this research is to compare the different behaviors from different programming languages given a list of SQL injection attack string and to create useful attack strings, since it is believed that automated tools are difficult to use and often the result is unreliable.

The research method the author used first was collecting data from various sources. From the data collected the author created a syntactic tree that was used to create SQL attack syntaxes. Then author used some of the syntaxes and tested it in the demo platform that the author created. After testing the syntaxes the author make comparison of the Java and PHP behavior against SQL injection in MySQL database.

The results of this research are a list of SQL injection syntaxes example, a syntactic tree that use to construct SQL injection attack string, and comparison of behavior between Java and PHP toward SQL injection attack. The comparison showed that there were different behaviors between Java and PHP. Therefore database fingerprint could be inferred from the behavior showed by injecting the SQL injection.

Keyword
SQL vulnerability, SQL injection, Java, PHP, SQL injection syntaxes, syntactic tree, Database, Database Fingerprint, MySQL