ABSTRACT

SQL injection attacks are a serious security threat to Web Applications. It allows the attackers to gain unauthorized access to the databases underlying the applications and to retrieve potentially sensitive information from the databases. SQL injection attack occurs when a malicious user, through specially crafted input, send a query that functions differently than the programmer intended structure of a vulnerable web application. In this report, we cited a brief description along with examples of various kinds of SQL injection attacks. We also developed two modules to experiment the detection mechanism of SQL injection attacks using Support Vector Machine (SVM) proposed in [1] and the other is based on Parse Tree Evaluation on a predefined grammar reported in [2]. It has been observed that these methods are considered to be one of the best methods in detecting SQL injection attack. The experimental results are also considered to be satisfactory due to the high detection rate found with method [1] compared to method [2].