Abstract

In today's world, web applications play a very important role in individual life as well as in any country's development. Web applications have gone through a very rapid growth in the recent years and their adoption is moving faster than that was expected few years ago. Now-a-days, billions of transactions are done online with the aid of different Web applications. Though these applications are used by millions of people, in many of these applications the security level is weak, which makes them vulnerable to various web application attacks. In most of the web applications, users have to be authenticated before any communication is established with the back-end database. An arbitrary user should not be allowed access to the system without authentication. However, it is found that sometimes, a maliciously crafted user input may give access to unauthorized users. This is mostly accomplished via SQL injection input. In spite of the development of different approaches to prevent SQL injection, it still remains an alarming threat to Web applications

There are many techniques which have been developed by the researchers to detect SQL injection attack. In our work, at first, we have done a comprehensive study on SQL injection attack and its detection methods. Next, we have experimented its detection using some standard and well known classification techniques – Bayesian, SVM and Edit Distance. Out of which one is probabilistic approach i.e. the Bayesian theorem, and one non-probabilistic approach i.e. the support vector machine and the third one i.e. Edit Distance is basically a string matching based approach. We finally, performed a comparative study of these approaches based on their ability to detect various types of attack queries.

Key Words: Attack, Injection, SQL, Vulnerability, Web