Abstract

SQL injection is a type of attack used to gain, manipulate, or delete information in any data-driven system regardless of whether the system is online or offline and whether this system is a web or non-web based. A common approach for an attacker to launch SQLIA is by modifying the user input to contain partial SQL queries and trick the server into executing them. In this paper, a literature review of the SQL injection attacks and their mitigation is presented. It shows that the study of SQL injection in general has been conducted in diverse range of areas. The main objective of this paper is to give an elaborate study on different types of SQL injection, their mitigation strategies, critiques of past approaches and finally the knowledge gap. It seeks to create knowledge on work done by others in the area of SQL injection attacks in web applications which remains a threat up-to-date despite the numerous studies done on the same field.

References
1. [Angelo et al.] Angelo Ciampa, Corrado Aaron Visaggio, Massimiliano Di Penta: "A heuristic-based approach for detecting SQL-injection vulnerabilities in Web applications".


Index Terms
Keywords

Structured Query Language, Structured Query Language Injection Attacks, Web Application Keywords.