Abstract

SQL injection is a predominant type of attack which targets web applications and databases. SQL injection bypasses the authentication logic and breaks the confidentiality of the database or manipulates the database. It helps the attacker to obtain unauthorized access into the back end database. Vulnerability exists within a web application when it does not provide a proper validation system for the data entered by the user in the input field. Vulnerability scanners aid in checking vulnerabilities embedded in a web application and has the potential to test invalid forms of input query. However, the limitation lies in the reduction of system availability due to denial of service, especially in case of false positives. In this paper, an approach which focuses on query template based detection of SQL injection attack and reconstruction of queries is proposed. Thus the proposed architecture can mitigate the denial of service and increase the availability by potentially reconstructing malicious queries.

References
1. Kumar, Pranaw, and R. K. Pateriya. "A Survey on SQL injection attacks, detection and
prevention techniques". Computing Communication & Networking Technologies (ICCCNT),
Application."
& Sons, 2002.
algorithm to prevent SQL injection." Trust, Security and Privacy in Computing and
Communications (TrustCom), 2012 IEEE 11th International Conference on. IEEE, 2012.
6. Bisht, Prithvi, Parthasarathy Madhusudan, and V. N. Venkatakrishnan. "CANDID:
Dynamic candidate evaluations for automatic prevention of SQL injection attacks." ACM
Neutralizing SQL-injection attacks." Proceedings of the 20th IEEE/ACM international
applications using positive tainting and syntax-aware evaluation." Software Engineering, IEEE
International Conference on. IEEE, 2005.
11. Johari, Rahul, and Pankaj Sharma. "A survey on web application vulnerabilities (SQLIA,
XSS) exploitation and security engine for SQL injection." Communication Systems and Network
15. Xie, Yichen, and Alex Aiken. "Static Detection of Security Vulnerabilities in Scripting
to prevent SQL injection attacks." Proceedings of the 5th international workshop on Software
SQL-injection attacks and countermeasures." Proceedings of the IEEE International

Index Terms

Computer Science

Software Engineering
Keywords

SQL Injection, Authentication, Vulnerability, Validation, Malicious, Reconstruct.