Abstract

Web application has various input functions which are susceptible to SQL-Injection attack. SQL-Injection occurs by injecting suspicious code or data fragments in a web application. Personal information disclosure, loss of authenticity, data theft and site fishing falls under this attack category. It is impossible to check original data code and suspicious data code using available algorithms and approaches because of inefficient and proper training techniques of dataset or design aspects. In this paper we will use SVM (Support Vector Machine) for classification and prediction of SQL-Injection attack. In our propose algorithm, SQL-Injection attack detection accuracy is (96.47%) and which is the highest among the existing SQL-Injection detection Techniques.

References

- SQL Injection Attack Examples based on the Taxonomy of Orso et al.
- Xiang Fu, Xin Lu, Boris Peltsverger, Shijun Chen; A Static Analysis Framework For Detecting SQL Injection Vulnerabilities; IEEE Transaction of computer software and application conference, 2007.
- Konstantinos Kemalis and Theodoros Tzouramanis; Specification based approach on SQL Injection detection; ACM, 2008.
- V. B. Livshits and M. S. Lam; Finding Security vulnerability in java applications with static analysis; In proceedings of the 14th Usenix Security Symposium, Aug 2005.
- W. G. J. Halfond and A. Orso; Combining Static Analysis and Run time monitoring to counter SQL Injection attacks; 3rd International workshop on Dynamic Analysis, St. Louis, Missouri, 2005, pp. 1.
- Marco Cova, Davide Balzarotti, Viktoria Felmetsger, and Giovanni vigna; Swaddler: An approach for the anamoly based character distribution models in the detection of SQL Injection attacks; Recent Advances in Intrusion Detection System, Pages 63-86, Springerlink, 2007.
- NTAGW ABIRA Lambert and KANG Song Lin; Use of Query Tokenization to detect and prevent SQL Injection Attacks; IEEE,2010.

**Index Terms**

Computer Science

Security

**Keywords**

Sql Injection Database Security Authentication Svm