IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.301

Volume 3, Issue 16, May 2023

Detection of SQL Injection Attacks Using Ensemblimg Machine Learning Techniques

Madugula Karthik Sharma[1], Y. Rajashekhar Reddy[2], B. Pardhu[3], Preethi Jeevan[4]

[1,2,3]Student, Department of Computer Science and Engineering,

[4]Professor, Department of Computer Science and Engineering

Sreenidhi Institute of Science & Technology, Hyderabad, India

Abstract: *SQL injection remains one of the most harmful security exploits from a privacy perspective Information leakage and exonomic loss. Injection attacks are the biggest Vulnerability on the internet. The latest OWASP top 10 report shows that the number of these attacks continues to grow. Traditional Defense strategies often include static, signature-based Intrusion Detection System (IDS) rules. In most cases, they are only effective against previously observed attacks. Many current research uses machine learning techniques that can recognize the unknown. However, the attack can be performance intensive depending on the algorithm. Moreover, recently an intrusion detection strategy involves capturing traffic entering your web application. Collect data from network devices or web application hosts, or from databases in other strategies server log. This project collects traffic from two points: Host web applications and a dataphy applicance mode between your web application host and its MySQL database server.*

Keywords: Decision Tree, Logistic Regression, SQL Injections

REFERENCES

[1] Sonali Mishra, “SQL Injection Detection using Machine Learning”, from https://scholarworks.sjsu.edu/cgi/viewcontent.cgi?arti c le=1727context=etdprojects, on23May2019 pp.10 - 29.

[2] Bojken Shehu and Aleksander Xhuvani, “A LiteratureReviewandComparativeAnalyseson SQL Injection: Vulnerabilities, Attacks and their Prevention and Detection Techniques”from https ://pdfs.semanticscholar.org,Vol.11,Issue4,No 1,July 2014 pp 20 - 34.

[3] SuhaimiIbrahim, “SQLInjectionDetectionand Prevention Techniques” from https://pdfs.semanticscholar.org/ Volume 3, Number 7, August 2011, pp 85 - 89.

[4] G.Wassermann,Z.Su,“Analysisframeworkfor security in web applications,” In: Proceedings of the FSE Workshop on Specificationand Verification of Component-Based Systems, fromhttps://link.springer.com/chapter/10.1007/978 −0 −387 − 44599−15 SAVCBS,pp. 70–78, 2004.

[5] Mei Junjin, “An Approach for SQL Injection Vulnerability Detection,” Proceedings. of the 6th Int. Conf. on InformationTechnology: NewGenerations,LasVegas,Nevada,pp.14-19, Apr. 2009.

[6] V.Haldar, D.Chandra, and M.Franz, "Dynamic Taint Propagation for Java," Proc. 2 1s t Annual Computer Security Applications Conference, Dec 2005.

[7] S.W.Boyd and AD.Keromytis, "SQLrand: Preventing SQL Injection Attacks," Proc. the 2nd Applied Cryptography and Network Security (ACNS) Conference, pp. 292-302, Jun 2004.

[8] G.T.Buehrer, RW.Weide, and P.AG.Sivilotti, "Using Parse Tree Validation to Prevent SQL Injection Attacks," International Workshop on Software Engineering and Middleware (SEM), 2005.

[9] Evans Dogbe, Richard Millham, Prenitha Singh “A Combined Approach to Prevent SQL Injection Attacks,” Science and Information Conference 2013 October 7-9, 2013, London, UK.

[10] Ryohei Komiya, Incheon Paik, Masayuki Hisada, “Classification of Malicious Web Code by Machine Learning,” Awareness Science and Technology (iCAST), 2011 3rd International Conference on, vol., no., pp.406,411, 27-30 Sept. 2011

DOI: 10.48175/IJARSCT-11137