Taxonomy of SQL Injection: ML Trends & Open Challenges

Raed Abdullah Abobakr Busaeed, Wan Isni Sofiah Wan Din, Quadri Waseem and Azlee Bin Zabidi

Faculty of Computing, Universiti Malaysia Pahang Al-Sultan Abdullah, Pekan, Pahang, Malaysia

ABSTRACT

SQL injections are a significant and ever-present threat to web applications and database security. During these attacks, malicious SQL statements are injected into input fields of data-driven systems, leading to unauthorized access and data breaches. Consequently, a need is generated to understand the nature of the attacks, detection, and effective prevention techniques. This research paper focuses on providing a taxonomy and comprehensive survey of SQL injection attacks, detection, and prevention, including their various types and techniques. Additionally, it explores the current state-of-the-art and evaluation for attacks, detection, and prevention techniques. This research paper also discusses and provides a taxonomy of current machine learning (ML) trends (Taxonomy) and their open challenges for detection purposes. Finally, this paper ends with a discussion aiming to equip system administrators, researchers, scientists and practitioners with the knowledge and strategies to mitigate the risks associated with SQL injection attacks effectively. Eventually, this will help to enhance the security and resilience of web applications and databases in the face of this significant threat.

KEYWORDS

Machine Learning, Attack, Detection, Prevention, SQL, SQL Injection

ACKNOWLEDGEMENT

This research was fully funded by the UMP Research Grant Scheme under grant RDU220374 and Tabung Persidangan Dalam Negara (TPDN), UMP.