Batch No: 15

Real-Time SQL Injection Attack Detection in Network Environments

ABSTRACT

SQL Injection (SQLi) attacks remain a prevalent and dangerous threat to web-based applications, often leading to unauthorized data access, data breaches, and system compromise. As these attacks evolve in complexity and frequency, real-time detection within network environments has become critical to maintaining system security. This research presents a novel framework for the real-time detection of SQL Injection attacks by analyzing network traffic patterns and payload content. The proposed system leverages machine learning algorithms, including Decision Trees and Long Short-Term Memory (LSTM) networks, to identify anomalous query structures embedded in HTTP requests. Unlike traditional rule-based intrusion detection systems (IDS), our model adapts to new attack variants by continuously learning from traffic data. Network packets are parsed and inspected at the application layer to extract SQL-related payloads, which are then evaluated for malicious intent. Experimental results on benchmark datasets demonstrate the system's high detection accuracy and low false positive rate, validating its effectiveness in dynamic and high-volume network environments. The proposed approach not only enhances early threat identification but also supports integration with existing intrusion prevention systems (IPS) for proactive defense. This research contributes to the advancement of intelligent, real-time security solutions for safeguarding modern web infrastructure.

BATCH NO :15

TEAM MEMBER

ROSHAN KUMAR	(810421104142)
RUPESH KUMAR	(810421104143)
VIKASH KUMAR	(810421104188)

GUIDED BY:

MS. M. HEMALATHA, M.E.,

ASSISTANT PROFESSOR,

DHANALAKSHMI SRINIVASAN
ENGINEERINGCOLLEGE(AUTONOMOUS),
PERAMBALUR