ANALISIS DIGITAL FORENSIK PADA APLIKASI WEB UNTUK DETEKSI SQL INJECTION

SITI SHAKIVA HILYA SOERONO

ABSTRAK

Dalam era digital saat ini, serangan *SQL Injection* masih menjadi salah satu ancaman serius terhadap keamanan aplikasi web. Penelitian ini bertujuan untuk menganalisis dan menerapkan metode digital forensik dalam mendeteksi serta merespons serangan *SQL Injection* pada *website* PT XYZ. Dengan integrasi *ELK Stack* (*Kibana SILK*) dan *Grafana*, penelitian ini melakukan pengumpulan dan analisis data log *server*, serta visualisasi data untuk mempercepat proses pemantauan dan investigasi insiden. Hasil pengamatan periode Januari hingga April 2025 mencatat sebanyak 243 serangan *SQL Injection*, dengan lonjakan serangan pada akhir Maret dan April, serta identifikasi 20 IP unik pelaku serangan. *Payload* terbanyak yang terdeteksi adalah `'UNION SELECT'`, `'OR '1'='1' --'`, dan `'DROP TABLE'`. Penerapan metode ini terbukti efektif dalam mendeteksi pola serangan, mempercepat respons keamanan, serta memberikan rekomendasi mitigasi untuk meningkatkan perlindungan aplikasi web terhadap ancaman serupa di masa mendatang.

Kata Kunci: Digital Forensik, *SQL Injection*, Keamanan Aplikasi Web, Analisis Log, *Kibana SILK*, *Grafana*

DIGITAL FORENSIC ANALYSIS ON WEB APPLICATIONS FOR SQL INJECTION DETECTION

SITI SHAKIVA HILYA SOERONO

ABSTRACT

In the current digital era, SQL Injection remains a significant threat to web application security. This study aims to analyze and apply digital forensic methods to detect and respond to SQL Injection attacks on the PT XYZ website. By integrating the ELK Stack (Kibana SILK) and Grafana, this research collects and analyzes server log data and visualizes it to accelerate incident monitoring and investigation processes. During the observation period from January to April 2025, a total of 243 SQL Injection attacks were recorded, with a surge in late March and April, and 20 unique attacker IPs identified. The most commonly detected payloads included `'UNION SELECT'`, `'OR '1'='1' --'`, *and* `'DROP TABLE'`. *The implemented methods proved effective in detecting attack patterns, speeding up security response, and providing mitigation recommendations to improve web application protection against similar threats in the future.*

Keywords: Digital Forensics, SQL Injection, Web Application Security, Log Analysis, Kibana SILK, Grafana