Abstract

SQL injection attacks pose a significant threat to web applications and database systems. This study evaluates the effectiveness of integrating Security Information and Event Management (SIEM) with multi-Wazuh agents and diverse Web Application Firewalls (WAF) to detect threats collaboratively SQL injection attacks. The system was designed using two web servers, each protected by a different WAF— ModSecurity and NAXSI—and a centralized SIEM server employing Wazuh. Tests were conducted using various SQL injection techniques, including Time-Based Blind, Error-Based, and Union-Based attacks. The results indicated that ModSecurity proved more effective in detecting and mitigating Time-Based and Error-Based SQL inj ection attacks, while both WAFs performed similarly in handling Union-Based attacks. The Wazuh platform collected and reported attack data efficiently, offering security teams a clear and centralized view of detected threats. This integration demonstrates the feasibility of implementing collaborative threat detection using a SIEM and diverse WAFs to enhance web application security against SQL injection attacks.

Keywords—SQL injection, SIEM, WAF, multi-agent, cybersecurity, collaborative detection