ABSTRACT

Server security is a critical aspect in the increasingly developing digital era, where cyber threats such as SQL injection, brute force attacks, and Distributed Denial of Service (DDoS) continue to experience significant increases. The complexity of server security problems lies in various types of attacks that can exploit security vulnerabilities, requiring a comprehensive testing system to identify and evaluate vulnerabilities before they are exploited by irresponsible parties.

This research develops a Website-based server security testing platform that integrates two main tools, namely Nmap and Nikto scanner, in an easily accessible web interface. This platform is designed using the Django framework with Python programming language for the backend, as well as HTML, CSS, and JavaScript for the frontend. The system is equipped with automatic scanning features, detailed reporting based on CVSS and OWASP Top 10 standards, and generative AI-based improvement recommendations that can be downloaded in PDF format.

The test results show that this platform is able to perform security scanning consistently with a good level of accuracy. Testing was conducted on three target categories: localhost on one device, localhost from different devices, and Websites from the internet, with each category tested three times to ensure result consistency. Reliability testing using Apache JMeter proves that the platform has a 0% error rate with increasing throughput as the number of requests increases, although it experiences performance degradation under very high loads. The platform successfully generates accurate vulnerability reports with Critical, High, Medium, Low, and Info categorization, accompanied by security scores that can help administrators make decisions for system improvements.

Keywords: Nikto, Nmap, server *security*, vulnerability *scanning*, *Website security* testing