ABSTRACT

Web applications, as one of the digital media that are often targeted by cyberattacks, experience around 75% of total cyberattacks. In 2023, as many as 30,000 websites are hacked every day, underscoring the vulnerability of web applications due to their availability that must be constant for users. One type of web application security threat is the existence of requests containing malicious payloads such as SQLi and XSS to web applications. Another type of web application security threat is DDoS. These attacks make the website dysfunctional or inaccessible.

To overcome this problem, a solution was designed in the form of designing and implementing WAF, rate limiting, as well as intrusion detection system for web application security. In the solution, WAF is implemented to filter malicious payloads in the form of SQLi and XSS. Meanwhile, rate limiting is implemented to filter DDoS attacks based on a specified threshold. Apart from that, Snort was implemented to send messages to the Telegram application as an alert when these three attacks occurred.

Based on test results, WAF obtained a security quality score of 99.6% and detection quality of 92.3%. The average throughput without rate limiting is 13382.389916 kbits/s, while the average throughput with rate limiting is 8004.082379 kbits/s. The average packet loss without rate limiting is 0.191928% while the average packet loss with rate limiting is 0.011805%. The average delay without rate limiting is 0.000355 s, while the average delay with rate limiting is 0.000284 s. The average jitter without rate limiting is 0.000012 s, while the average jitter with rate limiting is 0.000020 s. On IDS, Snort successfully sends warning messages according to the type of attack that occurred.

Keywords: web application firewall, rate limiting, intrusion detection system, cyber defense.