ABSTRACT

With an increase in Bruteforce attacks globally, including those that occurred in Indonesia, as well as significant SQL Injection vulnerabilities in web applications, as well as a record DoS attack recorded in the first quarter of 2023, it becomes clear that web server security needs to be improved to ensure integrity, data validity, and service availability for users. In dealing with this challenge, Intrusion Prevention System (IPS) has become a common approach. IPS has the function of detecting and preventing cyber attacks by analyzing network traffic in realtime, becoming an effective protection solution. IPS can protect against Bruteforce, SQL Injection, and DoS attacks, including ICMP floods which place an excessive load on server resources. The IPS evaluation test showed satisfactory results, where there was a decrease in CPU usage from 15.8% to 7.7%, memory usage increased from 47.8% to 61.7%. In SQL Injection attacks, CPU usage decreased from 7.1% to 5.5%, memory remained 48.4%. DoS attacks saw CPU usage drop drastically from 47.7% to 7.1%, with memory usage steady at 60.8%. Suricata managed to maintain a response time of 2.6 ms. In addition, research has successfully applied Telegram *bot to provide information to network administrators about the threat of attacks with a CPU usage limit of more than 70%. This mechanism allows administrators to enable mitigation actions in a timely manner. In conclusion, Suricata is effective in protecting the system from Bruteforce, SQL Injection, and DoS attacks. Special attention is needed on resource usage during DoS attacks for better efficiency. Test data shows that IPS is effective against Bruteforce, SQL Injection and DoS attacks with good performance.*

Keywords**:** *Intrusion Prevention System (IPS), Bruteforce, SQL Injection, DoS, Telegram*