ABSTRACT

Many web application developers neglect the security aspect of web applications, resulting in them being exploited by hackers. According to the Web Security Report by SiteLock in 2022, it was found that there were 172 attacks per day for a single website, and the website was accessed by bots 2,306 times per week. Bots are used by hackers to search for vulnerabilities in websites. The number of attacks in 2022 increased by 210% compared to 2020. There were two recorded highest vulnerability types, which are Cross-Site Scripting (XSS) with one million website pages affected, and SQL Injection with 332,000 website pages affected. To address various security issues related to web applications, a system is needed to prevent harmful attacks.

A WordPress plugin has been designed to display data from attacks and log reports, which is integrated with a SIEM (Security Information and Event Management) and a proxy-based WAF (Web Application Firewall) for security purposes. The proxy-based WAF enhances the website's security by checking for malicious requests based on proxy rules. It can detect and identify attacks based on OWASP (Open Web Application Security Project) standards, block IP addresses that make malicious requests, and log and store the IP addresses associated with malicious requests. The web application firewall utilizes a proxy that takes the form of a prototype. The SIEM collects security data from various sources, such as event logs, which include information about network activities, source and destination IP addresses, and severity. The SIEM transforms this data into a format that is easy to understand.

Based on the evaluation of XSS, SQL Injection, and LFI attacks, this system is capable of checking with an effectiveness rate of 100% for XSS, 97% for SQL Injection, and 74% for LFI, based on the standards provided by OWASP in their OWASP Cheat Sheet.

Keyword : OWASP, *Plugin*, SIEM, WAF