

ABSTRAK

Penelitian ini dilakukan karena serangan *SQL Injection* masih menjadi salah satu ancaman utama terhadap keamanan aplikasi web sehingga diperlukan mekanisme perlindungan tambahan berupa Web Application Firewall (WAF). Tujuan penelitian ini adalah membandingkan efektivitas *Modsecurity* dan *Naxsi* dalam mendeteksi serta mencegah serangan *SQL Injection*. Variabel yang diteliti meliputi tingkat efektivitas pemblokiran payload *SQL Injection* oleh *Modsecurity* dan *Naxsi* pada aplikasi DVWA. Penelitian menggunakan metode eksperimen dengan mengacu pada standar OWASP yang meliputi tahap reconnaissance, scanning, eksperimen, dan analisis. Pengujian dilakukan menggunakan aplikasi DVWA sebagai target serangan, OWASP ZAP sebagai alat pengujian, serta 63 payload *SQL Injection* yang diujikan pada modul *SQL Injection* dan *SQL Injection Blind*. Analisis dilakukan secara kuantitatif berdasarkan jumlah payload yang berhasil diblokir dan nilai efektivitas kontrol yang diperoleh dari masing-masing WAF. Hasil penelitian menunjukkan bahwa sebelum penerapan WAF tidak terdapat payload yang berhasil diblokir sehingga efektivitas kontrol bernilai 0%. Setelah penerapan *Modsecurity*, sebanyak 30 dari 63 payload berhasil diblokir dengan efektivitas sebesar 47,62%, sedangkan *Naxsi* berhasil memblokir 46 dari 63 payload dengan efektivitas sebesar 73,02%. Berdasarkan hasil tersebut, dapat disimpulkan bahwa kedua WAF mampu meningkatkan keamanan aplikasi web terhadap serangan *SQL Injection*, namun *Naxsi* menunjukkan tingkat efektivitas yang lebih tinggi dibandingkan *Modsecurity* pada lingkungan pengujian yang digunakan.

Kata kunci: *Web Application Firewall*, *Modsecurity*, *Naxsi*, *SQL Injection*, DVWA.

ABSTRACT

This research was conducted because SQL Injection attacks are still one of the main threats to web application security so that additional protection mechanisms are needed in the form of a Web Application Firewall (WAF). The purpose of this research is to compare the effectiveness of Modsecurity and Naxsi in detecting and preventing SQL Injection attacks. The variables studied include the level of effectiveness of blocking SQL Injection payloads by Modsecurity and Naxsi on the DVWA application. The research uses an experimental method with reference to the OWASP standard which includes the reconnaissance, scanning, experimentation, and analysis stages. Testing was carried out using the DVWA application as the target of the attack, OWASP ZAP as a testing tool, and 63 SQL Injection payloads tested on the SQL Injection and SQL Injection Blind modules. The analysis was carried out quantitatively based on the number of payloads successfully blocked and the control effectiveness value obtained from each WAF. The results showed that before the implementation of WAF, no payloads were successfully blocked, resulting in a control effectiveness of 0%. After the implementation of Modsecurity, 30 out of 63 payloads were successfully blocked with an effectiveness of 47.62%, while Naxsi successfully blocked 46 out of 63 payloads with an effectiveness of 73.02%. Based on these results, it can be concluded that both WAFs are able to improve web application security against SQL Injection attacks, but Naxsi showed a higher level of effectiveness than Modsecurity in the test environment used.

Keywords: Web Application Firewall, Modsecurity, Naxsi, SQL Injection, DVWA.