ABSTRAK

Seiring berkembangnya teknologi informasi, keamanan web menjadi semakin penting, namun keamanannya menghadapi tantangan besar akibat ancaman *siber*. Ancaman *siber* seperti *SQL Injection, XSS*, dan *CSRF* menjadi tantangan besar bagi pengelola web. Metode penelitian terdiri dari beberapa tahap yaitu studi litetatur, perencanaan pengujian, implementasi WAF, serta evaluasi kerentanan menggunakan *OWASP ZAP*. Penelitian ini merancang strategi pengujian menggunakan *VA* untuk mengidentifikasi celah keamanan pada *web* sakattaku.com yang dilindungi *WAF* serta mengevaluasi efektivitasnya. Pengujian dilakukan dengan membandingkan tingkat kerentanan pada *website* yang menggunakan *WAF* dan yang tidak menggunakan *WAF. WAF* diimplementasikan dengan menggunakan *ModSecurity* dan aturan *OWASP Core Rule Set*. Hasil pengujian menunjukkan bahwa sebelum *WAF* website memiliki 3 kerentanan *high*, 7 kerentanan *medium*, 7 kerentanan *low*. Setelah *WAF* diimplementasikan menunjukkan bahwa kerentanan tingkat *high* berhasil dieliminasi, meski masih terdapat 1 kerentanan *medium* dan 5 *low*. Aturan keamanan tambahan diterapkan untuk mengurangi risiko lebih lanjut, membuktikan bahwa *WAF* efektif dalam meningkatkan keamanan *web.*

Kata kunci : *ModSecurity, OWASP Core Rule Set, OWASP ZAP, Vulnerability Assessment, Web Application Firewall*

ABSTRACT

As information technology develops, web security is becoming increasingly important, but its security faces great challenges due to cyber threats. Cyber threats such as SQL Injection, XSS, and CSRF are a big challenge for web managers. The research method consists of several stages, namely literature study, test planning, WAF implementation, and vulnerability evaluation using OWASP ZAP. This research designs a testing strategy using Vulnerability Assessment (VA) to identify security gaps on the sakattaku.com web protected by Web Application Firewall (WAF) and evaluate its effectiveness. Testing is done by comparing the level of vulnerability on websites that use WAF and those that do not use WAF. WAF is implemented using ModSecurity and OWASP Core Rule Set rules. The test results show that before WAF the website has 3 high vulnerabilities, 7 medium vulnerabilities, 7 low vulnerabilities. After the WAF was implemented, it showed that the high level vulnerabilities were eliminated, although there were still 1 medium and 5 low vulnerabilities. Additional security rules were implemented to further reduce risks, proving that WAF is effective in improving web security.

Keyword : *ModSecurity, OWASP Core Rule Set, OWASP ZAP, Vulnerability Assessment, Web Application Firewall*