ABSTRACT

The web application firewall is a method of protecting against threat attacks on web applications. The implementation of a web application firewall can block several attacks, in terms of security problems, it can be analyzed how efficient the web application firewall is in protecting web applications. In this study, the implementation and analysis of a web application firewall is carried out based on vulnerabilities and threats in testing attacks on web applications that have installed a web application firewall as a control. The object used is DVWA (Damn Vulnerability Web Application) with the aim of knowing vulnerabilities and threats. The experiment was conducted based on the PTES (Penetration Testing Execution Standard) standard as the basis for the exploitation of five vulnerabilities. The web application firewall is able to block three attacks, namely SQL Injection, Cross-Site Scripting, Local File Inclusion. Based on the total attacks carried out, it can be used as a quantitative analysis that is 60%. While qualitative, using the results of vulnerability scanning with Acunetix based on the severity of the vulnerability that can be secured by a web application firewall.

Keywords : web application firewall, vulnerability, threat, control, PTES.