ABSTRACT

Exploitation against web applications can be formulated into an attack tree. This research aims to explore the relationship between the attack tree and exploitation characteristics based on time and cost metrics. The study is based on exploitation experiments conducted on the DVWA platform. The exploitation stages are used to construct the attack tree, which is then organized based on two conditions: with Web Application Firewall (WAF) and without WAF. The attack tree is composed of five types of exploitation: SQL Injection, XSS (Reflected), Command Injection, CSRF, and Brute Force. The analysis results without WAF show that the XSS (Reflected) attack tree occupies the top position with a score of 53.69, while the SQL Injection attack tree ranks last with a score of 682.49. However, with WAF, the XSS (Reflected) attack tree remains at the top with a score of 61.11, and the SQL Injection attack tree still occupies the last position, but with a lower score of 207.22. The characteristics of the results indicate that SQL Injection and brute force experience a change in position when WAF is enabled due to certain steps being blocked. On the other hand, for the XSS (Reflected), Command Injection, and CSRF attack trees, there is an increase in score attributed to the use of WAF. Consequently, this relationship can be used to categorize attack trees based on time and cost metrics. Thus, the comparison results lead to the conclusion that the lower the score, the less time and steps are required to execute the attack tree successfully. Future research opportunities may involve measuring subsystem processes of the system.

Keywords - **attack tree, exploitation, metric, time, cost**