ABSTRACT

The formulation of attack trees can be based on the exploitation stages of web-based applications. This research aims to understand the relationship between attack trees and exploitation characteristics using time and probability metrics. Attack trees were developed on a testing platform using the web-based application DVWA under both protected and unprotected conditions, with and without Web Application Firewall (WAF). Exploitation targeted five vulnerabilities: SQL Injection, XSS (Reflected), Command Injection, CSRF, and Brute Force.The analysis without WAF resulted in the Cross-Site Request Forgery attack tree ranking first with a score of 18.19, while the Brute Force attack tree ranked last with a score of 230.09. With WAF, the Command Injection attack tree obtained the top position with a score of 4.80, and the Brute Force attack tree remained at the bottom with a score of 43.08. The characteristics of the Brute Force attack tree showed significant changes with the presence of WAF, as WAF successfully blocked several exploitation stages. Additionally, the Command Injection had the lowest score among the other exploits. The relationship can be utilized for ranking attack trees based on time and probability metrics. The research findings demonstrated that smaller scores resulted in lower time and probability at each step of the attack tree. Further research could focus on detailed probability metrics and vulnerability factor calculations.

Keywords — attack tree, exploitation, metrics, time, probability