ABSTRAK

Perumusan *attack tree* dapat dilakukan berdasarkan tahapan eksploitasi pada aplikasi berbasis web. Berdasarkan rumusan tersebut, penelitian ini bertujuan untuk memahami relasi antara *attack tree* dan karakter eksploitasi menggunakan metrik *time* dan *probability*. Penyusunan *attack tree* berdasarkan *platform* percobaan terhadap aplikasi berbasis *web* DVWA dengan kondisi terlindungi dan tidak terlindungi oleh *Web Application Firewall* (WAF). Eksploitasi dilakukan berdasarkan lima kerentanan yaitu *SQL Injection*, XSS (*Reflected*), *Command Injection*, CSRF, dan *Brute Force*. Hasil analisis tanpa WAF menghasilkan *Cross-Site Request Forgery attack tree* menempati posisi pertama dengan skor 18,19. *Brute Force attack tree* menempati urutan terakhir dengan skor 230,09. Sedangkan dengan WAF menghasilkan *Command Injection attack tree* menempati posisi pertama dengan skor 4,80. *Brute Force attack tree* menempati urutan terakhir dengan skor 43,08. Karakteristik *Brute Force attack tree* terlihat mengalami perubahan signifikan dengan adanya WAF, karena beberapa tahapan eksploitasi berhasil diblokir oleh WAF. Selain itu, *Command Injection* memiliki skor terendah diantara eksploitasi lainnya. Dari relasi tersebut dapat digunakan dalam perangkingan antar *attack tree* berdasarkan metrik *time* dan *probability*. Hasil penelitian menunjukkan bahwa semakin kecil skor yang dihasilkan, maka waktu dan probabilitas pada setiap langkah *attack tree* semakin rendah. Kelanjutan penelitian ini dapat berupa rincian metrik *probability* dan memperhitungan faktor *vulnerability*.

Kata kunci — ***attack tree*, eksploitasi, metrik, *time*, *probability***