ABSTRAK

Indonesia mengalami peningkatan serangan siber setiap tahun, terutama pada aplikasi web yang berisiko menyebabkan gangguan operasional dan kebocoran data. Penelitian ini bertujuan untuk mengevaluasi keamanan aplikasi web melalui pengujian penetrasi berbasis *black box* menggunakan kerangka kerja ELEMENT. Pengujian difokuskan pada identifikasi kerentanan berdasarkan OWASP *Top* 10 2021, diikuti oleh analisis terhadap hasil yang diperoleh. Berdasarkan analisis tersebut, disusun rekomendasi mitigasi untuk mengurangi risiko dan meningkatkan keamanan aplikasi web yang diuji. Hasil pengujian menunjukkan bahwa aplikasi web target memiliki sejumlah kerentanan, diantaranya adalah sertifikat SSL yang telah kedaluwarsa, *Cross-Site Scripting* (*Reflected*), informasi *email* admin yang ditampilkan secara publik, penanganan kesalahan yang tidak sesuai, potensi terhadap serangan *clickjacking*, penggunaan versi Bootstrap dan PHP yang sudah usang, tidak diterapkannya mekanisme *lockout*, serta tidak adanya verifikasi terhadap integritas *file* eksternal. Kerentanan-kerentanan ini relevan dengan beberapa kategori yang tercantum dalam OWASP *Top* 10 2021. Penelitian ini berhasil mengidentifikasi kerentanan yang relevan, sekaligus menunjukkan bahwa pendekatan pengujian berbasis OWASP *Top* 10 2021 dengan menggunakan kerangka kerja ELEMENT efektif dalam mengevaluasi keamanan aplikasi web.

Kata Kunci: ELEMENT *framework*, owasp, pentest, vapt.