ABSTRAK

Semenjak terjadinya pandemi, penggunaan teknologi informasi meningkat secara signifikan terutama pada penggunaan aplikasi berbasis web. Dalam penggunaan teknologi tersebut, tentunya tidak akan lepas dari berbagai macam risiko yang mengancam aset-aset berharga serta dapat menimbulkan kerugian. Untuk menghindari hal tersebut diperlukan tindakan evaluasi terhadap keamanan tidak terkecuali aplikasi web milik Institut XYZ. Terdapat berbagai macam cara yang dapat digunakan untuk melakukan evaluasi, salah satunya adalah dengan melakukan vulnerability assessment & penetration testing (VAPT). Dalam metode ini peneliti melakukan simulasi penyerangan sebagai peretas untuk mengidentifikasi dan menganalisis celah keamanan yang ada pada aplikasi web Institut XYZ. Pengujian yang dilakukan menggunakan panduan OWASP Web Security Testing Guide version 4.2 yang dibuat khusus untuk pengujian aplikasi web. Setelah kerentanan berhasil diidentifikasi, kemudian dilanjutkan dengan analisis risiko menggunakan NIST SP 800-30 Rev 1. Hasil akhir dari tugas akhir ini adalah laporan mengenai risiko yang berhasil dievaluasi serta rekomendasi langkah mitigasi dari risiko-risiko tersebut. Diharapkan hasilnya dapat membantu untuk mengamankan aplikasi web milik Institut XYZ.

Kata Kunci: kerentanan, risiko, web, VAPT, OWASP, NIST