ABSTRAK

Penelitian ini bertujuan untuk menganalisis tingkat keamanan pada *website* praktikum Fakultas Rekayasa Industri Telkom University dengan pendekatan *Vulnerability Assessment and Penetration Testing* (VAPT). Metode ini terdiri dari tahap *information gathering*, *vulnerability detection*, *penetration testing*, dan *remediation*. Pengujian dilakukan menggunakan beberapa tools keamanan seperti NMAP digunakan untuk information gathering. Sedangkan Nessus, OWASP ZAP, dan Nikto digunakan untuk vulnerability detection. Hasil pengujian menunjukkan empat kerentanan ditemukan pada nessus, sembilan ditemukan pada nikto dan tidak ada kerentanan ditemukan pada OWASP ZAP. Kerentanan paling berbahaya seperti *Cookie XSRF-TOKEN tanpa HttpOnly*, yang mana dapat manipulasi data, *Missing Strict-Transport-Security* dapat *man-in-the-middle (MITM)* dan *SSL stripping*. Rekomendasi mitigasi kemudian diterapkan untuk menutup celah-celah tersebut dengan cara menambahkan *HttpOnly* pada *cookie XSRF-TOKEN* dan Menambahkan *header Strict-Transport Security*, diikuti dengan pengujian ulang mengvaluasi efektifitas perbaikan. Setelah dilakukan pengujian ulang, masih ada terdapat empat kerentanan yangbelum ditutup dan delapan kerentanan yang sudah berhasil ditutup. Selanjutnya, kerentanan yang belum bisa ditutup akan direkomendasikan kepada *developer* untuk memperbaiki konfigurasi dari segi code lebih mendalam. Penelitian ini menghasilkan rekomendasi peningkatan sistem keamanan yang dapat digunakan sebagai acuan dalam pengelolaan keamanan *website* berbasis akademik dan institusional.

Kata kunci: Keamanan, *Web*, VAPT, *Vulnerability Assessment*, *Penetration Testing*, Mitigasi