ABSTRAK

Banyak perusahaan maupun organisasi mulai menggunakan *website* dalam menjalankan proses bisnis dan memberikan layanan. Tetapi dalam penggunaannya, sering ditemukan adanya kekurangan yang muncul dari *website* itu sendiri. *Vulnerability* merupakan kerentanan dari suatu sistem atau jaringan yang memungkinan adanya akses tanpa izin oleh orang yang tidak bertanggung jawab. *Vulnerability Assessment and Penetration Testing* (*VAPT*) merupakan metode yang digunakan dalam analisis dan pengujian dari kerentanan yang dimiliki oleh *website*. Universitas XYZ menggunakan *website* dalam menjalankan proses bisnis dan pengelolaan data, seperti layanan akademik. Penerapan dari aspek keamanan informasi sudah diterapkan didalam sistem. Tetapi terdapat kekurangan dalam penerapannya dengan adanya kerentanan yang muncul dari proses *vulnerability detection*. Perlu adanya evaluasi kembali dalam menjaga aspek keamanan informasi sudah diterapkan pada *website*. Dalam pengujian dari celah keamanan *website* layanan akademik Universitas XYZ, penulis memilih menggunakan metode *Vulnerability Assessment and Penetration Testing (VAPT)* dengan menggunakan beberapa *tools* seperti *NMAP, Nessus, OWASP ZAP*, dan *Burp suite* kemudian dibuatkan *reporting*. Dasar dari pemilihan metode ini yaitu dapat menyesuaikan dari kebutuhan pengujian sesuai dengan *scope* yang sudah ditentukan dan melakukan *remediation* sebagai upaya evaluasi keamanan dari pengujian sistem *website*. Hasil dari *vulnerability detection* ditemukan beberapa kerentanan dengan kategori risiko masing - masing. Kerentanan yang ditemukan dilakukan proses *remediation* dengan melakukan *update* dari versi terbaru hingga konfigurasi ulang dari *file website*. Kerentanan yang tidak berhasil diperbaiki akan menjadi rekomendasi mitigasi perbaikan sistem.

Kata Kunci : *Vulnerability*, Celah keamanan, *Vulnerability Assessment, Penetration Testing, VAPT, Website* layanan akademik Universitas XYZ