ABSTRAK

Guna mengurangi angka kecelakaan lalu lintas di jalan, maka diperlukan perilaku positif dari semua pengendara, yaitu kepatuhan terhadap peraturan berkendara dan rambu-rambu lalu lintas. Pada jaman teknologi saat ini maka telah dikembangkan sebuah *website* yang dirancang khusus untuk melakukan pengawasan menggunakan sarana elektronik sehingga para pelanggar akan mendapatkan bukti pelanggaran secara elektronik yang disebut e-tilang yang merupakan proses digitalisasi tilang. Salah satu *website* yang dirancang khusus untuk melakukan pengawasan pelanggaran secara elektronik dimaksud adalah *website* XYZ yang merupakan sasaran penelitian yakni akan dilakukan analisis kerentanan dan pengujian keamanan menggunakan standar NIST 800-115. Permasalahan yang diangkat dalam penelitian ini adalah terkait dengan keamanan suatu *website*, yang terfokus pada keamanan *website* XYZ, dengan tujuan mengetahui hasil penilaian kerentanan pada *website* XYZ, mendapatkan hasil dan menganalisis celah pada *website* XYZ, serta melakukan pengujian keamanan pada *website* XYZ dengan kerentanan tingkat tinggi (*high level*). Adapun manfaat penelitian bagi pemilik *website* dapat digunakan untuk mengetahui celah yang ada sebagai acuan melakukan peningkatan keamanan, bagi peneliti dapat meningkatkan pengetahuan tentang analisis kerentanan dan pengujian keamanan sebagai acuan melakukannya pada *website* lainya sehingga dapat meningkatkan keamanan *website*. Sedangkan manfaat bagi penelitian berikutnya dapat digunakan sebagai bahan awal. Pengujian yang dilakukan dalam penelitian ini menggunakan metode *black box* yang menggunakan standar NIST 800 – 115 dengan melalui 4 tahapan utama yaitu *planning*, *discovery, attack*, dan *reporting.* Analisis kerentanan dilakukan menggunakan beberapa *tools* seperti Nmap, OWASP ZAP, Burp Suite dan foxyproxy. Pada tahap *attacking* penelitian ini menggunakan jenis pengujian SQL *Injection*, setelah mendapatkan informasi kerentanan pada tahap *discovery*. Dari analisis kerentanan ini ditemukan bahwa pada *website* XYZ terdapat 7 celah kerentanan dengan tingkatan yang berbeda-beda. Pada pengujian kerentanan terhadap kerentanan tingkat tinggi (SQL *Injection)* digunakan 198 kombinasi kode injeksi. Dari keseluruhan hasil penelitian dapat disimpulkan bahwa berdasarkan hasil analisis kerentanan didapatkan 7 celah kerentanan pada *website* XYZ dengan 3 tingkatan, yaitu tinggi, sedang, dan rendah. Pada tahap pengujian kerentanan tingkat tinggi (SQL *Injection*) diperoleh 2 informasi yaitu informasi tentang isi *database* dan informasi tentang *direktori website* XYZ. Saran yang dapat diberikan untuk penelitian selanjutnya agar hasil penelitian ini dapat digunakan sebagai bahan awal dan agar menggunakan *tools* yang lebih beragam sehingga akan mendapatkan informasi yang lebih banyak tentang *website* yang diteliti.

Kata kunci: Sistem Informasi, Akademik, Telkom, Kerentanan, dan NIST 800-115.