ABSTRAK

Pada mesin server tempat sebuah situs web di hosting, umumnya terdapat data sensitif atau rahasia yang tidak dapat dibaca oleh masyarakat umum. Hal ini diperlukan untuk melindungi data agar komputer lain tidak dapat melihatnya. Solusinya adalah dengan menerapkan *Vulnerability Assessment* dengan metode *Vulnerability Scan* untuk menilai apakah keamanan sudah terjamin. Penelitian ini dilakukan pada rentang bulan juni-juli 2022 untuk menguji kerentanan *web server repository* IT Telkom Purwokerto. Faktor penelitian berdasarkan dari hasil pemindaian dari sistem yang digunakan, jenis informasi pribadi apa yang disimpan dalam sistem, seberapa sederhana serangan, dan seberapa besar kerusakan yang dapat terjadi jika kerentanan dieksploitasi secara efektif. Dalam mendeteksi kerentanan dalam penelitian ini digunakan metodologi penelitian kuantitatif dengan menggunakan *software* Kali Linux *Operation System,* Zenmap, dan Nessus *Scanner,* yang dimulai dari studi literatur, *footprinting*, *vulnerability scanning*, analisis dan rekomendasi, serta *reporting* (dokumentasi). Hasil yang diperoleh dari pengujian *Port Scanning* mengungkapkan beberapa port terbuka dan tertutup pada server *repository* IT Telkom Purwokerto, antara lain port 80 *HTTP/WEB*, port 445 *HTTPS,* dan port 9595 *PDS*. Pengujian di Zenmap didapatkan host target yang diperiksa mendukung protokol *POST, OPTIONS, GET*, dan *HEAD*. Target ditemukan sebagai proxy yang difilter HTTP. Tidak ada *cross-site scripting* yang terdeteksi. Pada host target, injeksi SQL ditemukan. Pengujian menggunakan Nessus *tools* diperoleh empat kategori kerentanan IP target untuk IT Telkom Purwokerto Repository berupa 15 kerentanan untuk info, 3 untuk *medium*, 1 untuk *high*, dan 1 untuk *critical*.

Kata kunci: Situs Web, Kali Linux, Keamanan Situs Web, *Vulnerability Assessment*