ABSTRAK

Perkembangan teknologi informasi telah mendorong peningkatan penggunaan aplikasi berbasis web di berbagai bidang, yang sekaligus menimbulkan tantangan terkait aspek keamanan. Penelitian ini bertujuan untuk mengidentifikasi dan mengevaluasi kerentanan keamanan yang terdapat pada *website* XYZ melalui pendekatan *Vulnerability Assessment*, menggunakan kombinasi alat pemindai *OWASP ZAP* dan *Nikto*. Pendekatan yang dipilih adalah *black-box testing*, yang hanya melibatkan pengujian terhadap *endpoint* publik tanpa memperoleh akses ke kode sumber internal. Hasil pengujian mengungkapkan sebanyak 29 kerentanan, dan setelah dilakukan validasi manual, 15 kerentanan dikonfirmasi sebagai valid. Berdasarkan penilaian dari *Common Vulnerability Scoring System* (*CVSS*) versi 3.1, ditemukan satu kerentanan kritis (ketiadaan Header HSTS) dengan skor 9,3, serta beberapa konfigurasi header keamanan dan pengaturan *cookie* yang tidak optimal. Dengan mengintegrasikan hasil pemindaian dari kedua alat tersebut, diperoleh nilai *precision* sebesar 0,93 dan *recall* sebesar 0,93, yang menunjukkan efektivitas pendekatan gabungan dalam mendeteksi kerentanan tanpa meningkatkan jumlah *false positives* secara signifikan. Penelitian ini juga menyajikan sejumlah rekomendasi mitigasi praktis yang disusun berdasarkan tingkat risiko, sebagai panduan bagi tim pengembang dan keamanan guna memperkuat postur keamanan *website* XYZ.

Kata Kunci: *vulnerability assessment, OWASP ZAP, Nikto, black-box testing, CVSS, website security*.