ABSTRAK

Penelitian ini bertujuan untuk mengevaluasi postur keamanan empat aplikasi web layanan publik milik Pemerintah Kabupaten Purbalingga, yaitu Siintan, Sangjuara, Lapormasbup, dan Sipetarung, guna mengidentifikasi celah keamanan teknis yang berpotensi mengganggu layanan digital. Metode yang digunakan adalah *vulnerability assessment* dengan kerangka penilaian risiko *Common Vulnerability Scoring System* (CVSS) versi 3.1. Pengujian dilakukan melalui pendekatan *Black Box Testing* menggunakan perangkat lunak pemindai otomatis *OWASP ZAP* dan validasi manual menggunakan *Burp Suite* untuk memverifikasi temuan pada lingkungan produksi. Hasil penelitian menunjukkan adanya kerentanan pada kategori risiko tinggi (*high*), menengah (*medium*), dan rendah (*low*). Temuan paling kritis meliputi penggunaan *framework Next.js* versi usang (11.0.0) yang rentan terhadap serangan *Denial of Service* (DoS), ketiadaan *header* keamanan standar (*Content Security Policy* dan *Anti-clickjacking*), konfigurasi CORS yang permisif, serta ketiadaan token *Anti-CSRF* pada formulir input. Analisis dampak menunjukkan bahwa celah ini berisiko melumpuhkan ketersediaan layanan serta membuka peluang serangan sisi klien yang dapat merugikan pengguna. Disimpulkan bahwa postur keamanan keempat aplikasi memerlukan perbaikan segera untuk memitigasi risiko eksploitasi. Rekomendasi prioritas mencakup pembaruan komponen utama ke versi stabil terbaru, implementasi *middleware* keamanan untuk injeksi *header*, serta pengaktifan proteksi CSRF pada formulir. Hasil penelitian ini diharapkan dapat menjamin keberlangsungan sistem pemerintahan berbasis elektronik yang aman dan terpercaya di Kabupaten Purbalingga.

Kata kunci: *Vulnerability Assessment*, Purbalingga, CVSS, Keamanan Web

ABSTRACT

This research aims to evaluate the security posture of four public service web applications owned by the Purbalingga Regency Government (Siintan, Sangjuara, Lapormasbup, and Sipetarung) to identify technical security vulnerabilities that could disrupt digital services. The study employs a vulnerability assessment method using the Common Vulnerability Scoring System (CVSS) version 3.1 risk assessment framework. Testing was conducted using a Black Box Testing approach with OWASP ZAP automated scanning software and manual validation via Burp Suite to verify findings in a production environment. Results revealed security vulnerabilities in High, Medium, and Low risk categories. The most critical findings include the use of an outdated Next.js framework (version 11.0.0), which is vulnerable to Denial of Service (DoS) attacks, the absence of standard security headers (Content Security Policy and Anti-clickjacking), permissive CORS configurations, and the absence of Anti-CSRF tokens on input forms. Impact analysis indicates that these vulnerabilities pose a risk to disrupting service availability and enabling client-side attacks that could harm users. It is concluded that the security posture of the four applications requires immediate remediation to mitigate the risks of exploitation. Priority recommendations include updating core components to the latest stable versions, implementing security middleware for header injection, and enabling CSRF protection on sensitive forms. These improvements are expected to ensure the sustainability of a secure and trusted electronic-based government system in Purbalingga Regency.

Keyword: Vulnerability Assessment, Purbalingga, CVSS, Web Security