

ABSTRAK

Digitalisasi tata kelola pemerintahan desa melalui *website* merupakan langkah strategis untuk mewujudkan pelayanan publik yang transparan. Namun, adopsi teknologi ini menghadapi ancaman keamanan siber serius akibat keterbatasan kompetensi SDM dan kurangnya audit berkala. Penelitian ini dilakukan pada *Website* Pemerintah Desa Prapagan (prapagan.desa.id) berbasis CMS WordPress yang tercatat mengalami tiga kali insiden penyusupan konten judi online ilegal. Guna mengidentifikasi akar masalah, penelitian ini menerapkan metode *Vulnerability Assessment* (VA) mengacu pada kerangka kerja NIST SP 800-115 melalui tahapan *Planning*, *Discovery*, dan *Vulnerability Analysis*. Pengujian dilakukan secara non-destruktif menggunakan alat pemindai otomatis OWASP Zed Attack Proxy (ZAP), lalu tingkat risiko dianalisis menggunakan metode penilaian kuantitatif *Common Vulnerability Scoring System* (CVSS) v3.1. Hasil pengujian berhasil mengonfirmasi dua belas kategori celah keamanan pada *website* target. Kombinasi kerentanan dari pustaka JavaScript usang (*Vulnerable JS Library*) dan miskonfigurasi enkapsulasi *Header* HTTP diidentifikasi sebagai faktor paling kritis yang memicu terjadinya infeksi iklan judi online. Sebagai langkah remediasi, penelitian ini menghasilkan *blueprint* mitigasi berupa dokumen pedoman teknis dan draf skrip berkas *.htaccess* untuk mengoptimalkan instruksi pengamanan peladen (*server hardening*) tanpa mengganggu stabilitas pelayanan publik desa. Kesimpulannya, dokumen matriks pelaporan ini diserahkan kepada instansi desa sebagai panduan operasional demi menjamin aspek keamanan data masyarakat.

Kata kunci: *Vulnerability Assessment*, OWASP ZAP, WordPress, *.htaccess*, Judi Online.

ABSTRACT

The digitalization of village governance through websites is a strategic step toward achieving transparent public services. However, the adoption of this technology faces serious cyber security threats due to limited human resource competence and the lack of regular audits. This research was conducted on the Official Website of Prapagan Village (prapagan.desa.id) based on the WordPress CMS, which was recorded to have suffered three incidents of illegal online gambling content injection. To identify the root cause, this study applies the Vulnerability Assessment (VA) method based on the NIST SP 800-115 framework through the Planning, Discovery, and Vulnerability Analysis phases. Testing was conducted non-destructively using the automated scanning tool OWASP Zed Attack Proxy (ZAP), and risk levels were analyzed using the Common Vulnerability Scoring System (CVSS) v3.1 quantitative assessment method. The testing results successfully confirmed twelve categories of security vulnerabilities on the target website. The combination of vulnerabilities from outdated JavaScript libraries (Vulnerable JS Library) and HTTP Header encapsulation misconfigurations was identified as the most critical factor triggering the online gambling ad infections. As a remediation step, this research produces a mitigation blueprint consisting of technical guideline documents and a draft .htaccess file script to optimize server hardening instructions without disrupting the stability of the village's public services. In conclusion, this reporting matrix document was submitted to the village institution as an operational guide to guarantee the security aspect of community data.

Keywords: Vulnerability Assessment, OWASP ZAP, WordPress, .htaccess, Online Gambling.