ABSTRAK

Bayu Saputra. 2025. Analisis Kerentanan Dengan Metode NIST Dalam Penetration Testing Guna Meningkatkan Keamanan Website Disparbudpora Kabupaten Pacitan. Program Studi Sistem Informasi, FT, Universitas PGRI Madiun. Pembimbing (I) Andria, S.Kom., M.Kom. (II) Hani Atun Mumtahana, S.Kom., M.Kom.

Kerusakan pada website Disparbudpora Kabupaten Pacitan yang menyebabkan hilangnya seluruh konten dan perlunya pembangunan ulang sistem menunjukkan lemahnya perlindungan keamanannya. Hal ini menimbulkan urgensi untuk mengevaluasi kerentanan sistem guna mencegah kejadian serupa di masa depan. Penelitian ini bertujuan untuk mengetahui tingkat kerentanan website, merumuskan rekomendasi keamanan yang tepat, serta mengevaluasi implementasinya. Pengujian dilakukan menggunakan metode *penetration testing* berbasis NIST SP 800-115 dengan pendekatan *white-box* hingga *level dashboard admin WordPress*. Dari 38 temuan pada tahap *discovery*, terdapat 10 kerentanan berisiko tinggi (26,32%), seperti aktivasi *xmlrpc.php*, potensi *Blind SQL Injection*, keterbukaan data melalui REST API, serta konfigurasi DNS yang rentan terhadap *Subdomain Takeover*. Sisanya berupa temuan informasional yang tetap relevan. Nilai rata-rata CVSS sebesar 6,4 menunjukkan tingkat risiko sedang. Rekomendasi mitigasi meliputi penonaktifan fungsi rawan, pembatasan akses REST API, penggunaan plugin keamanan, penghapusan komponen tidak penting, dan penguatan header HTTP. Sebagian besar mitigasi berhasil diterapkan melalui *dashboard admin*, sedangkan sisanya memerlukan dukungan teknis dari pengelola. Hasil penelitian menunjukkan bahwa pendekatan pengujian keamanan yang sistematis mampu memberikan kontribusi nyata terhadap peningkatan perlindungan website.

Kata Kunci: Keamanan Website; *Penetration Testing*; NIST SP 800-115; *CVSS*; *WordPress;*

ABSTRACT

Bayu Saputra. 2025. *Vulnerability Analysis Using the NIST Method in Penetration Testing to Improve the Security of the Pacitan Regency Disparbudpora Website*, Universitas PGRI Madiun. *Advisor* (I) Andria, S.Kom., M.Kom. (II) Hani Atun Mumtahana, S.Kom., M.Kom.

The damage to the Pacitan Regency Tourism, Culture, and Youth Office (Disparbudpora) website, which resulted in the loss of all content and the need for a system rebuild, demonstrates the weakness of its security protections. This raises the urgency of evaluating system vulnerabilities to prevent similar incidents in the future. This study aims to determine the level of website vulnerability, formulate appropriate security recommendations, and evaluate their implementation. Testing was conducted using a NIST SP 800-115-based penetration testing method with a white-box approach down to the WordPress admin dashboard level. Of the 38 findings in the discovery stage, there were 10 high-risk vulnerabilities (26.32%), such as xmlrpc.php activation, potential Blind SQL Injection, data disclosure via the REST API, and DNS configuration vulnerable to Subdomain Takeover. The remaining findings were informational but remain relevant. The average CVSS score of 6.4 indicates a moderate level of risk. Mitigation recommendations include disabling vulnerable functions, restricting REST API access, using security plugins, removing non-critical components, and strengthening HTTP headers. Most mitigations were successfully implemented through the admin dashboard, while the remainder required technical support from the administrator. The research results show that a systematic security testing approach can make a real contribution to improving website protection.

Keywords: Cybersecurity; Penetration Testing; NIST SP 800-115; CVSS; WordPress;