ABSTRAK

Website pemerintah memiliki peran strategis dalam menyediakan akses informasi dan interaksi digital kepada publik, termasuk yang dikelola oleh Dinas Komunikasi dan Informatika (Dinkominfo) Kabupaten Banyumas. Namun, paparan terhadap internet meningkatkan kerentanannya terhadap berbagai serangan siber. Penelitian ini bertujuan untuk mengidentifikasi dan menganalisis kerentanan keamanan pada website Dinkominfo Banyumas menggunakan dua pendekatan penetration testing, yaitu Penetration Testing Execution Standard (PTES) dan OWASP Top 10. Pengujian dilakukan melalui pemetaan port, identifikasi direktori, pengujian konfigurasi keamanan, serta eksploitasi kerentanan menggunakan tools seperti Nmap, ZAP, SQLMap, dan Burp Suite. Hasil penelitian menunjukkan bahwa OWASP lebih efektif dalam mengidentifikasi kerentanan pada lapisan aplikasi seperti injection, broken access control, dan misconfiguration, serta lebih efisien dari segi waktu karena mampu menghasilkan temuan dalam durasi yang lebih singkat. Sebaliknya, PTES menawarkan pendekatan yang lebih sistematis dan menyeluruh dari tahap perencanaan hingga pelaporan, namun memerlukan waktu pelaksanaan yang lebih panjang. Temuan ini menunjukkan bahwa OWASP lebih cocok diterapkan pada pengujian keamanan aplikasi web instansi pemerintah daerah, sedangkan PTES relevan untuk pengujian berskala besar dengan kebutuhan dokumentasi menyeluruh. Hasil penelitian ini diharapkan menjadi acuan strategis dalam memperkuat keamanan dan perlindungan data pada layanan digital pemerintahan.

Kata kunci: Penetration Testing, OWASP Top 10, PTES, Keamanan Website, Efisiensi, Pemerintahan Daerah.