ABSTRACT

Government websites play a strategic role in providing public access to information and facilitating digital interaction, including those operated by the Department of Communication and Informatics (Dinkominfo) of Banyumas Regency. However, exposure to the internet increases their vulnerability to various cyberattacks. This study aims to identify and analyze the security vulnerabilities of the Dinkominfo Banyumas website using two penetration testing approaches: the Penetration Testing Execution Standard (PTES) and the OWASP Top 10. The testing process involved port mapping, directory enumeration, security configuration assessment, and exploitation using tools such as Nmap, ZAP, SQLMap, and Burp Suite. The results show that OWASP is more effective in identifying application-layer vulnerabilities such as injection, broken access control, and security misconfiguration, and it is also more time-efficient as it produces findings faster. In contrast, PTES offers a more systematic and comprehensive approach from planning to reporting, but requires a longer time to complete. These findings suggest that OWASP is more suitable for web security assessments in regional government institutions, while PTES is better suited for large-scale, enterprise-level testing. The outcomes of this research are expected to serve as a strategic reference for enhancing the security and data protection of government digital services.

***Keywords**: Penetration Testing, OWASP Top 10, PTES, Website Security, Efficiency, Local Government.*