

ABSTRACT

The increasing use of the internet from year to year along with the rapid development of information and communication technology, including websites, makes websites one of the important media used by the government to disseminate and obtain information. However, special attention needs to be given to security in the development of government websites, given the many cases of leakage of public data sourced from government-owned servers. This can reduce public trust in the government.

The Sudagaran Village website managed by the Ministry of Education and Culture is the object of this research to identify and evaluate its security level. The research was conducted using the penetration testing method and refers to the OWASP Top 10, with the steps of identifying vulnerabilities and simulating attacks on the vulnerabilities found.

The implementation results show the existence of several vulnerabilities, such as SQL Injection, Cross-Site Scripting (XSS), and security configuration weaknesses. Mitigation recommendations include implementing security headers, input validation, using HTTPS, and updating obsolete components. The implementation of these mitigation measures is expected to improve website security and restore public trust in digital-based services.

Keywords: owasp, penetration testing, website, government, Banyumas