ABSTRACT

VULNERABILITY ANALYSIS AND WEBSITE SECURITY STRENGTHENING USING THE OPEN WEB APPLICATION SECURITY PROJECT (OWASP) METHODOLOGY PADA WEBSITE SISTEM INFORMASI MANAJEMEN XYZ

By:
HARIZ HUSAIN
21102064

Threats to the security of government-owned websites continue to increase, especially as the public becomes increasingly reliant on digital services. The website of the XYZ Regency Government is among those potentially vulnerable to attacks, such as the injection of illegal content and leakage of sensitive data. This issue indicates that there are still security gaps that need to be promptly identified and addressed. Government websites are often targeted by cyberattacks because they store critical information and are widely used by the public. However, their security management is not yet fully optimized, which can disrupt public services. The solution implemented involves analyzing the website's security using the OWASP approach, a methodology used to identify the ten most common types of vulnerabilities. The process includes data gathering and vulnerability Information Gathering to determine the extent to which security gaps can be exploited. Additionally, this study provides technical recommendations to close the identified vulnerabilities. The testing results revealed serious vulnerabilities, with seven security issues ranging from medium to high risk, including weaknesses in Broken Access Control, Cryptographic Failures, Injection, Security Misconfiguration, Vulnerable and Outdated Components, Software and Data Integrity Failures, and Identification and Authentication Failures. Mitigation recommendations were provided for each vulnerability, such as restricting directory access, implementing HTTPS, input validation, updating outdated components, and using two-factor authentication (2FA). The evaluation showed that applying these corrective measures significantly improved the overall security. This study serves as a reference for strengthening cybersecurity for government website administrators.

Keywords: website security, OWASP, cyber vulnerability, mitigation, XYZ regency.