WEB-BASED SOFTWARE CODE SECURITY STRATEGY

Name : Dian Utami
Student ID Number : 6304221456
Advisors : M. Asep Subandri, S.Kom, M.Kom

ABSTRACT

Web-based software is vulnerable to various cyberattacks due to security flaws in programming code, such as Cross-Site Scripting (XSS), SQL Injection, Path Traversal, Cross-Site Request Forgery (CSRF), and File Upload Vulnerabilities. Developers often prioritize user interface features over security aspects. This study examines code security strategies for web-based software, using the Akalink academic information system as a case study, with the aim of reducing vulnerabilities prior to deployment. The research employs a qualitative method with a descriptive approach, supported by the Software Testing Life Cycle (STLC) framework to ensure a systematic testing process. The implemented STLC stages include requirement analysis, test planning, test case development, environment setup, test execution, and test cycle closure. Testing was conducted using OWASP ZAP to identify vulnerabilities before and after the implementation of security strategies. The results indicate that the implementation of security measures, including input validation, CSRF tokens, and secure file upload mechanisms, significantly reduced identified vulnerabilities. In conclusion, the applied security strategies proved effective in mitigating common cyberattacks on web applications without disrupting the system's core functionality, while the STLC approach provided a systematic and comprehensive framework for software security testing.

Keywords: Web Security, Software Testing Life Cycle (STLC), Code Security Strategy