Abstract

SIABDes Maxy is an application designed to assist in the administrative and financial management of Badan Usaha Milik Desa (BUMDes). In the development of versions 1 to 3, application security was not a top priority, so security testing was not implemented comprehensively. However, applications that handle administrative and financial data are vulnerable to security threats such as unauthorized access, data theft, and cyberattacks, which can harm both users and BUMDes administrators. Therefore, in the third version of SIABDes Maxy, security testing was conducted using penetration testing and fuzz testing methods to identify potential system vulnerabilities. The testing focused on critical modules such as the login feature and API endpoints using the OWASP ZAP tool. The test results showed that although some input validation mechanisms were functioning properly, the application still had significant weaknesses, such as the absence of protection against brute force attacks and replay attacks. This indicates that the application does not yet fully meet the security standards required by the ISO/IEC 25010 principles. These findings are expected to serve as an important reference for future developers to enhance the application's security aspects, thereby providing better protection for BUMDes data and operations.

Keywords: security testing, penetration testing, fuzz testing, SIABDes Maxy, application security.