ABSTRACT

In this rapidly developing era, an online-based public service system is a solution that can facilitate access to services for residents of Limapoccoe Village. However, one of the important stages in developing a system-based public service system is testing. Automated testing is preferred because it is more efficient and reduces the potential for errors. Security in public service systems is very important to protect sensitive data such as NIK and Family Cards from threats and leaks that can harm users and organizations. This study aims to identify security vulnerabilities in the system by automated testing using OWASP ZAP and the Behavior Driven Development (BDD) approach. OWASP ZAP was chosen because it is open source and capable of detecting various vulnerabilities. The testing process includes mapping test objectives based on the OWASP ASVS standard, threat modeling using STRIDE, creating user stories and test cases with the Giving-When-Then format, implementation and test results. The results showed several vulnerabilities, including one high-level threat in SQL injection, several medium-level threats, low-level threats, and OWASP ZAP also detected information warnings. Negative testing also revealed input validation weaknesses in the letter submission feature by staf. This research proves the importance of implementing security testing from the beginning of system development and provides recommendations for security improvements.

***Keywords**: OWASP ZAP, Security Testing, Behavior Driven Development (BDD), Public Service System, Automated Testing*