

INTISARI

REST API telah menjadi fondasi utama dalam arsitektur sistem modern, namun keamanannya sering diabaikan sehingga menimbulkan risiko signifikan seperti kebocoran data dan pelanggaran otorisasi. Berdasarkan laporan Salt Security (2025), 99% organisasi mengalami insiden keamanan API dalam satu tahun terakhir. Penelitian ini mengimplementasikan standar OWASP API Security Top 10:2023 dalam pengembangan REST API menggunakan framework FastAPI. Sistem dibangun dengan fitur registrasi, login, manajemen pengguna, dan pencatatan data pribadi, dilengkapi autentikasi JWT dan kontrol akses berbasis peran. Pengujian dilakukan terhadap seluruh endpoint menggunakan pendekatan gray-box testing dengan Postman dan OWASP ZAP. Hasil pengujian menunjukkan bahwa sistem berhasil mencegah seluruh skenario eksploitasi dari 10 kategori OWASP, termasuk Broken Object Level Authorization (BOLA), Security Misconfiguration, dan Broken Authentication. Penelitian ini menyimpulkan bahwa penerapan standar OWASP secara sistematis mampu meningkatkan ketahanan REST API terhadap ancaman siber secara signifikan.

Kata kunci: REST API, FastAPI, OWASP API Security, Postman, Gray-box Testing

ABSTRACT

REST APIs have become a foundational component in modern system architecture; however, their security is often neglected, leading to significant risks such as data breaches and authorization violations. According to Salt Security (2025), 99% of organizations experienced API security incidents in the past year. This study implements the OWASP API Security Top 10:2023 standard in the development of a REST API using the FastAPI framework. The system includes features such as user registration, login, user management, and personal note recording, secured with JSON Web Token (JWT) authentication and role-based access control. Security testing was conducted on all endpoints using a gray-box testing approach with tools such as Postman and OWASP ZAP. The results show that the system successfully prevented all exploitation scenarios based on the ten OWASP categories, including Broken Object Level Authorization (BOLA), Security Misconfiguration, and Broken Authentication. This study concludes that a systematic application of the OWASP standards significantly enhances REST API resilience against modern cyber threats.

Keywords: REST API, FastAPI, OWASP API Security, Postman, Gray-box Testing.