ABSTRAK

NURUL ALIYAH. Implementasi Autentikasi Adaptif menggunakan JSON Web *Token* Dinamis pada aplikasi Node.js dan Express (Dibimbing oleh Ida dan Darniati).

Penelitian ini mengimplementasikan autentikasi adaptif berbasis JSON Web Token (JWT) dinamis pada aplikasi web menggunakan Node.js dan Express. Berbeda dengan JWT konvensional yang menerapkan secret key global, sistem ini menggunakan secret key unik per pengguna yang digenerate otomatis dan disimpan di database MySQL/SQLite, dilengkapi middleware autentikasi adaptif untuk verifikasi konteks akses (IP address, user-agent) dengan algoritma HMAC-SHA256.

Pengujian dilakukan melalui simulasi pembuatan data dummy via form registrasi frontend, proses login untuk penerbitan JWT, serta skenario serangan seperti token sharing, replay attack, modifikasi payload, dan akses lintas browser/IP.

Hasil pengujian menunjukkan sistem secara konsisten mendeteksi dan menolak akses tidak sah dengan HTTP 401/403, membatasi dampak kebocoran secret key hanya pada akun terkait. Kesimpulannya, Implementasi JWT dinamis dengan autentikasi adaptif terbukti meningkatkan keamanan autentikasi secara signifikan dibandingkan skema konvensional melalui pengujian fungsionalitas dan simulasi serangan.

Kata Kunci: JWT dinamis, autentikasi adaptif, secret key unik, Node.js, HMAC-SHA256

ABSTRACT

NURUL ALIYAH. Implementation of Adaptive Authentication using Dynamic JSON Web Token on Node.js and Express Applications (Supervised by Ida and Darniati).

This research implements adaptive authentication based on dynamic JSON Web Token (JWT) on web applications using Node.js and Express. Unlike conventional JWT which employs a global secret key, this system utilizes unique secret key per user automatically generated and stored in MySQL/SQLite database, complemented by adaptive authentication middleware for access context verification (IP address, user-agent) using HMAC-SHA256 algorithm.

Testing was conducted through dummy data creation simulation via frontend registration form, login process for JWT issuance, and attack scenarios including token sharing, replay attack, payload modification, and cross-browser/IP access.

Test results demonstrate the system consistently detects and rejects unauthorized access with HTTP 401/403 responses, limiting secret key leakage impact to affected accounts only. The implementation of dynamic JWT with adaptive authentication significantly enhances authentication security compared to conventional schemes through functionality testing and attack simulation.

Keywords: Dynamic JWT, adaptive authentication, unique secret key, Node.js, HMAC-SHA256