

ABSTRAK

Penelitian ini bertujuan mengimplementasikan *password hashing* Argon2id pada sistem autentikasi aplikasi web serta membandingkan waktu *hashing* dan waktu verifikasi *login* antarskenario kombinasi parameter *memory cost*, *time cost*, dan *parallelism* untuk menentukan konfigurasi yang paling sesuai dalam lingkungan pengujian. Penelitian ini menggunakan metode eksperimen dengan desain eksperimen berorientasi teknologi (*technology-oriented experiment*) dan pendekatan *performance benchmarking*. Modul autentikasi berbasis Laravel digunakan untuk menguji delapan skenario parameter Argon2id. Pengujian mikro dilakukan melalui PHP CLI untuk mengukur waktu *hashing*, sedangkan pengujian makro dilakukan melalui alur autentikasi Laravel menggunakan `Auth::attempt()` untuk mengukur waktu verifikasi *login*. Setiap skenario dijalankan dengan 10 kali *warm-up* dan 50 iterasi pengukuran utama. Analisis data mencakup statistik deskriptif, uji Brown–Forsythe, Welch ANOVA, serta Welch *t-test* terhadap 28 pasangan skenario pada setiap lapisan dengan koreksi Holm. Hasil pengujian menunjukkan bahwa rata-rata waktu *hashing* berada pada rentang 18,37–493,02 ms, sedangkan rata-rata waktu verifikasi *login* berada pada rentang 19,44–496,75 ms. Welch ANOVA menunjukkan perbedaan rata-rata waktu yang signifikan antarskenario pada kedua lapisan, dan seluruh pasangan tetap signifikan setelah koreksi Holm. Konfigurasi B_OWASP_Min dengan *memory cost* 19.456 KiB, *time cost* 2, dan *parallelism* 1 dipilih sebagai konfigurasi paling sesuai karena memenuhi konfigurasi minimum OWASP serta menghasilkan rata-rata waktu *hashing* 37,95 ms dan waktu verifikasi *login* 37,71 ms, yang merupakan nilai terendah di antara skenario berbasis rujukan. Hasil penelitian ini berlaku pada lingkungan pengujian yang digunakan dan tidak diposisikan sebagai rekomendasi universal.

Kata kunci: Argon2id, autentikasi, *password hashing*, optimasi parameter, Laravel.

ABSTRACT

This study aimed to implement Argon2id password hashing in a web application authentication system and compare hashing time and login verification time across combinations of the memory cost, time cost, and parallelism parameters to determine the most suitable configuration within the testing environment. An experimental method with a technology-oriented design and performance benchmarking approach was applied to a Laravel-based authentication module using eight Argon2id scenarios. Micro testing through PHP CLI measured hashing time, while macro testing through the Laravel authentication flow using `Auth::attempt()` measured login verification time. Each scenario included 10 warm-up runs and 50 measured iterations. Data analysis used descriptive statistics, the Brown–Forsythe test, Welch ANOVA, and Welch t-tests for 28 pairwise comparisons at each testing layer with Holm correction. The average hashing time ranged from 18.37 to 493.02 ms, while the average login verification time ranged from 19.44 to 496.75 ms. Welch ANOVA showed significant differences in average time among scenarios at both testing layers, and all pairwise comparisons remained significant after Holm correction. The B_OWASP_Min configuration, with a memory cost of 19,456 KiB, a time cost of 2, and a parallelism value of 1, was selected as the most suitable configuration because it met the OWASP minimum configuration and produced average hashing and login verification times of 37.95 ms and 37.71 ms, respectively, the lowest among the reference-based scenarios. These findings apply only to the testing environment and are not presented as a universal recommendation.

Keywords: Argon2id, authentication, password hashing, parameter optimization, Laravel.