

ABSTRAK

Keamanan penyimpanan kata sandi pada aplikasi web memerlukan algoritma *password hashing* yang mampu meningkatkan biaya penebakan tanpa menimbulkan latensi dan konsumsi sumber daya yang berlebihan. Penelitian ini bertujuan membandingkan karakteristik bcrypt dan Argon2id pada aplikasi web uji berbasis PHP berdasarkan latensi verifikasi password dan konsumsi memori, serta menganalisis simulasi offline *password cracking* pada bcrypt dan karakteristik ketahanan Argon2id berdasarkan sifat *memory-hard*, hasil *benchmark*, dan literatur pendukung. Penelitian menggunakan metode eksperimen pada PHP 8.1.25 dan SQLite dengan analisis deskriptif komparatif. Algoritma bcrypt diuji pada *cost* 10 sampai 14, sedangkan Argon2id diuji melalui 48 kombinasi parameter. Lima konfigurasi representatif Argon2id disajikan pada tabel utama. Setiap konfigurasi dijalankan 30 kali untuk memperoleh median waktu *hashing*, median waktu verifikasi, dan *peak* RSS proses PHP. Simulasi *time-boxed dictionary attack* dilakukan terhadap bcrypt *cost* 10 menggunakan Hashcat dengan dua skenario *wordlist*. Hasil menunjukkan bahwa median verifikasi bcrypt meningkat dari 60,48 ms menjadi 918,65 ms dengan *peak* RSS 18,88 sampai 18,96 MiB. Pada lima konfigurasi representatif, median verifikasi Argon2id berada pada 28,69 sampai 419,12 ms dengan *peak* RSS 38,02 sampai 147,53 MiB. Skenario top10k_n10 menemukan 10/10 *hash*, sedangkan rank100k_n10_vs_top10k tidak menemukan *hash* dalam 600 detik karena kandidat target berada di luar *wordlist*. Di antara lima konfigurasi representatif, Argon2id m=19456, t=2, p=1 mencatat median verifikasi dan *peak* RSS terendah, yaitu 28,69 ms dan 38,02 MiB. Argon2id m=47104, t=1, p=1 mencatat 39,88 ms dan 65,00 MiB pada kedua metrik tersebut. Hasil ini tidak merupakan perbandingan *cracking* langsung yang setara antara bcrypt dan Argon2id.

Kata kunci: Argon2id, bcrypt, konsumsi memori, latensi verifikasi *password*, *offline password cracking*.

ABSTRACT

Password storage security in web applications requires password-hashing algorithms that increase guessing costs without imposing excessive latency or resource use. This study compares bcrypt and Argon2id in a PHP-based web test application using password-verification latency and memory consumption, and examines an offline password-cracking simulation against bcrypt alongside Argon2id resistance characteristics derived from its memory-hard design, benchmark results, and supporting literature. Experiments used PHP 8.1.25 and SQLite with descriptive comparative analysis. Bcrypt was tested at costs 10–14, while Argon2id was evaluated through 48 parameter combinations. Five representative Argon2id configurations are presented in the main table. Each configuration was executed 30 times to obtain median hashing time, median verification time, and peak RSS of the PHP process. A time-boxed dictionary attack tested bcrypt cost 10 in Hashcat under two wordlist scenarios. Bcrypt median verification time increased from 60.48 to 918.65 ms while peak RSS remained 18.88–18.96 MiB. Among the five representative configurations, Argon2id median verification time ranged from 28.69 to 419.12 ms and peak RSS from 38.02 to 147.53 MiB. The top10k_n10 scenario recovered 10/10 hashes, whereas rank100k_n10_vs_top10k recovered none within 600 seconds because its targets were outside the wordlist. Among five representative configurations, Argon2id $m=19456$, $t=2$, $p=1$ recorded the lowest median verification time and peak RSS, at 28.69 ms and 38.02 MiB. Argon2id $m=47104$, $t=1$, $p=1$ recorded 39.88 ms and 65.00 MiB for the two metrics, respectively. The results do not represent a direct, equivalent cracking comparison between bcrypt and Argon2id.

Keywords: Argon2id, bcrypt, password verification latency, memory consumption, offline password cracking.