

LAPORAN PENTEST FINAL

Aplikasi RTIK | 28 April 2026

Ringkasan Eksekutif

Aplikasi berada dalam kondisi jauh lebih aman setelah hardening berlapis.
Catatan: .env production sudah disesuaikan oleh tim.

Kontrol Keamanan yang Terverifikasi

- 1. Proteksi brute-force aktif di login admin dan anggota (throttle:login).
- 2. RateLimiter login aktif: 5 percobaan/menit per username + IP.
- 3. Konfigurasi database tidak menyimpan password default plaintext.
- 4. Logging sensitif di admin upload flow sudah dibersihkan.
- 5. Script setup berisiko sudah dihapus dari root aplikasi.

Temuan Residual

Severity	Temuan	Lokasi
MEDIUM	Log debug di LocationService masih bisa dipangkas	app/Services/LocationService.php

TINDAK LANJUT PRODUCTION

Checklist final pasca hardening

1. Pertahankan APP_DEBUG=false di production.
2. Jangan reintroduce file setup/dev script ke root saat deploy.
3. Jalankan rutin: php artisan config:clear, cache:clear, route:clear.
4. Pastikan log retention aktif dan akses log dibatasi admin ops.
5. Lakukan security review ringan setiap ada update manual.
6. Simpan backup .env secara aman di secret vault/internal manager.

Kesimpulan Akhir

Tidak ditemukan temuan kritis pada retest final ini.

Risiko saat ini berada pada level rendah-menengah (operasional logging).