LAPORAN PENTEST ULANG

Aplikasi RTIK | 28 April 2026

Kesimpulan Umum:

Keamanan aplikasi sudah lebih baik dibanding audit sebelumnya.
Kontrol login dan secret utama sudah dalam kondisi aman.

Kontrol yang Berhasil Diverifikasi

1. Route login admin & anggota sudah memakai throttle:login.
2. RateLimiter login sudah aktif (5 percobaan/menit per username+IP).
3. config/database.php tidak lagi menyimpan default password plaintext.
4. Logging detail sensitif pada admin upload flow sudah dibersihkan.
5. Seeder password hardcoded sudah tidak ditemukan (folder seeder dibersihkan).

Temuan Tersisa

Severity	Temuan	Lokasi
MEDIUM	Log info di LocationService masih cukup detail	app/Services/LocationService.php
LOW	1 file laporan pentest lama masih di root (terkunci/open)	Laporan_Pentest_Ulang_RTIK_Awam_2026-04-28.pdf

REKOMENDASI FINAL

Checklist implementasi production

1. Pertahankan throttle login dan RateLimiter (jangan dihapus saat update manual).
2. Sederhanakan Log::info di LocationService untuk mode production.
3. Pastikan APP_DEBUG=false di .env production.
4. Jalankan berkala: php artisan config:clear, cache:clear, route:clear.
5. Pastikan tidak ada script setup/test yang kembali ke root aplikasi.
6. Tutup file PDF yang masih terbuka lalu pindahkan ke folder arsip.

Status Akhir Audit Ulang

Mayor temuan prioritas tinggi sudah ditutup. Residual risk saat ini rendah-menengah.