LAPORAN PENETRATION TEST

Aplikasi RTIK (Laravel) | 28 April 2026

Target: C:\laragon\www\rtik
Metode: Source Code Security Review (White-box)
Penguji: Tim Internal
Status: Assessment awal + hardening prioritas

Ringkasan Eksekutif

Ditemukan 1 temuan kritis, 1 tinggi, 1 menengah (sudah mitigasi), dan 1 rendah/menengah.
Prioritas: manajemen secret, hardening deployment, serta minimisasi data sensitif pada log.

Ringkasan Temuan

ID	Severity	Temuan	Status
F-01		Hardcoded DB credentials pada script setup	Open
F-02		Script operasional berisiko terekspos web root	Open
F-03		Rate limit login belum ada (sudah diterapkan)	Mitigated
F-04		Verbose logging detail upload/profile	Open

KEAMANAN YANG SUDAH DITERAPKAN

Status kontrol saat assessment

1. Multi-guard authentication untuk admin dan anggota.
2. Middleware akses berbasis role: admin, pembina, wilayah, anggota.
3. Session hardening: regenerate saat login; invalidate + regenerateToken saat logout.
4. Validasi input request pada endpoint utama (login/create/update).
5. Password hashing via Hash::make / Hash::check.
6. Validasi upload file (tipe, mime, ukuran).
7. Rate limiting login (5 request/menit per username+IP).
8. Query builder/Eloquent parameter binding untuk minim risiko SQL injection.
9. CSRF protection bawaan Laravel untuk state-changing requests.
10. Beberapa handler file memakai basename() untuk menekan risiko path traversal sederhana.

Rencana Tindak Lanjut (7 Hari)

1. Rotate seluruh credential DB yang pernah hardcoded.
2. Pindahkan/hapus script setup dari area publik.
3. Kurangi logging sensitif pada environment production.
4. Lakukan retest untuk verifikasi closure semua temuan prioritas.