LAPORAN PENTEST TERBARU

Aplikasi RTIK | 28 April 2026

Ringkasan:

Keamanan membaik. Proteksi login aktif kembali dan secret default di config sudah dibersihkan.

Status Kontrol yang Sudah Aktif

1. Throttle login aktif untuk admin dan anggota.
2. RateLimiter login (5 percobaan/menit per username+IP).
3. Default DB_PASSWORD di config sudah dikosongkan.
4. Script setup online database yang berisiko sudah dihapus.

Temuan yang Masih Perlu Diperbaiki

Severity	Temuan	Lokasi
HIGH	Password hardcoded di seeder	database/seeders/*.php
MEDIUM	Log upload admin terlalu detail	app/Http/Controllers/AnggotaController.php
LOW	1 file laporan masih di root (terkunci)	Laporan_Pentest_Ulang_RTIK_Awam_2026-04-28.

REKOMENDASI TINDAK LANJUT

Checklist untuk production

1. Rotate password database dan akun admin lama sekarang juga.
2. Bersihkan hardcoded password di semua file seeder.
3. Pastikan seeder akun default tidak dijalankan di production.
4. Kurangi Log::info detail file/path pada controller upload admin.
5. Pastikan APP_DEBUG=false di production.
6. Jalankan: php artisan config:clear, cache:clear, route:clear.
7. Uji login: pastikan rate limit benar-benar aktif saat salah password berulang.
8. Pindahkan sisa file laporan di root setelah file tidak sedang dibuka.

Kesimpulan:

Aplikasi sudah bergerak ke arah lebih aman, namun masih perlu cleanup seeder dan logging.