

## LAPORAN PENTEST

Target: Aplikasi Laravel RTIK (C:\laragon\www\rtik)

Tanggal Uji: 28 April 2026

Metode: Source Code Security Review (white-box, non-intrusive)

### Ringkasan Eksekutif

Ditemukan 1 temuan kritis, 1 tinggi, 1 menengah (sudah mitigasi), dan 1 rendah/menengah. Fokus perbaikan utama: secret management, hardening deployment, dan minimisasi data sensitif pada log.

### Temuan Utama

- 1) Critical - Hardcoded DB credentials pada setup\_online\_database.php  
Dampak: Risiko akses database tidak sah jika file/repo terekspos.  
Rekomendasi: Rotate kredensial, hapus hardcoded secret, pakai .env.
- 2) High - Script operasional berisiko terekspos web root  
File: create\_symlink.php, cpanel\_create\_symlink.php, setup\_online\_database.php  
Rekomendasi: pindah ke non-public path, batasi akses, hapus setelah dipakai.
- 3) Medium - Proteksi brute-force login belum ada (sudah diperbaiki)  
Mitigasi diterapkan: throttle:login + RateLimiter 5 req/menit (username+IP).
- 4) Low/Medium - Verbose logging upload profile  
Rekomendasi: kurangi log debug sensitif di production.

### Status Patch Saat Uji

- Sudah diterapkan hardening brute-force login.
- Validasi sintaks file patch: lulus (php -l).

### Keamanan yang Sudah Diterapkan di Proyek

1. Multi-guard authentication (admin dan anggota).
2. Middleware role-based access control: admin, pembina, wilayah, anggota.
3. Session hardening saat login/logout:
  - session()->regenerate() setelah login
  - invalidate() + regenerateToken() saat logout
4. Validasi input request di controller utama (create/update/login).
5. Password disimpan dengan hashing (Hash::make / Hash::check).
6. Validasi upload file (tipe image, mimes, batas ukuran).
7. Proteksi brute-force login (throttle:login + RateLimiter).
8. Query parameterized via Eloquent/Query Builder (minim SQL injection).
9. Fallback file serving menggunakan basename() untuk cegah path traversal sederhana.
10. CSRF protection bawaan Laravel untuk request state-changing.

### Keterbatasan

- Verifikasi runtime penuh belum tuntas karena koneksi DB lokal gagal (SQLSTATE[HY000] [2002]) saat pengujian.

### Prioritas 7 Hari

1. Rotate credential DB dan audit jejak secret.
2. Isolasi/hapus script setup dari area publik.