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).

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.
3. Kurangi log sensitif dan retest.