Laporan Audit Keamanan

RawatApp, perawatan dan pembersihan aplikasi bisnis. Contoh laporan nyata, identitas klien disamarkan sebelum diterbitkan.

1. Ringkasan Eksekutif

Situs klien adalah situs PHP satu file (5.181 baris di `index.php`, total 3 file PHP dan 5.289 baris) di hosting bersama. Pemindaian statis menemukan indikasi kuat kompromi: satu webshell aktif yang menyamar sebagai file konfigurasi, satu file entri tak dikenal, dan satu file jejak penyerang. Jejak waktu file menunjukkan insiden terjadi sekitar awal Mei 2026. Sebagian pengaman sudah diterapkan beberapa hari setelahnya (eksekusi PHP diblokir lewat konfigurasi server).

Kesimpulan: Tier C, indikasi webshell/backdoor. Diperlukan tindakan pembersihan dan hardening lengkap. Estimasi 8 sampai 15 jam kerja.

2. Temuan

#	Temuan	Dampak	Lokasi
1	**Webshell aktif**: gerbang password, lalu mengunduh dan mengeksekusi kode dari server pihak ketiga melalui `eval()`	Eksekusi kode arbitrer oleh penyerang, kendali penuh atas situs dan server	`.env.php` baris 44, 59, dan 60
2	File entri tak dikenal `indexx.php` (30 baris), bukan bagian dari situs asli	Pintu masuk potensial	`indexx.php`
3	File `cmd.txt` berisi tulisan tangan penyerang, khas uji akses	Konfirmasi aktivitas manual penyerang	`cmd.txt`
4	Dua file verifikasi Search Console berbeda	Kemungkinan penyerang sempat mengklaim situs	direktori utama
5	Kompatibilitas PHP: 0 error, 2 peringatan minor	Situs asli aman dijalankan di PHP 8.3	`index.php`

Catatan positif: konfigurasi server saat ini sudah memblokir eksekusi semua file PHP dan menolak akses file tersembunyi. Webshell pada temuan 1 kemungkinan sudah tidak bisa dieksekusi, tetapi masih ada di server dan wajib dihapus, karena konfigurasi hosting bisa berubah sewaktu-waktu.

3. Rencana Pekerjaan

1. Snapshot lengkap kode dan database sebagai bukti investigasi.
2. Hapus semua artefak penyerang (temuan 1 sampai 4) dan file asing lain hasil tinjauan manual.
3. Rotasi semua kredensial: password hosting, FTP, database, dan akun admin.
4. Tinjau log akses dan error sekitar tanggal insiden untuk menemukan pintu masuk.
5. Hardening permanen: aturan server, header keamanan, dan pemantauan integritas file.
6. Laporan tindakan tertulis beserta rekomendasi perawatan berkelanjutan.

4. Investasi

Paket	Isi	Harga
Audit (laporan ini)	Pemindaian statis dan laporan tertulis	Rp 200.000, dikreditkan jika paket di bawah dipesan dalam 30 hari
Pembersihan dan Hardening	Butir 1 sampai 6 di atas, garansi 14 hari	Rp 3.000.000 sampai Rp 5.000.000, dikonfirmasi setelah tinjauan log

Pembayaran: 50% di muka, 50% setelah serah terima laporan tindakan.

5. Batasan Audit

Audit ini berbasis pemindaian statis. Kami tidak menjalankan aplikasi dan tidak membaca log server. Batas waktu insiden disimpulkan dari waktu modifikasi file. Tinjauan log akses server, bagian dari paket pembersihan, akan memverifikasi temuan ini.