

Studi Kasus Riset Keamanan — Versi Publik Terealisasi

Daftar isi

Sampul dan kendali dokumen

1. Ringkasan hasil
 2. Scope, otorisasi, dan batas penggunaan
 3. Metode dan mutu bukti
 4. Arsitektur dan trust boundary
 5. F-01 — Kandidat akses baca fungsi admin tanpa otorisasi
 6. F-02 — Kandidat pengungkapan objek user pada respons impersonate
 7. F-03 — Kandidat akses baca data bisnis melalui anon
- ***

8. Observasi yang tidak menjadi finding mandiri

9. Matriks tuple dan batas klaim prioritas
 10. Gap per field dan tindakan verifikasi minimum
 11. Rujukan klasifikasi dan skor
 12. Indeks bukti dan lampiran
- Lampiran A — Dua catatan audit historis lengkap
- Lampiran B — Probe dan recon historis lengkap
- Lampiran C — Manifest seluruh sumber
- Lampiran D — Fingerprint kredensial

Sampul dan kendali dokumen

VERSI PUBLIK TEREDAKSI — ARSIP HISTORIS

Metadata	Nilai
Identitas laporan	***
Pemilik arsip	***
Tanggal observasi sumber	***
Tanggal penyusunan dan pemeriksaan arsip	***
Versi dokumen	2.0 — studi kasus berbasis 15 berkas sumber
Bahasa	Bahasa Indonesia
Tujuan	Mendokumentasikan kasus historis dalam studi teknis publik terealisasi
Klasifikasi	Publik terealisasi; nilai identitas dan provider diganti ***
Status kesimpulan	Kandidat akses baca; belum tervalidasi independen sebagai eksploitasi saat ini
Prioritas	P3-ish candidate; bukan penetapan P1/P2 final
Cakupan operasi penyusunan	Pembacaan offline; tanpa pengujian aktif target

Sumber asli berada dalam arsip privat dan tidak dipublikasikan. Laporan menggunakan kasus September 2026 yang dipilih pengguna. Struktur kasus, field, dan angka agregat yang tercatat dipertahankan; identitas target, endpoint spesifik, dan email diganti ***. API key pengguna, JWT, dan hash autentikasi ditampilkan sebagai ***; sumber asli tidak diubah.

Dokumen disusun sebagai studi kasus teknis: konteks, aset, kondisi awal, langkah yang tercatat, perilaku yang diharapkan dan aktual, dampak, batas bukti, serta fix singkat. Struktur ini tidak mengubah status verifikasi historis dari temuan.

Cara membaca: Lampiran A menyalin klaim dari catatan audit lama. Label P0/P1, takeover, dan dampak hukum pada lampiran bukan keputusan studi kasus ini; ikuti penilaian pada bagian 1-12.

1. Ringkasan hasil

Dua catatan audit bertanggal *** menggambarkan akses ke data administratif dan tabel bisnis ***. Catatan pertama menyebut endpoint administratif pada *** mengembalikan statistik, profil, API key, dan respons fitur impersonasi dalam konteks yang ditulis sebagai tanpa autentikasi. Catatan kedua menyebut akses baca *** menggunakan kredensial anon yang terdapat dalam JavaScript publik. Kedua jalur merupakan kelompok risiko yang berbeda karena lapisan keputusan aksesnya berbeda.

Bukti yang masih tersedia terdiri atas catatan analis, ringkasan probe, HTML, JavaScript frontend, DNS, header beranda, dan daftar URL. Tidak tersedia rekaman request/response HTTP lengkap untuk transaksi admin atau pembacaan tabel. Tidak tersedia kode backend, konfigurasi RLS, sesi pembandingan, dataset hasil pagination, atau bukti perubahan state yang dilanjutkan dengan pemanggilan produk. Karena itu, arsip mendukung rekonstruksi apa yang ditulis oleh penguji lama, tetapi tidak memenuhi dasar untuk mengesahkan setiap klaim dampaknya.

Kesimpulan laporan dibagi menjadi tiga kelompok kandidat: F-01 akses baca fungsi admin; F-02 respons impersonate yang memuat objek pengguna dan hash password menurut catatan; F-03 akses baca tabel bisnis melalui role anon. F-02 tidak dinyatakan sebagai account takeover. F-03 tidak dinyatakan memberi hak tulis atau hapus. Catatan lama tentang P0, P1, manipulasi saldo, seluruh panel admin, pipeline inferensi lengkap, dan pelanggaran hukum tidak diadopsi sebagai kesimpulan laporan ini.

Angka 604 profil, 492 API key, 11 pembayaran, 528 pesan, dan 1.251 transaksi kredit adalah angka yang ditulis dalam ringkasan lama. Pembacaan ulang arsip tidak dapat menghitungnya kembali dari dataset mentah. Delapan contoh API key unik terdapat dalam catatan admin; itu tidak sama dengan bukti tersimpan untuk seluruh 492 key. Angka tersebut perlu dilabeli sebagai cakupan tercatat, bukan populasi korban yang telah diverifikasi.

Kelompok	Observasi historis dalam catatan	Keputusan laporan
F-01	Statistik, API key, dan profil dikatakan terbaca tanpa auth	Kandidat missing authorization pada fungsi admin
F-02	POST impersonate dikatakan mengembalikan success dan user	Kandidat eksposur respons sensitif; sesi korban tidak terbukti
F-03	GET tabel bisnis dikatakan mengembalikan HTTP 200 dengan data	Kandidat kebijakan akses baca anon terlalu luas
WRITE/DELETE	HTTP 204 pada filter ID yang tidak mengenai baris	Tidak membuktikan perubahan atau hak mutasi

Kelompok	Observasi historis dalam catatan	Keputusan laporan
AI inference	Respons insufficient balance dengan satu key contoh	Tidak membuktikan inference, penggunaan layanan, atau tagihan
Email verification	Akun tercatat active; OTP salah ditolak	Bypass verifikasi tidak terbukti

2. Scope, otorisasi, dan batas penggunaan

2.1 Aset yang muncul dalam arsip

Aset	Hubungan yang diamati	Status scope resmi
***	Beranda, signup, verifikasi, dashboard, route user/payment	Unknown; tidak ada brief program tersimpan
***	Route admin dan gateway AI menurut catatan	Unknown; kepemilikan dan izin pengujian belum didokumentasikan
***	URL konfigurasi di bundle signup	Hubungan aplikasi terbukti frontend; izin pengujian project Unknown
Host lain di subdomains.txt	Daftar percobaan host dengan kode 200 atau 000	Penemuan nama bukan perluasan scope

Tidak ada engagement JSON, rujukan otorisasi tertulis, tanggal kedaluwarsa, atau daftar teknik terlarang di 15 berkas ini. Penyusunan laporan privat dari backup adalah pekerjaan offline yang diminta pengguna. Dokumen ini tidak memberikan izin untuk memanggil endpoint target atau meneruskan kasus ke pihak lain. Pengujian baru membutuhkan konteks otorisasi yang sesuai pada saat tindakan dilakukan.

Halaman yang disimpan sebagai security.txt berisi HTML halaman tidak ditemukan, bukan kebijakan disclosure dengan contact dan scope yang tervalidasi. robots.txt memperbolehkan crawling dan menyebut sitemap; isi tersebut bukan surat izin pengujian keamanan. Tidak ditemukan brief pengujian atau kebijakan disclosure yang menetapkan scope resmi. Detail izin dan batas pengujian tetap Unknown.

2.2 Cakupan yang benar-benar dapat dinilai

Penilaian meliputi seluruh 15 berkas dalam folder sumber, bukan seluruh aplikasi ***. Tinjauan memeriksa asal URL dan field, konsistensi catatan, hubungan frontend dengan API, kekuatan bukti dampak, dan koreksi kesimpulan yang melampaui hasil. Tidak dilakukan pengumpulan ulang data, enumerasi akun, penggunaan key, pemanggilan gateway AI, pengujian mutasi, atau pengujian sesi.

Tidak ada dasar untuk menyatakan audit menyeluruh atas autentikasi, pembayaran, penyimpanan, dukungan, dan semua route admin. Daftar route hanya menunjukkan permukaan yang pernah dicatat. Terbukanya satu endpoint tidak membuktikan seluruh panel dapat dijalankan; return HTML tidak membuktikan akses data sensitif di balik UI.

2.3 Waktu dan freshness

Header beranda merekam Tue, *** 11:16:22 GMT, setara 19:16:22 WITA. Waktu modifikasi berkas berkisar 11:16–11:55 UTC. Waktu modifikasi membantu menempatkan arsip, tetapi tidak membuktikan saat eksekusi setiap request. Catatan admin dan RLS hanya memberi tanggal harian; urutan rinci, durasi, dan timezone pengujian tidak ditulis.

Kondisi target saat *** adalah **Not verified**. Tidak ada klaim bahwa endpoint masih terbuka, key masih berlaku, jumlah akun masih sama, atau patch belum dibuat. Penyusunan studi kasus pada *** tidak memperbarui keadaan aplikasi maupun bukti scope pengujian.

3. Metode dan mutu bukti

3.1 Pengelompokan bukti

Bukti primer lokal yang dapat diperiksa langsung adalah isi berkas tersimpan. JavaScript membuktikan string konfigurasi dan alur frontend yang terkandung dalam bundle. Header membuktikan respons beranda tersimpan. Catatan audit merupakan bukti sekunder terhadap transaksi API: pembaca dapat memverifikasi bahwa pernyataan itu ditulis, tetapi tidak dapat memverifikasi paket HTTP asli hanya dari ringkasannya.

Label **Observed** dalam laporan berarti terlihat pada arsip tertentu. Untuk transaksi admin/REST, label tersebut selalu dibaca sebagai “Observed dalam catatan historis”. **Inference** berarti penjelasan yang konsisten dengan catatan tetapi implementasinya belum terlihat. **Not proven** berarti efek yang diklaim tidak memiliki bukti cukup. **Not verified** berarti belum diperiksa independen atau pada runtime saat ini. **Unknown** menandai informasi yang belum tersedia.

3.2 Pemeriksaan yang selesai

Seluruh berkas dibaca offline dan dicocokkan dengan manifest sumber. Manifest berisi nama, byte, SHA-256, path, dan mtime untuk setiap berkas. Pemeriksaan checksum membuktikan konsistensi isi backup dengan manifest saat penyusunan. Checksum tidak membuktikan siapa yang mengumpulkan data, kelengkapan sesi asli, validitas otorisasi, atau kebenaran kesimpulan penulis lama.

Teks dipindai untuk mengenali kredensial sebelum masuk laporan. Sepuluh kredensial unik tercatat sebagai fingerprint: delapan API key pengguna, satu JWT anon ***, dan satu bcrypt hash. Metadata ini menjaga hubungan antara sumber dan lampiran tanpa mencetak material autentikasi. Tidak ada cracking hash atau penggunaan kredensial untuk validasi.

3.3 Gerbang verifikasi klaim

Gate	Status dan alasan	Bukti minimum yang belum tersedia
Reproduksi dari sesi bersih	Belum lulus; header request admin/REST hilang	Request/response dan konteks cookie/auth lengkap
Scope dan accepted impact	Unknown; brief tidak ada	Brief program dan izin aset yang berlaku
Batas aktor/owner	Belum lulus; tidak ada dua identitas terkendali	Marker akun peneliti dan hasil pembandingan
Dampak baca	Dicatat, belum divalidasi independen	Respons raw dengan data terkendali di luar hak aktor

Gate	Status dan alasan	Bukti minimum yang belum tersedia
Dampak mutasi	Tidak terbukti	State awal/akhir dan efek panggilan produk
Deduplication	Not verified	Known issue atau hasil pemeriksaan resmi
Kesiapan lampiran	Parsial; catatan dan JS ada	Raw HTTP transaksi penentu dan bukti runtime

Dengan hasil gate tersebut, studi kasus berstatus **REKONSTRUKSI HISTORIS — BELUM TERVERIFIKASI INDEPENDEN**. Uraian langkah dan severity bersyarat tidak boleh dibaca sebagai hasil pengujian baru.

4. Arsitektur dan trust boundary

4.1 Komponen yang memiliki bukti

headers.txt memuat header *** dan ***. Beranda menggunakan route dan chunk /_next/***. Versi *** server tidak tersimpan. js-signup-page.js modul 3941 membuat klien *** untuk project *** dengan konfigurasi auth pkce, autoRefreshToken, detectSessionInUrl, dan persistSession. Ini menghubungkan frontend dengan URL project; konfigurasi browser bukan bukti izin data pada backend.

Bundle js-***-client.txt memuat versi *** JS 2.57.4 dan *** 2.71.1 pada baris 21, sekitar offset karakter 45442 dan 45634. Offset dihitung dari nol atas teks Unicode. Angka tersebut adalah versi string pada SDK browser yang tersimpan. Versi database, ***, backend route, runtime Node, middleware auth, dan SQL policy adalah Unknown. Tidak ada CVE yang dipilih atau dicocokkan hanya dari kedua string versi tersebut.

4.2 Alur pendaftaran dan verifikasi yang tersimpan

Bundle signup memiliki fetch ke /api/*** dengan body email, password, dan attribution. Sesudah respons yang dianggap berhasil, frontend mengarahkan pengguna ke /verify-email?email=... Bundle verifikasi mengirim email dan OTP ke /api/***; respons error tampil di UI. Sesudah respons sukses, frontend menyimpan userEmail dan userData, mengisi cookie user-data, lalu berpindah ke dashboard. Bundle juga memanggil /api/***.

Penyimpanan objek user pada browser adalah observasi desain frontend. Tidak ada bukti bahwa backend menerima isi cookie tersebut sebagai otoritas role atau identitas. Menemukan cookie yang dapat ditulis JavaScript tidak cukup untuk menyimpulkan bypass server. Catatan /api/*** dan /api/*** yang mengembalikan Unauthorized bahkan menunjukkan adanya penolakan pada permukaan tertentu, meskipun mekanisme penolakannya belum terlihat.

4.3 Batas kepercayaan yang dianalisis

Jalur	Input dari batas luar	Keputusan akses yang semestinya	Bukti yang tersedia
Browser → signup/OTP	Email, password, attribution, OTP	Validasi pendaftaran dan verifikasi	Fetch frontend dan ringkasan probe
Pemanggil → admin API	Request admin, filter, userId	Identitas dan privilege admin pada server	Catatan sekunder; backend tidak ada

Jalur	Input dari batas luar	Keputusan akses yang semestinya	Bukti yang tersedia
Browser/klien → *** REST	Role anon dan pemilihan tabel/filter	Izin tabel/kolom/baris sesuai role	Konfigurasi publik dan catatan read
Pemanggil → AI gateway	API key dan model	Validasi key, izin, saldo, pemakaian	Error ringkas dalam catatan
Browser → payment channel	Permintaan katalog channel	Konten publik sesuai desain produk	Bundle dashboard dan probe 200

Dua dugaan kegagalan yang paling relevan berada di keputusan privilege admin dan pembatasan pembacaan tabel bisnis. Dangerous sink tidak dapat diverifikasi dari kode server yang tidak tersedia. Laporan tidak menebak nama fungsi auth, query SQL, middleware, atau policy. Root cause tetap dijelaskan pada lapisan yang didukung bukti: respons administratif atau data bisnis tercatat melewati batas akses yang diharapkan.

5. F-01 — Kandidat akses baca fungsi admin tanpa otorisasi

5.1 Identitas dan aset

Judul: Catatan API admin *** menunjukkan pengungkapan key, profil, dan statistik dalam konteks yang dicatat sebagai tanpa autentikasi.

Klasifikasi kerja: Missing authorization pada fungsi administratif; CWE-862 merupakan mapping kandidat yang lebih dekat. OWASP API5:2023 Broken Function Level Authorization digunakan sebagai kategori analisis, bukan klaim uji framework lengkap. CWE-284 adalah kategori lebih umum. BOLA/CWE-639 belum dibuktikan karena tidak ada pasangan aktor dan owner terkendali.

Referensi: admin-panel-audit.md baris 6–24 dan 30–33. **Status:** Observed dalam catatan historis; Not verified independen maupun pada target saat ini.

5.2 Endpoint dan data tercatat

Endpoint historis	Metode	Isi yang dicatat
/api/***	GET	Jumlah user/key, credits, balance, service, domain
/api/***	GET	Key, owner, nama key, status, waktu, credit_limit
/api/***	GET	Profil, kontak, role, status, credits, balance, financials
`/api/***	30d all`	GET

Ringkasan stats mencantumkan totalUsers=604, totalApiKeys=492, totalCredits=1283.0487227709716, totalBalance=4012207.4206026597, activeServices=7, suspendedServices=67, dan activeDomains=4. Unit mata uang totalBalance tidak ditetapkan oleh snippet. Angka ini tidak ditulis sebagai nilai uang yang telah dicuri atau tagihan akibat pengujian.

Untuk API key, catatan menyebut 25 halaman dengan 20 key per halaman kecuali halaman terakhir berisi 12. Perhitungan $24 \times 20 + 12$ konsisten dengan 492, tetapi respons semua halaman tidak tersimpan. Delapan contoh key tercatat bersama nama key dan beberapa email. Laporan memuat fingerprint agar bukti contoh tetap dapat dicocokkan. Klaim cakupan semua key menunggu dataset pagination yang dapat diperiksa.

5.3 Kondisi awal dan rekonstruksi historis

Kondisi awal menurut penulis lama adalah request tanpa autentikasi. Arti teknisnya belum dapat diaudit karena header Authorization, Cookie, proxy state, dan konfigurasi client tidak tersimpan. Tidak ada biaya, privilege, atau akun penyerang yang dapat ditetapkan sebagai fakta dari arsip ini.

1. Catatan lama menempatkan host administratif pada *** dan memberi label “tanpa auth”.
2. Penguji lama mencatat hasil GET summary dengan objek statistik yang dicantumkan di atas.
3. Penguji mencatat daftar API key berpaginasi dan delapan contoh; field `api_key` dijelaskan sebagai plaintext.
4. Penguji mencatat daftar user dengan email, nama, nomor telepon, status akun, dan finansial.
5. Penguji mencatat statistik 30 hari sebesar 39.321 request dan \$100.83 cost, termasuk breakdown model.
6. Tidak ada transaksi HTTP raw yang memungkinkan pembaca memverifikasi bahwa semua panggilan berasal dari konteks bersih yang sama.

Langkah ini merupakan rekonstruksi catatan, bukan instruksi yang dieksekusi saat penyusunan. Nama host/route dipertahankan karena ada pada sumber. Tidak dibuat payload, curl, ataupun script untuk menguji ulang sistem eksternal.

5.4 Expected versus actual

Expected: fungsi administrative yang mengeluarkan secret atau data nonpublik memerlukan identitas dan privilege admin yang valid. Pemanggil tanpa kewenangan seharusnya tidak menerima key, profil lengkap, atau agregat bisnis privat.

Actual menurut arsip: catatan mengaku menerima field sensitif dari endpoint tersebut tanpa auth. Snippet summary memberi contoh konkret bentuk data, sedangkan body lengkap daftar key/users tidak tersedia. Pernyataan penulis lama belum membuktikan keadaan header dan hak akses pemanggil.

5.5 Root cause dan batas dampak

Inference: keputusan otorisasi pada fungsi admin tidak diterapkan dengan benar atau tidak mencakup jalur respons tersebut, jika konteks tanpa auth yang ditulis benar. Tidak diketahui apakah penyebabnya middleware yang tidak dipasang, pemeriksaan role yang salah, deployment yang berbeda, cache, atau request yang sebenarnya membawa state sesi. Laporan tidak memilih salah satu tanpa bukti backend/raw request.

Dampak yang tercatat adalah kerahasiaan: akses key, kontak/profil, dan data agregat penggunaan. Delapan key yang tertulis adalah material sensitif; penanganan internal perlu mempertimbangkan apakah key masih aktif. Tidak ada bukti bahwa seluruh key dapat digunakan, akun memiliki saldo positif, layanan selesai dijalankan, atau biaya benar-benar berpindah. Pengungkapan field `user_financials` tidak membuktikan kemampuan mengubahnya.

Tidak ada dampak integritas atau availability yang ditunjukkan. Tidak ada transaksi pembayaran tak sah, perubahan role, penghapusan data, atau eksploitasi provider downstream. Risiko privasi masuk akal berdasarkan jenis field kontak dan finansial yang disebut, namun status pelanggaran hukum tidak dapat diputuskan dari arsip.

5.6 Severity, fix note, dan retest

Prioritas kerja adalah P3-ish candidate karena bukti penentu belum cukup untuk final severity. **CVSS 3.1 conditional 7.5** dengan vector AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N hanya berlaku apabila respons privat lintas akun benar-benar dapat diperoleh melalui network tanpa privilege, tanpa interaksi korban, dengan confidentiality high. Ini tidak menetapkan P2, P1, atau seluruh cakupan user secara otomatis.

Fix note: terapkan keputusan identitas dan privilege administratif pada server untuk setiap route admin sebelum data sensitif diserialisasi. Keluarkan API key dan material autentikasi dari respons yang tidak memerlukannya.

Retest penerimaan: pihak yang berwenang memeriksa respons dengan konteks tanpa sesi, user biasa, dan admin terhadap data uji yang disepakati; respons nonadmin tidak boleh memuat field privat, sedangkan alur admin yang sah tetap berfungsi. Arsip belum memuat hasil retest tersebut.

6. F-02 — Kandidat pengungkapan objek user pada respons impersonate

6.1 Bukti dan kondisi

Catatan admin-panel-audit.md baris 26–28 mencantumkan POST /api/** dengan userId=**, lalu respons ringkas success:true dan user. Field yang disebut mencakup email, role, credits, balance, nama, no_hp, auth_provider, dan password berupa bcrypt. Fingerprint bcrypt terdapat pada lampiran kredensial.

Objek user ini berhubungan dengan akun probe yang juga disebut pada catatan signup. Karena identitas itu merupakan akun probe, penerimaan data akun tersebut saja tidak membuktikan akses ke korban lain. Konteks tanpa auth tetap merupakan pernyataan penulis lama yang belum dilengkapi raw header. Tidak ada Set-Cookie, token sesi baru, auth code, refresh token, atau panggilan produk menggunakan identitas hasil impersonasi.

6.2 Rekonstruksi historis dan expected/actual

1. Akun probe ** dicatat tercipta melalui signup dan memiliki ID yang mulai **.
2. Catatan admin menuliskan userId lengkap pada panggilan impersonate.
3. Respons diringkas sebagai success dan user dengan field yang disebutkan.
4. Tidak terdapat tindakan sesudah respons yang membuktikan akses dashboard, pembacaan data korban, atau perubahan finansial atas identitas hasil respons.

Expected: fungsi impersonasi yang sensitif memerlukan kewenangan admin; hash password tidak diperlukan sebagai atribut respons browser. **Actual menurut catatan:** objek user dan hash tercatat dikembalikan. Perilaku ini mendukung kandidat eksposur respons, bukan penyelesaian account takeover.

6.3 Root cause dan dampak terbatas

Inference: route mengembalikan terlalu banyak atribut user dan keputusan privilege perlu ditinjau. Serialisasi seluruh record database adalah kemungkinan, bukan hasil inspeksi source. Tidak diketahui apakah field password benar-benar berasal langsung dari tabel atau dari object lain pada backend.

Eksposur hash merupakan masalah kerahasiaan material verifikasi password jika respons dan konteksnya benar. Hash bukan password plaintext. Tidak dilakukan pemecahan hash; tidak ada hasil password atau sesi login. Label “takeover penuh” pada catatan lama dihapus dari kesimpulan. Tidak ada dasar untuk menetapkan severity tersendiri berbasis takeover, menggabungkan efek korban yang belum terlihat, atau mengklaim seluruh user dapat diimpersonasi.

Fix note: batasi route impersonasi pada admin yang sah dan whitelist atribut respons; jangan serialisasikan password hash atau secret akun. **Retest penerimaan:** respons pada data uji tidak memuat password/material autentikasi dan penolakan nonadmin terverifikasi; alur impersonasi sah diperiksa oleh pemilik sistem dengan identitas terkendali.

Status F-02 tetap kandidat. Penentuan apakah ia akar masalah terpisah dari F-01 menunggu bukti implementasi. Nama fitur berbeda tidak otomatis berarti root cause berbeda.

7. F-03 — Kandidat akses baca data bisnis melalui anon ***

7.1 Aset dan asal kredensial

js-signup-page.js baris 1 modul 3941 mengonfigurasi project *** yang sama dengan api-probes.txt dan ***-rls-audit.md. JWT pada arsip memiliki role claim anon, ref project, issuer ***, serta iat/exp yang dicatat. Tidak dilakukan validasi tanda tangan atau validitas runtime; JWT tersedia sebagai fingerprint SHA-256.

Keberadaan konfigurasi anon di JavaScript frontend adalah observasi desain client. Temuan yang relevan adalah data nonpublik yang menurut catatan dapat dibaca dengan role itu. Public key sendiri tidak dinyatakan sebagai secret server yang bocor. Tidak ada service_role credential dalam bundle yang ditunjukkan oleh sumber.

7.2 Hasil baca dalam catatan

Tabel	Hasil/jumlah tercatat	Field atau isi yang disebut
profiles	HTTP 200; 604 baris	id, email, role, credits, nama, no_hp, balance, status
payments	HTTP 200; 11 baris	user_id, order_id, amount, credits, status, payment_type
messages	HTTP 200; 528 baris	conversation_id, role, content, feedback, created_at
credit_transactions	HTTP 200; 1.251 baris	user_id, amount, riwayat finansial
services	HTTP 200; jumlah Unknown	Nama layanan dan display_name
plans	HTTP 200; jumlah Unknown	service_id dan harga
api_usage	HTTP 200; jumlah Unknown	user_id dan endpoint
api_keys	HTTP 200; kosong	Tidak ada record sensitif terbukti pada jalur ini
domain_orders	HTTP 200; kosong	Tidak ada record sensitif terbukti pada jalur ini

Referensi tabel adalah ***-rls-audit.md baris 13–24. Dataset raw tidak tersedia. Tidak dapat diperiksa nilai content pesan, penerima pembayaran, ownership setiap row, pagination, header count, atau apakah jumlah yang tertulis berasal dari satu respons, beberapa halaman, maupun total query.

Services dan plans mungkin merupakan katalog publik; sifat privatnya tidak ditetapkan oleh arsip. Api_usage menyebut field user_id/endpoint namun tidak memberi jumlah atau contoh row. Laporan menempatkan kelompok profil, pembayaran, pesan, dan transaksi kredit sebagai kandidat utama karena jenis datanya berkaitan dengan pengguna dan operasi bisnis.

7.3 Rekonstruksi historis

1. Penguji lama mengekstrak URL project dan JWT anon dari bundle signup.
2. Catatan menyebut pembacaan tabel REST dilakukan dengan key tersebut tanpa login.
3. HTTP 200 dan jumlah data dicatat untuk empat tabel bisnis utama.
4. Catatan tambahan menyebut lookup profil akun probe menggunakan filter email menghasilkan objek role user dengan saldo nol dan status active.
5. Catatan juga mencantumkan no-op PATCH/DELETE yang mengenai nol baris; tidak ada perubahan sebelum/sesudah tersimpan.
6. Bukti raw read lintas akun dan state mutasi tidak tersedia dalam folder sumber.

Langkah ini menjaga teknik *** REST terpisah dari route admin aplikasi. Tidak diasumsikan kedua jalur memakai credential atau middleware yang sama. Root hint yang menyebut service_role tidak menjembatani bukti tersebut.

7.4 Expected/actual dan root cause

Expected: akses role anon terhadap tabel yang memuat profil, percakapan, dan finansial dibatasi sesuai kebijakan pemilik data. **Actual menurut catatan:** data dari tabel tersebut dikatakan terbaca tanpa login. Hak publik yang memang dirancang untuk katalog perlu dibedakan sebelum seluruh HTTP 200 dianggap masalah.

Inference: konfigurasi grant, policy SELECT/RLS, view, atau jalur API memberi akses baca lebih luas dari kebijakan yang diharapkan. Tidak ada SQL policy maupun schema untuk memastikan bahwa RLS disabled, policy menggunakan ekspresi terlalu permisif, atau objek tertentu merupakan view. Root cause spesifik tetap Unknown.

Mapping kerja adalah CWE-284; CWE-862 relevan jika otorisasi tidak ada pada permukaan data. BOLA/CWE-639 memerlukan bukti pemilihan object milik identitas lain yang melanggar ownership, belum tersedia. Karena aktor dinyatakan anon, missing access control dapat menjadi deskripsi lebih tepat daripada IDOR klasik dengan dua sesi login.

7.5 Dampak, mutasi, dan severity

Dampak baca yang diklaim meliputi profil/kontak, referensi pembayaran, isi pesan, dan riwayat kredit. Isi pesan tidak dikutip sehingga sifat sensitif tiap pesan belum dapat dinilai. Tidak ada bukti seluruh rows merupakan data korban atau bahwa data dikeluarkan tanpa hak di runtime saat ini. Potensi luas data tidak menggantikan verifikasi ownership.

PATCH dan DELETE dengan filter ID nol yang tidak cocok menghasilkan HTTP 204 menurut catatan. Respons sukses kosong dapat terjadi ketika nol baris terpengaruh atau kebijakan tidak menampilkan/menjangkau row yang diminta. Tanpa record uji yang berubah dan pembacaan setelah perubahan, tidak terbukti hak UPDATE/DELETE. Laporan tidak menyimpulkan manipulasi role, credits, balance, pencurian layanan, atau penghapusan profil.

Prioritas kerja tetap P3-ish candidate. CVSS 7.5 conditional dapat digunakan sebagai skenario confidentiality-only apabila akses anon ke data privat lintas pengguna benar-benar terverifikasi. Nilai integritas/availability tetap N pada skenario tersebut; tidak dinaikkan berdasarkan no-op.

Fix note: sesuaikan grant dan policy akses baca anon pada tabel/view bisnis dengan batas data yang dimaksud; pisahkan data katalog publik dari profil, pesan, dan finansial privat. **Retest penerimaan:** pemilik sistem membandingkan respons role anon, user A, dan user B pada record uji berowner jelas; data privat tidak keluar dari batas ownership yang sah. Retest mutasi membutuhkan bukti state tersendiri dan bukan syarat yang sudah lulus dalam arsip ini.

8. Observasi yang tidak menjadi finding mandiri

Observasi	Kesimpulan yang sah	Klaim yang tidak didukung
Signup success dan requiresVerification:true	Pendaftaran dicatat berhasil dan verifikasi diminta	Akses layanan penuh sebelum verifikasi
account_status:active dan email_verified:false	Dua field status memiliki nilai berbeda	Status active meniadakan semua gate OTP
OTP salah, 4 attempts remaining	Penolakan kode salah tercatat	Brute force berhasil atau limit global 5 pasti
Resend otpSent:true	Respons aplikasi menyatakan pengiriman	Email benar terkirim atau rate limit tidak ada
Model catalog 200, 77+ model	Katalog model dicatat dapat diakses	Model valid untuk inference atau rahasia bisnis
*** channels 200	Metadata channel pembayaran tercatat	Bypass pembayaran atau fraud
REST api_keys/domain_orders kosong	Endpoint merespons tanpa data row	Secret dari dua tabel tersebut terungkap
PGRST205 hint tabel	Nama schema/table muncul pada catatan	Akses isi seluruh tabel atau hak mutasi
REST root Invalid API key + service_role hint	Pesan validasi root tercatat	Backend aplikasi terbukti memakai service_role
Missing API key / Invalid API key	Penolakan gateway berbeda menurut catatan	Seluruh validasi gateway aman atau seluruh route lemah
Insufficient balance dengan key contoh	Catatan konsisten dengan key melewati sebagian validasi	Inferensi selesai, biaya timbul, saldo korban dipakai
Header *** / ***	Fingerprint permukaan beranda	Versi backend pasti atau CVE berlaku

Catatan lama menyatakan “pipeline lengkap bekerja” hingga inference. Respons insufficient balance justru tidak memuat hasil model. Indikasi bahwa key dikenali berguna untuk konteks eksposur key, tetapi efek pemakaian produk masih Not proven. Model yang tertulis dalam statistik adalah nama historis di catatan; laporan tidak memverifikasi keberadaan atau rilis terkini model itu.

Subdomains memuat *** -> 000, sedangkan catatan admin kemudian menyebut respons dari host tersebut. Kode 000 bukan status HTTP server. Cause dan waktu percobaan tidak cukup rinci untuk menentukan apakah terjadi timeout, TLS error, koneksi gagal, atau keadaan lain. Dua observasi dicatat sebagai gap konsistensi; salah satunya tidak dipakai untuk menghapus atau membenarkan yang lain tanpa raw log.

wayback.txt mencatat timeout setelah 40001 milidetik dengan nol byte, bukan hasil pencarian arsip tanpa entri. sitemap.txt terpotong di bagian changefreq contact; tidak dianggap inventaris route lengkap. Kegagalan akuisisi dan truncation membatasi cakupan recon yang dapat direkonstruksi.

9. Matriks tuple dan batas klaim prioritas

Kelompok	PRODUCT-CONTROL	STATE-CHANGE	POST-CHANGE-CALL	EFFECT	Putusan
Admin read	Label tanpa auth pada catatan	Tidak ada mutasi terbukti	Tidak tersedia	Read sensitif dicatat	Kandidat confidentiality; P1/P2 belum sah
Impersonate	Route menerima userId menurut catatan	Sesi/identitas tidak terbukti berubah	Tidak ada pemanggilan atas identitas hasil	User object/ hash dicatat	ATO tidak terbukti
*** read	Role anon di bundle/catatan	Tidak ada perubahan data	Tidak relevan untuk read murni; tidak direkayasa	Jumlah row dicatat	Kandidat read; cross-owner belum diverifikasi
*** PATCH/DELETE	Method diterima menurut catatan	Nol row target; tidak ada perubahan	Tidak tersedia	Tidak tersedia	Write/delete tidak terbukti
Key → AI gateway	Key contoh dipakai menurut catatan	Saldo/usage tidak terbukti berubah	Tidak tersedia	Insufficient balance	Inference/ tagihan tidak terbukti

Read-only tidak membutuhkan perubahan state untuk menjelaskan confidentiality. Namun tuple yang diwajibkan untuk klaim prioritas final tidak boleh diisi dengan peristiwa fiktif. Dalam laporan ini tidak ada klaim final P1/P2, dan tidak ada efek mutasi yang dikonversi dari respons sukses tanpa data.

10. Gap per field dan tindakan verifikasi minimum

Field pelaporan	Isi saat ini	Gap dan pemeriksaan minimum
Otorisasi pengujian	Unknown	Brief dan izin tertulis yang valid
Aset scoped	Tiga host muncul pada arsip	Konfirmasi exact host serta project pihak ketiga
Session/actor	Tanpa auth/anon menurut catatan	Rekaman request bersih tanpa cookie/session tak sengaja
Victim/owner	Akun probe dan statistik	Owner marker berbeda dalam data uji terkendali
Request lengkap	Metode/route parsial	Header, body, waktu, konteks identitas lengkap

Field pelaporan	Isi saat ini	Gap dan pemeriksaan minimum
Response lengkap	Snippet dan ringkasan	Raw status/header/body untuk setiap transaksi penentu
Root cause	Inference pada otorisasi	Source server atau SQL policy yang relevan
Cakupan populasi	Angka ringkasan lama	Dataset/pagination/count yang dapat dihitung ulang
Efek mutasi	Not proven	State awal/akhir, call sesudahnya, efek produk
Severity final	Candidate	Dampak yang terverifikasi dan dasar skor yang sesuai
Fix/retest	Kriteria penerimaan tersedia	Hasil retest setelah patch dari pihak berwenang
Status terkini	Not verified	Verifikasi saat ini dalam engagement yang sah

Tindakan minimum berikutnya adalah mendapatkan bukti mentah historis yang masih dimiliki pemilik arsip atau pemilik sistem, terutama transaksi penentu dan ownership. Bila bukti tersebut tidak ada, studi kasus tetap menjadi arsip risiko yang jujur; kelengkapan format tidak mengubah klaim yang belum terverifikasi menjadi temuan terkonfirmasi.

11. Rujukan klasifikasi dan skor

Tidak ada CVE, status patch, atau keadaan runtime terkini yang diklaim dari arsip ini. String versi SDK browser tidak diperlakukan sebagai versi backend yang pasti rentan.

- [MITRE CWE-862 - Missing Authorization](#): rujukan kategori kandidat keputusan otorisasi yang tidak ada.
- [OWASP API5:2023 - Broken Function Level Authorization](#): rujukan perbedaan hak akses fungsi administratif.
- [FIRST CVSS v3.1 Specification](#): rujukan metrik dan perhitungan skor bersyarat. Vector lengkap yang dibahas adalah CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N, skor 7.5. Asumsi akses tanpa privilege dan confidentiality high masih memerlukan pembuktian; skor tidak mengesahkan temuan atau prioritas program.

Rujukan klasifikasi menjelaskan kategori dan metrik. Keputusan tentang kasus historis ini tetap mengikuti bukti lokal dan batas penilaian di atas.

12. Indeks bukti dan lampiran

Lampiran A memuat seluruh isi dua catatan Markdown sumber setelah substitusi kredensial. **Label severity, hukum, takeover, dan akses tulis di lampiran adalah teks historis penulis lama, bukan kesimpulan laporan.** Koreksi yang berlaku adalah bagian 1–11 di atas. Pemeliharaan teks sumber memungkinkan pembaca mengaudit perbedaan antara observasi awal dan keputusan laporan.

Lampiran B memuat ringkasan probe mentah yang tersimpan, DNS, header, robots, sitemap, subdomains, dan timeout wayback. Istilah “mentah” hanya berarti isi file asal ditampilkan, bukan bahwa api-probes.txt merupakan capture lengkap transaksi HTTP. HTML dan bundle JavaScript tidak dicetak seluruhnya karena bersifat minified/panjang; file lengkap tetap tersedia pada arsip dan diindeks pada lampiran C.

Lampiran C memuat hash seluruh 15 file untuk penelusuran. Lampiran D memuat fingerprint sepuluh kredensial unik. Manifest dan fingerprint tidak membuka akses target. Email dan identitas pada sumber privat diganti *** dalam versi publik ini.

Lampiran A — Dua catatan audit historis lengkap

Teks di bawah adalah isi sumber, termasuk penilaian awal yang sudah dikoreksi dalam laporan utama. Kredensial dan identitas diganti ***. Lampiran ini adalah transkripsi teredaksi; sumber privat tidak dipublikasikan.

A. admin-panel-audit.md

```
# AUDIT ADMIN PANEL + AI API — *** / ***
# Tanggal: *** | Status: P0 — Admin API tanpa autentikasi (CWE-284, OWASP API1:2023
BOLA, OWASP A01:2025)

## P0: Admin API TANPA AUTENTIKASI (***)

### 1. /api/*** (GET, tanpa auth)
{"totalUsers":604,"totalApiKeys":492,"totalCredits":1283.0487227709716,"totalBalance":4012207.420602
6597,"activeServices":7,"suspendedServices":67,"activeDomains":4}

### 2. /api/*** (GET, tanpa auth) — 492 API KEY PLAINTEXT
- 25 halaman x 20 key (halaman terakhir 12) = 492 key
- Field: id, user_id, key_name, api_key (sk-* plaintext), is_active, created_at, last_used_at,
credit_limit, user.email, user.nama
- Contoh key ter-expose:
  - [SHA256:***] (key, pemilik, label: ***)
  - [SHA256:***] (key, pemilik, label: ***)
  - [SHA256:***] (key, pemilik, label: ***)
  - [SHA256:***] (key, pemilik, label: ***)
  - [SHA256:***] (key, pemilik, label: ***)
  - [SHA256:***] (key, pemilik, label: ***)
  - [SHA256:***] (key, pemilik, label: ***)
  - [SHA256:***] (key, pemilik, label: ***)

### 3. /api/*** (GET, tanpa auth) — 604 USER LENGKAP
- Field: id, email, nama, no_hp, created_at, auth_provider, email_verified, role,
account_status, credits, balance, user_financials
- Termasuk akun probe: *** (email_verified:false, account_status:"active")

### 4. /api/*** (POST, tanpa auth) — IMPERSONASI + PASSWORD HASH
- POST {"userId":"****"} -> {"success":true,"user":{...}}
- Mengembalikan: email, role, credits, balance, nama, no_hp, auth_provider, password (bcrypt
hash: [SHA256:***])

### 5. /api/***|30d|all (GET, tanpa auth) — USAGE + DAILY
- 30 hari: 39.321 request, $100.83 total cost
- Model terpakai (30d): *** 31.185 req ($23.41), *** 1.694
($10.20), *** 1.501 ($1.62), *** 1.443 ($12.05), *** 700 ($3.92),
*** 453, *** 415 ($15.39), *** 357, *** 265,
*** 219, *** 210, *** 176, ***
78, *** 76 ($5.02), *** 73, *** 68, ***
63, *** 60, *** 55 ($9.39), other 38
- Daily usage per tanggal (1/9 s.d. sekarang) dengan breakdown per model

## Test LLM (chat completions)
- Key ter-expose VALID:
```

```
[SHA256:***]
- POST /v1/** {model: ***/**} -> {"error":"Insufficient
balance","details":"Your account balance is $0.0000. Please top up your account to continue
using the API."}
- POST /v1/** {model: **} -> sama (Insufficient balance)
- Kesimpulan: pipeline lengkap bekerja (auth -> validasi key -> cek balance -> inference). Key
valid, akun tanpa balance.
- Tanpa key: {"error":"Missing API key"}; key palsu: {"error":"Invalid API key"}; **
anon JWT: {"error":"Invalid API key"}

## Endpoint lain
- /api/** (**, tanpa auth) -> {"rate":17837}
- /api/**, /api/** (**) -> {"error":"Unauthorized"} (auth aktif di
sisi user)
- /api/**, /api/** (**) – payment gateway kedua (**)
selain **
- /api/** (**) – topup credits
- Admin pages (HTML): /admin, /admin/**, /admin/**, /admin/**,
/admin/**, /admin/**, /admin/**, /admin/**,
/admin/**, /admin/**, /admin/**, /admin/**,
/admin/**, /admin/**, /admin/**, /admin/**, /admin/**

## Dampak
1. P0: Seluruh admin panel dapat diakses tanpa autentikasi – 492 API key plaintext, 604 profil
user (PII), password hash bcrypt, data finansial
2. P1: ** RLS terbuka (baca+tulis+hapus) – lihat **-rls-audit.md
3. P1: 604 profil + 11 pembayaran + 528 pesan + 1.251 transaksi kredit terbaca publik
4. PII: email, nama, no_hp, balance, riwayat transaksi – pelanggaran UU PDP No. 27/2022
5. Impersonate memungkinkan takeover akun penuh (password hash bcrypt bisa di-crack/offline)

## Mapping
- CWE-284 (Improper Access Control), CWE-639 (Authorization Bypass), CWE-522 (Insufficiently
Protected Credentials)
- OWASP API1:2023 BOLA, OWASP API2:2023 Broken Authentication
- OWASP A01:2025 Broken Access Control
- WSTG-ATHZ-02 (Bypassing Authorization Schema)
- UU PDP No. 27/2022
```

A. ***-rls-audit.md

```
# AUDIT ** RLS – ** (**)
# Tanggal: ** | Metode: anon key publik dari JS bundle (js-signup-page.js:1)
# Status: P1 – Broken Object Level Authorization / RLS misconfiguration (CWE-639/CWE-284,
OWASP API1:2023 BOLA, OWASP A01:2025)

## Kredensial ter-expose (dari JS publik, tanpa autentikasi)
- ** URL: **
- Anon key (JWT HS256):
[SHA256:***]
- JWT claims: iss=**, ref=**, role=anon, iat=1756869152,
exp=2072445152
- Sumber: ** (baris
1, modul 3941)

## Hasil probe REST (semua dengan anon key, tanpa login)

### READ – data terbaca (HTTP 200)
| Tabel | Jumlah baris | Data ter-expose |
|---|---|---|
| profiles | 604 | id, email, role, credits, nama, no_hp, balance, auth_provider,
account_status, status_reason, status_changed_by, suspended_until, deactivated_at |
| payments | 11 | id, user_id, order_id, amount, credits, status, payment_type,
**_transaction_id, created_at |
| messages | 528 | id, conversation_id, role, content, feedback, created_at |
| credit_transactions | 1251 | id, user_id, amount, (riwayat finansial) |
| services | 200 OK | nama layanan, display_name |
```

```

| plans | 200 OK | service_id, harga |
| api_usage | 200 OK | user_id, endpoint |
| api_keys | 200 OK (kosong) | tabel ter-expose |
| domain_orders | 200 OK (kosong) | tabel ter-expose |

### WRITE – akses tulis terbuka (no-op, 0 baris terpengaruh)
- PATCH /rest/** -> HTTP 204 (DIIZINKAN)
- PATCH /rest/** -> HTTP 204 (DIIZINKAN)
- DELETE /rest/** -> HTTP 204 (DIIZINKAN)

### Enumeration schema via error hint (PGRST205)
Tabel terkonfirmasi: services, payments, plans, credit_transactions, domain_orders, api_keys,
profiles, user_attributions, credit_audit_log, api_usage, messages, system_messages,
support_tickets

### Bukti akun tanpa verifikasi
- POST /api/** {email: **} ->
{"success":true,"requiresVerification":true,"otpSent":true}
- GET /rest/** ->
[{"id":****,"email":****,"role":"user","credits":0,"balance":0.00,"account_status":"active"}]
- Kesimpulan: akun tercipta dan LANGSUNG AKTIF tanpa verifikasi email (account_status=active)

## Endpoint lain yang diuji
- GET /api/** -> 200 tanpa auth (channel VA/QRIS/e-wallet, merchant ** aktif)
- POST /api/** (OTP salah) -> {"error":"Invalid or expired verification code. 4
attempts remaining."} (rate limit 5x)
- POST /api/** -> {"success":true,"otpSent":true} (tanpa rate limit terlihat)
- GET ** -> 200 tanpa auth (77+ model terdaftar)
- POST ** tanpa key -> {"error":"Missing API key"}
- POST ** key palsu -> {"error":"Invalid API key"}
- GET /rest/** (root) -> {"message":"Invalid API key","hint":"Only the service_role API key
can be used for this endpoint."} (mengonfirmasi service_role dipakai server-side)

## Dampak
1. PII seluruh user (email, nama, no_hp, balance) terbaca publik – pelanggaran UU PDP (UU
27/2022)
2. Data finansial (payments, credit_transactions) terbaca publik
3. Akses tulis (UPDATE/DELETE) memungkinkan manipulasi credits/balance/role – pencurian
layanan
4. Akun aktif tanpa verifikasi email – memudahkan abuse & pembuatan akun massal
5. Endpoint AI API memerlukan key (kontrol baik), tapi /v1/** terbuka (info disclosure
minor)

## Mapping
- CWE-639 (Authorization Bypass Through User-Controlled Key) / CWE-284 (Improper Access
Control)
- OWASP API1:2023 Broken Object Level Authorization
- OWASP A01:2025 Broken Access Control
- WSTG-ATHZ-02 (Testing for Bypassing Authorization Schema)
- UU PDP No. 27/2022 (perlindungan data pribadi)

```

Lampiran B — Probe dan recon historis lengkap

Semua nilai ini berasal dari file tersimpan; tidak ada request baru. Isi sitemap memang terpotong pada sumber.

B. api-probes.txt

```

=== API PROBES (***) ===
[signup] POST /api/** ** ->
{"success":true,"message":"Akun berhasil dibuat. Silakan verifikasi email
Anda.", "requiresVerification":true,"otpSent":true}
[**-rest] GET /rest/** anon ->
{"message":"Invalid API key","hint":"Only the service_role API key can be used for this

```

```

endpoint."}
[***] GET /api/** -> 200, channels VA/QRIS/e-wallet
[verify-otp] wrong OTP -> Invalid or expired verification code. 4 attempts remaining.
[resend-otp] -> success:true otpSent:true
[***.url] ***
[***-anon-jwt] [SHA256:***]

```

B. dns.txt

```

***.      119      IN      A      ***
***.      119      IN      A      ***
***.      120      IN      AAAA   2606:4700:3035::6815:7b8
***.      120      IN      AAAA   2606:4700:3032::ac43:892a
***.      85938   IN      NS     ***.
***.      85938   IN      NS     ***.
;; communications error to ***#53: timed out
***.      300      IN      MX     50 ***.
***.      300      IN      MX     10 ***.
***.      300      IN      MX     20 ***.
***.      300      IN      TXT    "v=spf1 include:*** ~all"
***.      300      IN      TXT
"zoho-verification=***"
***.      300      IN      TXT    "ca3-***"
***.      300      IN      TXT
"***-site-verification=Vz1PbPhd7YTykr9bnRaCqeVw0jhzctg0cEd9jY9XgfM"
***.      1800     IN      SOA     ***. ***.
2414231877 10000 2400 604800 1800

```

B. headers.txt

```

HTTP/2 200
date: Tue, *** 11:16:22 GMT
content-type: text/html; charset=utf-8
server: ***
vary: rsc, next-router-state-tree, next-router-prefetch, next-router-segment-prefetch,
Accept-Encoding
x-nextjs-cache: HIT
x-nextjs-prerender: 1
x-nextjs-prerender: 1
x-nextjs-stale-time: 300
x-powered-by: ***
cache-control: s-maxage=31536000
report-to:
{"group":"cf-nel","max_age":604800,"endpoints":[{"url":"***
nel: {"report_to":"cf-nel","success_fraction":0.0,"max_age":604800}
cf-cache-status: DYNAMIC
cf-ray: a3b738066e38897c-SIN
alt-svc: h3=":443"; ma=86400

```

B. robots.txt

```

User-Agent: *
Allow: /

Sitemap: ***

```

B. sitemap.txt

```

<?xml version="1.0" encoding="UTF-8"?>
<urlset xmlns="***>
<url>

```

```

<loc>***</loc>
<lastmod>***</lastmod>
<changefreq>daily</changefreq>
<priority>1</priority>
</url>
<url>
<loc>***</loc>
<lastmod>***</lastmod>
<changefreq>daily</changefreq>
<priority>0.9</priority>
</url>
<url>
<loc>***</loc>
<lastmod>***</lastmod>
<changefreq>monthly</changefreq>
<priority>0.8</priority>
</url>
<url>
<loc>***</loc>
<lastmod>***</lastmod>
<changefreq>monthly</changefreq>
<priority>0.8</priority>
</url>
<url>
<loc>***</loc>
<lastmod>***</lastmod>
<changefreq>mo

```

B. subdomains.txt

```

*** -> 200
*** -> 000
*** -> 000
*** -> 000
*** -> 000
*** -> 000
*** -> 000
*** -> 000
*** -> 000
*** -> 000
*** -> 000
*** -> 000
*** -> 000
*** -> 000
*** -> 000

```

B. wayback.txt

```
curl: (28) Operation timed out after 40001 milliseconds with 0 bytes received
```

Lampiran C — Manifest seluruh sumber

Daftar berasal dari evidence/source-manifest.json. Seluruh 15 hash dicocokkan dengan file asal. SHA-256 panjang ditampilkan utuh agar dapat dicari dan diverifikasi.

C.01 admin-panel-audit.md

- Ukuran: 4,951 byte.
- Mtime UTC: ***.
- SHA-256: ***.

- Sumber: ***-September-2026/evidence-***/admin-panel-audit.md.

C.02 api-probes.txt

- Ukuran: 827 byte.
- Mtime UTC: ***.
- SHA-256: ***.
- Sumber: ***-September-2026/evidence-***/api-probes.txt.

C.03 dns.txt

- Ukuran: 849 byte.
- Mtime UTC: ***.
- SHA-256: ***.
- Sumber: ***-September-2026/evidence-***/dns.txt.

C.04 headers.txt

- Ukuran: 769 byte.
- Mtime UTC: ***.
- SHA-256: ***.
- Sumber: ***-September-2026/evidence-***/headers.txt.

C.05 homepage.html

- Ukuran: 52,426 byte.
- Mtime UTC: ***.
- SHA-256: ***.
- Sumber: ***-September-2026/evidence-***/homepage.html.

C.06 js-dashboard.txt

- Ukuran: 25,057 byte.
- Mtime UTC: ***.
- SHA-256: ***.
- Sumber: ***-September-2026/evidence-***/js-dashboard.txt.

C.07 js-signup-page.js

- Ukuran: 8,329 byte.
- Mtime UTC: ***.
- SHA-256: ***.
- Sumber: ***-September-2026/evidence-***/js-signup-page.js.

C.08 js-*-client.txt**

- Ukuran: 144,356 byte.
- Mtime UTC: ***.
- SHA-256: ***.

- Sumber: ***-September-2026/evidence-***/js-***-client.txt.

C.09 js-verify-email.js

- Ukuran: 6,917 byte.
- Mtime UTC: ***.
- SHA-256: ***.
- Sumber: ***-September-2026/evidence-***/js-verify-email.js.

C.10 robots.txt

- Ukuran: 65 byte.
- Mtime UTC: ***.
- SHA-256: ***.
- Sumber: ***-September-2026/evidence-***/robots.txt.

C.11 security.txt

- Ukuran: 12,301 byte.
- Mtime UTC: ***.
- SHA-256: ***.
- Sumber: ***-September-2026/evidence-***/security.txt.

C.12 sitemap.txt

- Ukuran: 800 byte.
- Mtime UTC: ***.
- SHA-256: ***.
- Sumber: ***-September-2026/evidence-***/sitemap.txt.

C.13 subdomains.txt

- Ukuran: 342 byte.
- Mtime UTC: ***.
- SHA-256: ***.
- Sumber: ***-September-2026/evidence-***/subdomains.txt.

C.14 *-rls-audit.md**

- Ukuran: 4,143 byte.
- Mtime UTC: ***.
- SHA-256: ***.
- Sumber: ***-September-2026/evidence-***/***-rls-audit.md.

C.15 wayback.txt

- Ukuran: 78 byte.
- Mtime UTC: ***.
- SHA-256: ***.

- Sumber: `***-September-2026/evidence-***/wayback.txt`.

Lampiran D — Fingerprint kredensial

Sepuluh nilai unik ditemukan pada snapshot. Status aktif, expiry runtime, ownership, dan kemampuan penggunaan adalah Not verified. Fingerprint dibuat dari nilai persis di sumber, tanpa memberi akses ke target.

D.01 jwt

- Panjang historis: 208 karakter.
- SHA-256: `***`.
- Lokasi: `api-probes.txt`, `js-signup-page.js`, `***-rls-audit.md`.

D.02 user_api_key

- Panjang historis: 51 karakter.
- SHA-256: `***`.
- Lokasi: `admin-panel-audit.md`.

D.03 user_api_key

- Panjang historis: 51 karakter.
- SHA-256: `***`.
- Lokasi: `admin-panel-audit.md`.

D.04 user_api_key

- Panjang historis: 51 karakter.
- SHA-256: `***`.
- Lokasi: `admin-panel-audit.md`.

D.05 user_api_key

- Panjang historis: 51 karakter.
- SHA-256: `***`.
- Lokasi: `admin-panel-audit.md`.

D.06 user_api_key

- Panjang historis: 51 karakter.
- SHA-256: `***`.
- Lokasi: `admin-panel-audit.md`.

D.07 user_api_key

- Panjang historis: 51 karakter.
- SHA-256: `***`.
- Lokasi: `admin-panel-audit.md`.

D.08 user_api_key

- Panjang historis: 51 karakter.
- SHA-256: ***.
- Lokasi: admin-panel-audit.md.

D.09 user_api_key

- Panjang historis: 51 karakter.
- SHA-256: ***.
- Lokasi: admin-panel-audit.md.

D.10 bcrypt

- Panjang historis: 60 karakter.
- SHA-256: ***.
- Lokasi: admin-panel-audit.md.