CONFIDENTIAL

EGIDE

April 13, 2026

PENETRATION TEST REPORT

fullenrich.com

B2B Data Enrichment SaaS Platform

For FullEnrich

3 critical · 10 high · 5 medium · 0 low

SCOPE	STACK	METHODOLOGY
fullenrich.com	—	OWASP WSTG v4.2 · PTES

EGIDE.AI

Pentesting for startups, scale-ups & SMBs

TABLE OF CONTENTS

Contents

SECTION 1

Executive Summary

1.1 Confidentiality

This document is the exclusive property of FullEnrich and EGIDE. It contains proprietary and confidential information. Any duplication, redistribution, or use requires the written consent of FullEnrich.

1.2 Overview

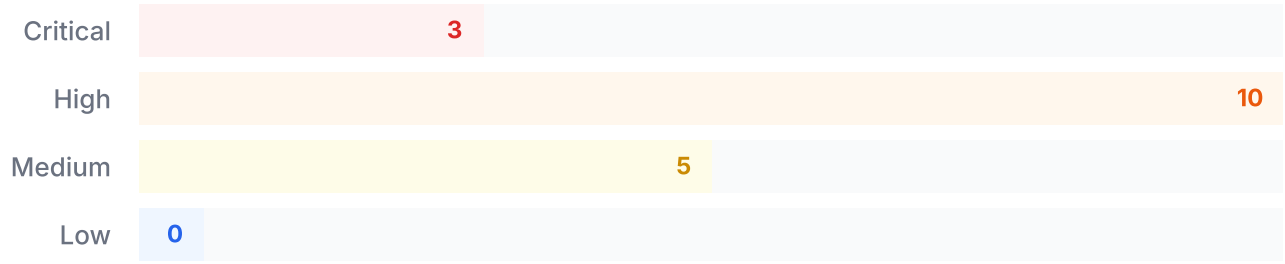
> AT A GLANCE
>
> EGIDE conducted a security assessment of fullenrich.com. The assessment identified 18 vulnerabilities, including 3 critical and 10 high severity. Overall risk level is assessed as —. Priority remediation is recommended for critical and high findings before any production deployment or additional exposure.

On April 13, 2026, EGIDE conducted an authorized penetration test on **fullenrich.com**. The assessment revealed **3 critical, 10 high, 5 medium and 0 low vulnerabilities**.

SECTION 2

Findings

2.1 Vulnerability Distribution



2.2 Summary Table

#	VULNERABILITY	SEVERITY	CVSS	STATUS
PT-1	Unauthenticated Tempo Trace Server — 7 Third-Party API Keys Leaked (5 Confirmed Valid)	CRITICAL	9.8	Unresolved
PT-2	Unauthenticated Tempo — PII Exposure (1,612 Emails + 74 Phone Numbers)	CRITICAL	9.1	Unresolved
PT-3	Unauthenticated Prometheus — Revenue, User Base, Provider Credits, Full Business Intelligence	CRITICAL	9.1	Unresolved
PT-4	Tempo /shutdown Endpoint Accessible — Production Monitoring Denial of Service	HIGH	8.6	Unresolved
PT-5	Unauthenticated OTLP Write Access — Trace/Log/Metric Injection on Production	HIGH	8.2	Unresolved
PT-6	Unauthenticated Loki Log Server — Application Logs with PII, Client Workspace IDs, Source Code Paths	HIGH	7.5	Unresolved

#	VULNERABILITY	SEVERITY	CVSS	STATUS
PT-7	Source Maps Publicly Accessible — Full Application Source Code Exposure	HIGH	7.5	Unresolved
PT-8	Cloudflare WAF Bypass via Direct DigitalOcean Origin	HIGH	7.5	Unresolved
PT-9	Internet-Exposed n8n Instance v1.66.0 — 57 Known CVEs (23 RCE)	HIGH	7.5	Unresolved
PT-10	DSAR Portal — Verification Token Leak + Do-Not-Sell Without Verification	HIGH	7.5	Unresolved
PT-11	Svelte 3.x + SvelteKit 1.x End-of-Life — 10 Unpatched CVEs	HIGH	7.5	Unresolved
PT-12	Grafana /metrics Unauthenticated — Full Infrastructure Intelligence Leak	HIGH	7.5	Unresolved
PT-13	Affiliate Portal — 971 Routes Exposed via Ziggy + CAPTCHA Bypass	HIGH	7.3	Unresolved
PT-14	Feature Bypass — Free User Can Enable Paid Personal Email Enrichment	MEDIUM	6.5	Unresolved
PT-15	Stripe Pricing Configuration Fully Exposed — 33 Production Price IDs	MEDIUM	5.3	Unresolved
PT-16	MCP Server — Open OAuth Client Registration + Wildcard CORS	MEDIUM	5.3	Unresolved
PT-17	Missing All Security Headers on Application	MEDIUM	5.3	Unresolved
PT-18	Go Backend Nil Pointer Dereference — Stack Trace Leaked to Client	MEDIUM	5.3	Unresolved

SECTION 2.3

Detailed Findings

CRITICAL PT-1

Unauthenticated Tempo Trace Server — 7 Third-Party API Keys Leaked (5 Confirmed Valid)

CVSS 9.8 · CWE CWE-200 · OWASP A01:2021 · Unresolved

AT A GLANCE

Your internal monitoring server (Tempo) is freely accessible on the internet with no password. Inside its recorded data, we found the access keys to 5 of your data providers — including Hunter.io with over one million credits. Anyone can use these keys to consume your provider credits, representing a direct financial cost of tens of thousands of euros.

DESCRIPTION

The Grafana Tempo distributed tracing server at 104.248.243.101:3200 (PROD) and 209.38.252.65:3200 (DEV) are accessible without any authentication. Trace data contains third-party API keys passed as URL query parameters. 7 keys extracted, 5 confirmed valid: - Hunter.io: `8352f60f916ddf7dde60a430eeb3165aa92a50c4` — 1,043,349 credits, enterprise plan (Data-platform Level 5), owner: Jean-Luc Manceron (jean-luc@fullenrich.com) - Scrapin.io: `sk_3a770fd51478fc35000ea7277d95e84428b70a06` — 37,430/100,000 credits - Datagma: `fb85a3c196ed` — active - EmailListVerify: `Sg8sStuA0WC7ELGkoVZP0` — active - Mixrank: `cd2277eb5fa9b17b26c59968e3f20fb8` — active - CaptainVerify: `alRIe6C0OPlU47kucIietmBdGf3h95e0` — expired - Listmint: `fb842183-d173-4909-9f75-8fbd832b5aee` — endpoint not found

IMPACT

Direct financial impact — attacker can consume provider credits (1M+ Hunter.io searches). Full LinkedIn enrichment, email verification, person matching available using FullEnrich's accounts. Provider relationships and spending exposed.

REMEDIATION

1. Block external access to port 3200 on both servers immediately
2. Rotate all 7 API keys at affected providers
3. Move Tempo behind VPN or Cloudflare Access
4. Pass API keys in HTTP headers instead of URL parameters

CRITICAL PT-2

Unauthenticated Tempo — PII Exposure (1,612 Emails + 74 Phone Numbers)

CVSS **9.1** · CWE **CWE-200** · OWASP **A01:2021** · Unresolved

AT A GLANCE

The same monitoring server exposes personal data of real people: 1,612 email addresses and 74 phone numbers (French, Belgian, Spanish, Italian, British). This data is visible to anyone on the internet. This constitutes a direct GDPR violation, with a potential fine of up to 4% of global annual revenue.

DESCRIPTION

The unauthenticated Tempo server exposes PII in trace URL attributes. CaptainVerify phone verification URLs contain real phone numbers. Hunter.io and other provider URLs contain email addresses being enriched. 1,612 unique email addresses and 74 phone numbers (FR +33, BE +32, ES +34, IT +39, UK +44) extracted. 384 HubSpot CRM link IDs reveal customer integration data.

IMPACT

GDPR violation — real PII of data subjects exposed without access controls. Potential fine up to 4% of global revenue. 384 customer HubSpot integrations also leaked.

REMEDIATION

1. Block port 3200 (same as PT-1)
2. Scrub PII from trace attributes before storage
3. Implement data retention policies on Tempo

CRITICAL PT-3

Unauthenticated Prometheus — Revenue, User Base, Provider Credits, Full Business Intelligence

CVSS 9.1 · CWE CWE-200 · OWASP A01:2021 · Unresolved

AT A GLANCE

Your metrics server (Prometheus) is freely accessible and exposes all your financial and business indicators: real-time revenue (~163,000 EUR/week), number of users (152,694), credit balances at your 22 data providers, traffic sources, and LinkedIn scraping capacity. A competitor could use this information to understand your entire business model.

DESCRIPTION

Prometheus at 104.248.243.101:9090 (PROD) and 209.38.252.65:9090 (DEV) fully accessible without authentication. 121 metrics, 65 days retention. Revenue: ~163,000 EUR/week (~23K/day). Users: 152,694 (growing ~750/day). 22 provider credit balances (Datagma: 81.7M, Enrow: 19.5M, Wiza: 10M, Prospeo: 5.5M, etc.). Traffic: API (374K), Clay (157K), n8n (11.7K), Make (1.4K). LinkedIn capacity: 75,056. 5 internal service instances. Remote-write receiver enabled (metric injection possible).

IMPACT

Full business intelligence exposure. Competitor can understand exact revenue, growth rate, provider stack, credit spending, and capacity.

REMEDIATION

1. Block external access to port 9090
2. Disable remote-write receiver or add authentication
3. Move behind VPN
4. Configure alert rules

HIGH PT-4

Tempo /shutdown Endpoint Accessible — Production Monitoring Denial of Service

CVSS 8.6 · CWE CWE-284 · Unresolved

AT A GLANCE

Your trace server has a shutdown button accessible to anyone on the internet. An attacker could turn off your monitoring with a single request, making you blind to technical problems and security incidents.

DESCRIPTION

Tempo at 104.248.243.101:3200 exposes /shutdown (would stop the service) and /flush (confirmed accessible, returns 204) without authentication.

IMPACT

Denial of service on production monitoring. Attacker could blind the operations team during an attack.

REMEDIATION

1. Block port 3200 from external access
2. Disable admin endpoints or require authentication

HIGH PT-5

Unauthenticated OTLP Write Access — Trace/Log/Metric Injection on Production

CVSS 8.2 · CWE CWE-284 · Unresolved

AT A GLANCE

Your monitoring data collectors accept data from anyone without verification. An attacker can inject fake data into your dashboards: fake revenue, fake error logs, fake alerts. This can mask a real attack or trigger false emergencies for your technical team.

DESCRIPTION

OTLP HTTP (4318) and gRPC (4317) receivers on PROD (104.248.243.101) and DEV (209.38.252.65) accept arbitrary trace, metric, and log data without authentication. PoC trace injected successfully (HTTP 200). Prometheus remote-write receiver also enabled.

IMPACT

Observability poisoning, alert manipulation, log forging, cost amplification.

REMEDIATION

1. Add authentication to OTLP receivers
2. Block ports 4317/4318 externally
3. Disable Prometheus remote-write receiver

HIGH PT-6

Unauthenticated Loki Log Server — Application Logs with PII, Client Workspace IDs, Source Code Paths

CVSS 7.5 · CWE CWE-200 · Unresolved

AT A GLANCE

Your application log server is accessible without a password and contains logs with user email addresses, client IP addresses, identifiers of 15 real customer workspaces, and complete database queries. An attacker can understand exactly how your application works by reading these logs.

DESCRIPTION

Loki at 104.248.243.101:3100 (PROD, v3.6.0) and 209.38.252.65:3100 (DEV, v2.9.9) accessible without auth. Contains: 6 user emails (including admin@fullenrich.com), client IPs, 15 customer workspace IDs, complete OpenSearch queries (DB schema), Go source code paths, password reset events, billing transitions, 32 gRPC endpoints.

IMPACT

Application architecture exposed. Customer workspace IDs leaked. Database schema reverse-engineered. Source code structure revealed.

REMEDIATION

1. Block external access to port 3100
2. Move behind VPN
3. Sanitize logs to remove PII

HIGH PT-7

Source Maps Publicly Accessible — Full Application Source Code Exposure

CVSS 7.5 · CWE CWE-540 · Unresolved

AT A GLANCE

Your web application's development files are accessible to everyone. They contain your complete source code, including the list of all 90 internal functions, an internal developer package name, and the full structure of your API. It's like leaving the architectural blueprints of a vault in plain sight.

DESCRIPTION

All .js.map source map files publicly accessible on app.fullenrich.com. Exposes: 90+ gRPC method definitions across 8 services, internal npm package @aymeric_henry_sr/svelte-proto, full protobuf field structures, admin-only methods (AddPack, RefundPack, UpdateCost, AdminBulkLocalRegister).

IMPACT

Complete API surface exposed. Targeted attacks against all gRPC endpoints possible. Internal developer identity revealed.

REMEDIATION

1. Disable source maps in production: config.kit.vite.build.sourcemap = false
2. Add Cloudflare rule to block *.map files

HIGH PT-8

Cloudflare WAF Bypass via Direct DigitalOcean Origin

CVSS 7.5 · CWE CWE-16 · Unresolved

AT A GLANCE

Your Cloudflare web firewall protection can be completely bypassed by accessing your DigitalOcean hosting server directly. All security rules, DDoS protection, and bot blocking become ineffective.

DESCRIPTION

The DigitalOcean origin server is directly accessible at oyster-app-eic6h.ondigitalocean.app, bypassing all Cloudflare WAF protection. x-do-app-origin header (05ac75ab-2baf-4d2b-8ec8-f357a59736a0) leaked on every response.

IMPACT

All Cloudflare WAF rules, rate limiting, bot management, and DDoS protection bypassed.

REMEDIATION

1. Restrict DigitalOcean to only accept Cloudflare IPs
2. Remove x-do-app-origin header
3. Use Cloudflare Tunnel

HIGH PT-9

Internet-Exposed n8n Instance v1.66.0 — 57 Known CVEs (23 RCE)

CVSS 7.5 · CWE CWE-1104 · Unresolved

AT A GLANCE

Your internal automation tool (n8n) is accessible from the internet and uses a one-year-old version with 57 known security flaws, 23 of which allow executing malicious code on your server. If an attacker finds the password (there's no protection against repeated attempts), they get complete access to your server and all data passing through it.

DESCRIPTION

n8n v1.66.0 at n8n-growth.fullenrich.com (206.81.24.211:5678). Docker, SQLite, NodeJS 20.18.0. Settings leaked via /rest/settings without auth. Swagger UI at /api/v1/docs/. 568 nodes, 383 credential types. Custom nodes: fullenrich + HeyReach (LinkedIn automation). Ubuntu 24.04 LTS.

IMPACT

Any authenticated user can execute arbitrary OS commands via 23 RCE CVEs. Settings exposure reveals infrastructure.

REMEDIATION

1. Remove from public internet — place behind VPN
2. Upgrade to n8n 2.13.3+
3. Rotate all credentials stored in n8n
4. Add rate limiting on login

HIGH PT-10

DSAR Portal — Verification Token Leak + Do-Not-Sell Without Verification

CVSS 7.5 · CWE CWE-200 · Unresolved

AT A GLANCE

Your GDPR privacy rights portal has two serious flaws: the email and SMS verification codes are visible directly in the web page source code, and 'do not sell my data' requests require no identity verification at all. An attacker could submit data deletion requests for any person in your database.

DESCRIPTION

DSAR portal at dsar.fullenrich.com leaks email_token (SHA-256) and sms_token (6-digit) in Next.js RSC flight payload on status pages. Do-not-sell requests skip ALL verification (requiresVerification: false). Admin panel at /admin renders without server-side auth. No rate limiting on /api/admin/auth (12,700 attempts, zero blocks). Rate limit bypass via X-Forwarded-For.

IMPACT

Mass data suppression via do-not-sell. Verification bypass for data access/deletion requests. Admin brute-forceable.

REMEDIATION

1. Strip sensitive fields from RSC payload
2. Require verification for do-not-sell
3. Add server-side auth on /admin
4. Implement rate limiting on /api/admin/auth
5. Use CF-Connecting-IP instead of X-Forwarded-For

HIGH PT-11

Svelte 3.x + SvelteKit 1.x End-of-Life — 10 Unpatched CVEs

CVSS 7.5 · CWE CWE-1104 · Unresolved

AT A GLANCE

Your web application uses framework versions (Svelte and SvelteKit) that no longer receive security updates. Ten known flaws have no fix available for these versions, including risks of session theft and request forgery.

DESCRIPTION

Application runs Svelte 3.x (EOL) and SvelteKit 1.x (EOL). 10 CVEs: CVE-2024-45047 (mXSS), CVE-2026-27125/27121/27122 (SSR XSS), CVE-2023-29003/29008 (CSRF), CVE-2024-53262 (error page XSS), CVE-2024-23641 (DoS). SSR confirmed.

IMPACT

Multiple XSS vectors through framework vulnerabilities. No security patches available.

REMEDIATION

1. Migrate to Svelte 5.x + SvelteKit 2.x
2. Implement automated dependency scanning

HIGH PT-12

Grafana /metrics Unauthenticated — Full Infrastructure Intelligence Leak

CVSS 7.5 · CWE CWE-200 · Unresolved

AT A GLANCE

The metrics pages of both your Grafana instances (production and development) are accessible without login. They reveal the number of users (9), connected database types, internal data sources, and the fact that all your email alerts fail (17,483 failures). An attacker knows exactly what you're monitoring and how.

DESCRIPTION

Both Grafana instances (PROD v12.2.1, DEV v11.1.0) expose /metrics without auth. Leaks: 9 users (7 admins), 3 service accounts, 9 dashboards, 12 alert rules, 7 datasources, 17,483 failed email alerts (100% failure rate), Google OAuth client ID.

IMPACT

Full infrastructure intelligence. Attacker knows monitoring stack, user count, alert configuration, and that email alerting is broken.

REMEDIATION

1. Add authentication to /metrics
2. Fix email alerting
3. Move Grafana behind VPN

HIGH PT-13

Affiliate Portal — 971 Routes Exposed via Ziggy + CAPTCHA Bypass

CVSS 7.3 · CWE CWE-200 · Unresolved

AT A GLANCE

Your affiliate platform exposes a complete map of its 971 internal pages in every page's source code, including admin panels, queue management tools, and account takeover mechanisms. Additionally, the anti-bot system (CAPTCHA) is never verified server-side, allowing scripts to create affiliate accounts en masse.

DESCRIPTION

Partnero affiliate platform at affiliate.fullenrich.com embeds 971 Ziggy routes in client JS: Nova admin (23), Horizon (22), Laravel Passport OAuth (15), 4 impersonation mechanisms, internal APIs, webhook secrets. Turnstile CAPTCHA not validated server-side — mass registration confirmed.

IMPACT

Complete application blueprint exposed. Mass bot registration possible. Impersonation endpoints revealed.

REMEDIATION

1. Remove Ziggy routes from client JS or filter to public only
2. Validate Turnstile server-side
3. Disable unused impersonation endpoints

MEDIUM PT-14

Feature Bypass — Free User Can Enable Paid Personal Email Enrichment

CVSS 6.5 · CWE CWE-284 · Unresolved

AT A GLANCE

A user on the free plan can activate a feature normally reserved for paid subscriptions (personal email enrichment) by sending a direct command to the server. The server does not check the subscription level before accepting the request.

DESCRIPTION

workspace.Workspaces/UpdatePersonalEmailActivation gRPC endpoint allows any authenticated user to enable Personal Email Enrichment without subscription validation. Confirmed: grpc-status 0 (OK) for free-plan account.

IMPACT

Revenue loss — paid feature accessible without subscription.

REMEDIATION

1 Add subscription validation before enabling premium features

MEDIUM PT-15

Stripe Pricing Configuration Fully Exposed — 33 Production Price IDs

CVSS 5.3 · CWE CWE-200 · Unresolved

AT A GLANCE

Your entire Stripe pricing grid is visible in your website's source code: 33 production price identifiers, old identifiers from a previous Stripe account, and test identifiers. A competitor can see exactly your prices, margins, and plans.

DESCRIPTION

billing.constants.js exposes 33 production Stripe price IDs, 11 old/legacy price IDs (account BpGJAH1B75), staging/dev price IDs, two Stripe account IDs, Sales Navigator tier limits (Free=50, Limited=2000, Unlimited=2500).

IMPACT

Full pricing intelligence. Two Stripe accounts visible. Business intelligence leakage.

REMEDIATION

1. Move pricing configuration to server-side
2. Deactivate old Stripe price IDs

MEDIUM PT-16

MCP Server — Open OAuth Client Registration + Wildcard CORS

CVSS 5.3 · CWE CWE-942 · Unresolved

AT A GLANCE

Your AI integration server (MCP) allows anyone to register a third-party application and accepts requests from any website. Combined with a phishing attack, an attacker could gain access to enrichment tools on behalf of a legitimate user.

DESCRIPTION

mcp.fullenrich.com has Access-Control-Allow-Origin: * and /register accepts unauthenticated dynamic OAuth client registration. Full OAuth flow completed, MCP token obtained with search/enrich capabilities.

IMPACT

OAuth phishing vector. Attacker can register malicious OAuth client and trick users into granting access.

REMEDIATION

1. Replace wildcard CORS with specific origins
2. Restrict dynamic client registration
3. Implement redirect_uri validation

MEDIUM PT-17

Missing All Security Headers on Application

CVSS 5.3 · CWE CWE-693 · Unresolved

AT A GLANCE

Your application does not implement any of the standard browser security protections recommended by security standards: no content security policy, no framing protection, no HTTPS enforcement. This makes certain attacks like content injection or clickjacking easier.

DESCRIPTION

app.fullenrich.com missing: Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Strict-Transport-Security, Referrer-Policy, Permissions-Policy.

IMPACT

Clickjacking, MIME confusion, SSL stripping, referrer leakage all possible.

REMEDIATION

1 Add all security headers via Cloudflare transform rules

MEDIUM PT-18

Go Backend Nil Pointer Dereference — Stack Trace Leaked to Client

CVSS **5.3** · CWE **CWE-476** · Unresolved

AT A GLANCE

Certain commands sent to your server cause an internal crash whose technical error message is returned directly to the user. These messages confirm your server technology and reveal a lack of input validation.

DESCRIPTION

Several gRPC endpoints crash with Go runtime nil pointer dereference on empty protobuf payloads. Full error 'runtime error: invalid memory address or nil pointer dereference' returned to client. Affected: enrichment.Enrichments/CreateOne, workspace.Workspaces/Update, workspace.Workspaces/UpdateConfig.

IMPACT

Information disclosure — confirms Go backend, reveals missing input validation. Potential DoS.

REMEDIATION

1. Add nil checks on deserialized protobuf fields
2. Implement gRPC interceptors with recover()

APPENDIX A

Scope & Methodology

The assessment combined automated security analysis with penetration testing methodologies aligned with industry standards.

OWASP WSTG v4.2

Comprehensive coverage of web application vulnerabilities per the Web Security Testing Guide.

PTES

Structured framework covering the complete penetration testing lifecycle.

Test Types

	BLACK BOX	GREY BOX	WHITE BOX
Objective	Simulate an external attacker	Test with partial access	Full audit, total access
Realism	Maximum	Balanced	Maximum coverage

APPENDIX B

Glossary

CVSS	Common Vulnerability Scoring System — standardized vulnerability severity scoring (0 to 10).
CWE	Common Weakness Enumeration — catalog of software weakness types.
IDOR	Insecure Direct Object Reference — unauthorized access to resources by tampering with identifiers.
SSRF	Server-Side Request Forgery — abusing the server to reach internal resources.

GDPR	General Data Protection Regulation — European framework, fines up to €20M or 4% of turnover.
JWT	JSON Web Token — standard for securely transmitting information as a signed token.