SAMPLE · FICTIONALIZED FROM REAL SCAN PATTERNS · NOT A REAL COMPANY, NOT A RESULT FOR YOUR DOMAIN

Luxero FREE REPORT · REDACTED

EXPOSURE REPORT · TIER 1 PUBLIC-SURFACE CHECK

WHAT MERIDIANSHORE.EXAMPLE IS LEAKING RIGHT NOW

F

EXPOSURE GRADE

Exposure score **84/100** · 80+ means act now

One live leak of customer identity data, one producer-book leak, and a public map of every sensitive field in your core system.

1 Critical | **1** High | **4** Medium | **3** Low | **1** Info

COMPANY	DOMAIN	SCAN DATE	SENT ONLY TO
Meridian Shore (fictional)	meridianshore.example	2 Dec 2026	dana.r@meridianshore.example

FOR LEADERSHIP · 1-MINUTE READ

WHAT THIS MEANS FOR YOUR BUSINESS

Your site is handing out customer identity data right now. A leftover data-migration tool answers anyone who asks, and returns insured customers' names, dates of birth and Social Security numbers. No password, no hacking — just a normal request.

Two more things stand out: your public agent finder ships your producers' commission tiers, CRM IDs and personal phone numbers, and your core system publishes a map of every sensitive field it holds.

In plain terms: if a reporter, competitor or plaintiff's lawyer found this before you, it would read as "agency leaks 48,000 customers' SSNs." That's why we flag it first, and include the fix for the critical item for free.

Top 3 to fix first

1. **Lock the migration tool** (Critical) — customer SSNs and DOBs readable.
2. **Trim the agent-finder data** (High) — CRM and personal agent data.
3. **Gate the public data model** (Medium) — map of every sensitive field.

Who's affected

Insured customers of your agencies · your producers · anyone emailed "from" your domain.

Because you ticked "Call, text or email me if you find something critical," Luxero's automated assistant called the number you gave on 2 Dec 2026 at 10:14 (America/New_York) and followed up by email. It never asks for passwords or payment.

FOR YOUR TECHNICAL TEAM

The technical picture. Hostnames, paths and record values are redacted in this free report. Field names are shown in full, because anyone can read them today.

WHAT WE LOOKED AT

SCAN COVERAGE

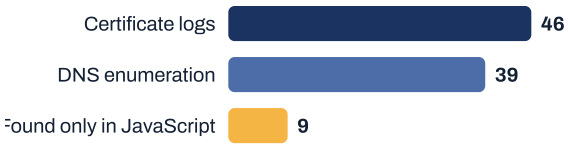
Every number below is something we actually reached, read or checked during this scan — so you can see how much ground a stranger can cover without a login.

94 Hostnames discovered	**58** Live hosts probed	**19** Third-party / vendor hosts followed	**41** JavaScript bundles read	**1,486** Endpoints & paths checked
6 API specs / data models found	**7,212** Requests sent (read-only, throttled)	**24** Business surfaces walked (forms, portals, locators)	**37** DNS / email-auth records checked	**61** TLS certificates checked

From names to findings



Where we found your hostnames



9 hosts appeared **only** inside your website's JavaScript. Certificate logs alone would have missed them — including the host behind the critical finding.

TECHNOLOGY WE DETECTED

YOUR PUBLIC STACK

22 technologies fingerprinted from headers, DNS, certificates and page code. Each one is a place data can be handed out — or a place a leak hides.

CF **Cloudflare** CDN / WAF	Hs **HubSpot CMS** Website / CMS	Az **Microsoft Azure** Hosting
λ **AWS Lambda** Hosting	▲ **Vercel** Hosting	.N **ASP.NET Core / Kestrel** API framework

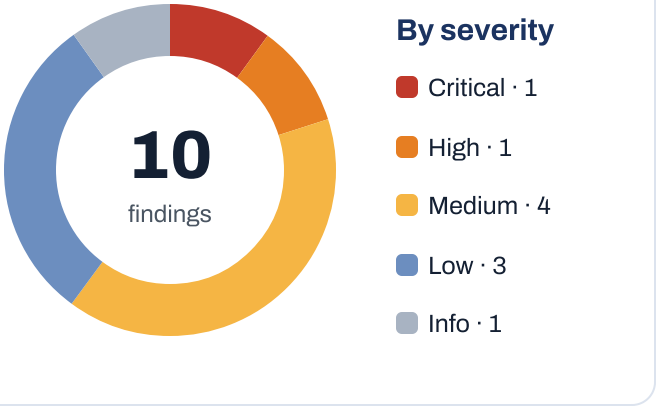
OData v4 API protocol	**Python FastAPI** API framework	**nginx 1.24** Web server
Auth0 Identity / SSO	**Microsoft Entra ID** Identity / SSO	**Grafana 12.1** Monitoring
Stoplight API docs	**Lovable** No-code / vibe-coded	**Bubble** No-code / vibe-coded
ElevenLabs widget Third-party widget	**Google Tag Manager** Analytics	**Google Workspace** Email
Zoho Mail Email	**Let's Encrypt** Certificates	**Discourse** Community
MCP server (SQL tools) AI tooling		

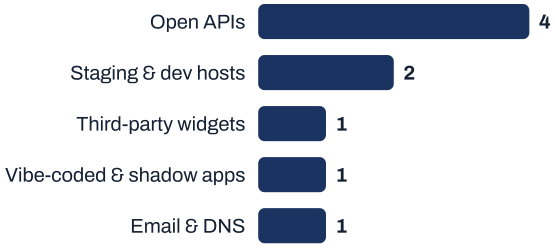
Marks are simplified monograms for identification only. Names belong to their owners; detection does not mean the product is misconfigured.

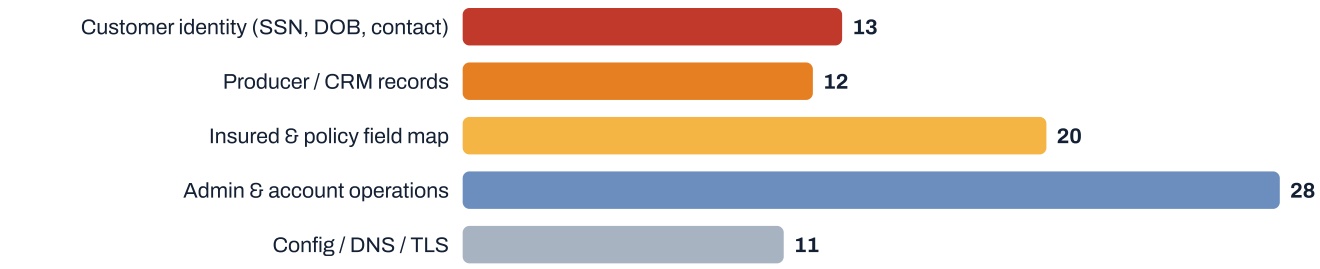
AT A GLANCE

FINDINGS IN CHARTS

10 confirmed findings, 84 distinct exposed field or route names.







SAMPLE · FICTIONALIZED FROM REAL PATTERNS

FINDINGS

ALL 10 FINDINGS · EVERY FIELD NAME

Values are masked (•••). Tap a finding to expand it. Field-map findings list names only — we read no values there.

CRITICAL **F-01 · Data-migration tool returns live customer records with no login** Unintended Live records -

Customer identity (SSN, DOB, contact) · 48,210 customer records in one database; 9 agency databases listed

A stranger can read your agencies' insured customers — names, dates of birth, Social Security numbers and contact details — from a leftover migration tool. No password, no key.

Where	[redacted].meridianshore.example · [redacted] (exact path in full report)
Data type	Customer identity (SSN, DOB, contact)
Scale	48,210 customer records in one database; 9 agency databases listed
Login required	No
Meant to be public	No

EVERY EXPOSED FIELD NAME (13)

FIELD NAME (AS RETURNED)	EXAMPLE VALUE
CustNo	1235•
FirstName	J•••
LastName	L•••
City	S••••••
State	FL
DateOfBirth	19••-••-08
SSN	•••-••-8434
Email	j•••@yahoo.com
Phone	(•••) •••-2777
DriversLicenseNo	L•••••••••••••-0
BankAccountNo	••••••4410
TaxId (FEIN)	••-••••1207
AgencyPortalPassword	[hash] ••••

Why it matters: Identity data for insured customers is readable from the open internet. For a licensed agency this is a notifiable-breach scenario in most states.

> **Fix today (free, so you can act now):** Put /mcp behind the same token as /api today, then rotate any database credentials the tool holds. Treat every database behind it as exposed until logs say otherwise.

HIGH **F-02 · Find-an-agent locator hands out CRM fields the page never shows** Unintended

Live records

Agent / producer records (CRM) · 1,734 producer records returned in one request (UI shows 10 at a time)

Your public agent finder shows a name and phone. The data behind it also carries internal CRM IDs, commission tiers, suspension flags and agents' personal mobile numbers and home addresses.

Where	[redacted].meridianshore.example · [redacted] (exact path in full report)
Data type	Agent / producer records (CRM)
Scale	1,734 producer records returned in one request (UI shows 10 at a time)
Login required	No
Meant to be public	No

EVERY EXPOSED FIELD NAME (12)

FIELD NAME (AS RETURNED)	EXAMPLE VALUE
crm_account_id	0015•••••••QA2
producer_npn	•••••219
commission_tier	[present]
max_invoiced_amount	$••,•••
is_suspended	[true/false]
appointment_status	[present]
carrier_appointments	[list, 6]
book_size_band	[present]
personal_mobile	(•••) •••-0142
home_address	••• W ••••• St, Tampa
hidden_from_ui	[true/false]
last_audit_note	[text, 1 line]

Why it matters: Competitors can lift your full producer book with commission tiers; agents' home addresses are personal data you hold in trust.

Exact location, evidence and step-by-step fix are in the full report.

MEDIUM **F-03 · Public API data model lists every insured, policy and commission field** Unintended

Field map · no values read

Field map only (no values read) · 106 entity types / 104 entity sets; 301 KB model

Anyone can download the complete map of the system that runs your business — every field name for insureds, policies, receipts and commissions. The records themselves are still locked.

Where	[redacted].meridianshore.example · [redacted] (exact path in full report)
Data type	Field map only (no values read)
Scale	106 entity types / 104 entity sets; 301 KB model
Login required	No
Meant to be public	No

EVERY EXPOSED FIELD NAME (20)

FIELD / ROUTE NAME (AS PUBLISHED)	TYPE	VALUE READ?
InsuredDetail.dateOfBirth	date	No — name only
InsuredDetail.ssn	string	No — name only
InsuredDetail.fein	string	No — name only
InsuredDetail.medicareHICN	string	No — name only
InsuredDetail.customerId	guid	No — name only
InsuredDetail.naics	string	No — name only
PolicyDetail.totalPremium	decimal	No — name only
PolicyDetail.totalAgencyCommission	decimal	No — name only
PolicyDetail.carrierFEIN	string	No — name only
PolicyDetail.carrierNAIC	string	No — name only
PolicyDetail.reasonForCancellation	string	No — name only
Receipts.totalFinancedAmount	decimal	No — name only
Receipts.paymentMethod	string	No — name only
Receipts.financingDetails	string	No — name only
Driver.ssn	string	No — name only
Driver.licenseNumber	string	No — name only
Driver.driverViolations	collection	No — name only
Agent.npnNumber	string	No — name only
Agent.email	string	No — name only
CommissionDetail.commissionValue	decimal	No — name only

No values were read. We list every field name because anyone can see them today, without your API documentation.

Why it matters: Graded medium because no values were read. But a stranger no longer needs your API documentation: they know exactly which fields hold SSNs and commissions, which shortens any attack to finding one open door (see F-01).

Exact location, evidence and step-by-step fix are in the full report.

MEDIUM **F-04 · Internal operations-portal backend is reachable and self-describing** Unintended

Field map · no values read

SAMPLE · FICTIONALIZED FROM REAL PATTERNS

Admin route names (no values read) · 13 admin routes, all 401

An internal admin back end that isn't listed anywhere answers from the internet and names its own admin functions.

Where	[redacted].meridianshore.example · [redacted] (exact path in full report)
Data type	Admin route names (no values read)
Scale	13 admin routes, all 401
Login required	No
Meant to be public	No

EVERY EXPOSED FIELD NAME (11)

FIELD / ROUTE NAME (AS PUBLISHED)	TYPE	VALUE READ?
/api/admin/users	route	No — name only
/api/admin/settings	route	No — name only
/api/audit/actions	route	No — name only
/api/servers	route	No — name only
/api/servers/rescan	route	No — name only
/api/vaults/refresh	route	No — name only
/api/provision	route	No — name only
/api/provision/domains	route	No — name only
/api/provision/reserve	route	No — name only
/api/dashboard	route	No — name only
/api/me	route	No — name only

No values were read. We list every field name because anyone can see them today, without your API documentation.

Why it matters: Whoever obtains one token reaches user administration and the secrets vault from anywhere.

Exact location, evidence and step-by-step fix are in the full report.

MEDIUM **F-05 · Login service publishes its full contract, including an impersonate operation** Unintended

Field map · no values read

Account operations & schemas (no values read) · 38 operations, 5 schemas

Your sign-in service publishes how every account action works — including a feature that lets one user act as another.

Where	[redacted].meridianshore.example · [redacted] (exact path in full report)
Data type	Account operations & schemas (no values read)
Scale	38 operations, 5 schemas
Login required	No
Meant to be public	No

EVERY EXPOSED FIELD NAME (9)

FIELD / ROUTE NAME (AS PUBLISHED)	TYPE	VALUE READ?

SAMPLE · FICTIONALIZED FROM REAL PATTERNS

/impersonate	operation	No — name only
/api/Account/loginwithsecretkey	operation	No — name only
/api/Account/adminlogin	operation	No — name only
/api/Account/registeruser	operation	No — name only
/api/Account/agencyonboarding	operation	No — name only
/api/Account/ssotoken	operation	No — name only
/api/Account/validatetoken	operation	No — name only
UserModel{email, phone, role, agencyId}	schema	No — name only
SecretModel{apiKey, secretKey}	schema	No — name only

No values were read. We list every field name because anyone can see them today, without your API documentation.

Why it matters: Structure only, but it names the exact operations an attacker would target first.

Exact location, evidence and step-by-step fix are in the full report.

MEDIUM **F-06 · AI assistant service lists 49 operations, including an admin SQL runner** Unintended -

Field map · no values read

Operation names (no values read) · 49 operations

An AI tool built for staff publishes its full list of functions, including 'run SQL against the app database' and commission forecasts.

Where	[redacted].meridianshore.example · [redacted] (exact path in full report)
Data type	Operation names (no values read)
Scale	49 operations
Login required	No
Meant to be public	No

EVERY EXPOSED FIELD NAME (8)

FIELD / ROUTE NAME (AS PUBLISHED)	TYPE	VALUE READ?
/api/admin/sql	operation	No — name only
/api/admin/schema	operation	No — name only
/api/commission-report/30-day-forecast	operation	No — name only
/api/commission-report/90-day-forecast	operation	No — name only
/api/commission-report/ar-aging	operation	No — name only
/api/commission-report/trailing-12m	operation	No — name only
/api/data-quality-report	operation	No — name only
/api/insured-graph/build	operation	No — name only

No values were read. We list every field name because anyone can see them today, without your API documentation.

Why it matters: The money view of the business is visible in the blueprint.

SAMPLE · FICTIONALIZED FROM REAL PATTERNS

Exact location, evidence and step-by-step fix are in the full report.

LOW **F-07 · Health checks name internal services and a 31-tool inventory** Unintended

Field map · no values read

Service names · 4 hosts

-

Small status pages reveal internal service names — and the tool list that pointed us to F-01.

Where	4 hosts · [redacted] (exact path in full report)
Data type	Service names
Scale	4 hosts
Login required	No
Meant to be public	No

EVERY EXPOSED FIELD NAME (4)

FIELD / ROUTE NAME (AS PUBLISHED)	TYPE	VALUE READ?
service	string	No — name only
tools[]	list (31)	No — name only
tool_count	int	No — name only
connections	int	No — name only

No values were read. We list every field name because anyone can see them today, without your API documentation.

Why it matters: Free reconnaissance.

Exact location, evidence and step-by-step fix are in the full report.

LOW **F-08 · DMARC is monitor-only (p=none)** Unintended Field map · no values read

DNS record · 1 record

-

Someone can send email that looks like it's from you, and your domain policy won't stop it.

Where	meridianshore.example · [redacted] (exact path in full report)
Data type	DNS record
Scale	1 record
Login required	No
Meant to be public	No

EVERY EXPOSED FIELD NAME (4)

FIELD / ROUTE NAME (AS PUBLISHED)	TYPE	VALUE READ?
v	DMARC1	No — name only
p	none	No — name only
rua	(absent)	No — name only
SPF	-all (strict)	No — name only

No values were read. We list every field name because anyone can see them today, without your API documentation.

Why it matters: Phishing aimed at your agents and customers.

Exact location, evidence and step-by-step fix are in the full report.

LOW **F-09 · Expired certificate and two mis-bound portal domains** Unintended

Field map · no values read

Config · 3 hosts

-

Three customer-facing names show browser warnings or errors.

Where	3 hosts · [redacted] (exact path in full report)
Data type	Config
Scale	3 hosts
Login required	No
Meant to be public	No

EVERY EXPOSED FIELD NAME (3)

FIELD / ROUTE NAME (AS PUBLISHED)	TYPE	VALUE READ?
cert notAfter	expired 11 Aug 2026	No — name only
SAN mismatch	2 hosts	No — name only
edge error	1034	No — name only

No values were read. We list every field name because anyone can see them today, without your API documentation.

Why it matters: Trust and availability, not data.

Exact location, evidence and step-by-step fix are in the full report.

INFO **F-10 · Public agent directory (by design)** Intended Field map · no values read

Display fields · —

-

Agent names and office phones on your Find-an-Agent page. Public by design; no action needed.

Where	[redacted].meridianshore.example · [redacted] (exact path in full report)
Data type	Display fields
Scale	—
Login required	No
Meant to be public	Yes

EVERY EXPOSED FIELD NAME (3)

FIELD / ROUTE NAME (AS PUBLISHED)	TYPE	VALUE READ?
display_name	string	No — name only
office_phone	string	No — name only
city	string	No — name only

No values were read. We list every field name because anyone can see them today, without your API documentation.

Why it matters: None.

Exact location, evidence and step-by-step fix are in the full report.

YOUR NEXT STEP

SEE EXACTLY WHERE — AND FIX IT BEFORE SOMEONE ELSE FINDS IT

The full report names every host and path, shows the evidence, and gives your team a step-by-step fix plan, plus a 30-minute walkthrough with a Luxero analyst. Monitoring re-checks every month and emails you what's new, fixed or still open.

Full report delivered in about 5 business days. No login, no dashboard — it comes by email, to you only.

Start monitoring — full report included free

$12,000/year, billed annually (2 months free) · renews yearly until cancelled · cancel online

Just the full report — $2,900

Upgrade to monitoring within 30 days and the $2,900 is credited (first year $9,100).

Your price

Full report (one-time, includes a 30-minute walkthrough)	**$2,900**
Monitoring, full report included	**$12,000/year**

Bought the full report first? Its price is credited toward a year of monitoring if you upgrade within 30 days.

Confirm these signals (free, optional). Four findings are a field map with the rows locked. With your written authorization, a Tier 2 check confirms whether real records sit behind them — read-only, capped at 5 masked example records per finding, reviewed by a person before it runs. Your first confirmation sample is free. **Authorize a Tier 2 check →**

Prices are per company, in USD, before tax. Link valid 30 days from 2 Dec 2026; ask for a fresh link anytime from the same email address. Terms: luxero.io/terms · Paid services terms · DPA (draft, pending counsel review).

HOW TO CHECK A FIX YOURSELF

After you change something, request the same URL from a browser in a private window, or with `curl`. You should see 401 (login required) or 404 (gone). We don't re-scan for free within 12 months; a paid report includes one re-check within 30 days.

SAMPLE · fictionalized from real patterns. Company, hostnames, people and values are invented; "meridianshore.example" uses a reserved test domain. Read-only check of what any visitor can already reach. Confidential to the verified recipient; do not forward outside your organization. Product names and marks shown in "Technology we detected" belong to their owners and identify detected technology only; no affiliation or endorsement is implied. Not legal advice.