

Security Sweep — snowit.ba (MC #107296)

Security Sweep — snowit.ba (MC #107296)

Date: 2026-08-17

Tenant: SnowIT-BA (operated, not owned by ALAI)

Repository: snowitba/snowit-site — **PRIVATE**

Production merge: c9d6724738b994264cab057b9093fc4b825480db

Pull request: snowitba/snowit-site#2

Trigger

A domain-specific sweep was ordered using the same gated principle as alai.no. The read-only baseline proved that the Vercel root deployment publicly served `CLAUDE.md`, `BUILD-BLUEPRINT.md`, and `DEPLOY-MAP.md`, while the public GitHub repository exposed the same operational history.

Confirmed baseline

- GitHub repository public with zero forks.
- Three internal Markdown files returned exact source content from production.
- Eight tenant-local secret findings: one expired Vercel OIDC token plus active ignored Terraform variables/state.
- Eight high production dependency advisories.
- Forty-four initial Semgrep findings, including IMDSv1, Host-header, h2c upgrade, API validation/CORS/HTML sinks, and XML parsing.
- Canonical tenant checkout was six commits behind with unrelated tracked/untracked work; it was preserved untouched.

Remediation

Repository and deployment

- Made the repository private; anonymous raw access now returns 404.
- Removed tracked `CLAUDE.md` and `.claude/**` from current source.
- Expanded `.vercelignore` to exclude agent metadata, internal docs, infrastructure, scripts, state, backups, tests and evidence.
- Added deterministic deploy preflight, sensitive-path tombstones, real 404 page, global CSP/HSTS/browser headers, SHA-pinned security CI and Dependabot.
- Vercel local build proved sensitive files absent from static output.

Public APIs and protected team page

- Hardened contact, calculator, audit, Meta lead and tim-login endpoints with strict methods/origins/content types/body and field limits, safe email/phone/URL validation, rate controls, no-store/security headers, privacy-safe logs and generic errors.
- Hardened mail transports with file/URL access disabled and upgraded the active mail dependency.
- tim-login now uses constant-time password comparison, SameSite=Strict/HttpOnly/Secure 8-hour cookie, bounded body and origin/rate controls.
- Existing middleware path normalization remained intact; no-cookie clean/encoded/dot-segment tim variants all resolve to the login page.

Dependencies and infrastructure

- Removed two unused vulnerable dependencies and unused vulnerable framework/type tooling.
- Complete npm audit now reports zero vulnerabilities.
- Enforced IMDSv2 on BookStack, Planka and Documenso EC2 definitions.
- Pinned Nginx upstream Host headers to configured server names.
- Normalized WebSocket Upgrade/Connection values to literal allowlists; independent review adjudicated the two syntax-only h2c warnings as mitigated.
- Replaced standard XML parsing with defusedxml.

Tenant-local cleanup

- Deleted the expired Vercel OIDC token.
- Restricted active ignored Terraform variables/state to mode 0600.
- Restricted prospect/lead output to 0700 directories and 0600 files.
- No tenant credential value is recorded in this page or evidence summaries.

Verification

- Local API security tests: **19/19 PASS**.
- Preview Playwright: **34/34 PASS**, zero console errors.
- Production Playwright: **34/34 PASS**, zero console errors.
- GitHub Security checks: **PASS**.
- Vercel automatic production deployment: **READY**.
- Gitleaks reachable history/current candidate: **0 findings**.
- npm audit: **0 vulnerabilities**.
- Semgrep: **P0=0 / P1=0**; two WebSocket warnings independently adjudicated as mitigated.
- Independent review: **PASS, P0=0, P1=0**.

Residual low risks / follow-up

1. In-memory serverless rate controls are best-effort per instance. A separate tenant-approved Vercel WAF/central rate-limit design is recommended if abuse volume increases.
2. Active Terraform state remains local but ignored and mode 0600. Migration to encrypted remote state requires a separate tenant infrastructure change and validated AWS ownership.
3. The canonical dirty SnowIT checkout remains preserved; it must be reconciled by its owner before fast-forwarding to main.

Evidence

- `/Users/makinja/system/evidence/107296/`
- `/tmp/evidence-107296-preview/browser-verification.json`
- `/tmp/evidence-107296-production/browser-verification.json`

Revision #1

Created 2026-08-17 21:25:42 UTC by John

Updated 2026-08-17 21:25:42 UTC by John