Security Sweep — Public Repository & alai.no Hardening (MC #107285)

Security Sweep — Public Repository & alai.no Hardening (MC #107285)

Date: 2026-08-16
Scope: `johnatbasicas/alai-web`, `https://alai.no`, and `https://ucenje.alai.no`
Production commit: `620dd3af082952b7dbded28a4c5b4685b5445366`
Pull request: `johnatbasicas/alai-web#2`

Trigger

The source repository was public and exposed tracked `CLAUDE.md` and `.claude/**` files. A full sweep was ordered to identify and remove repository, deployment, secret-handling, browser, and production exposure risks.

Confirmed findings

1. Public GitHub access exposed agent metadata and internal operational instructions.
2. A stale `index.html.bak` file was publicly readable on `alai.no`.
3. A hidden internal `.credits.md` file was publicly readable on `ucenje.alai.no`.
4. Deprecated Vercel state contained expired OIDC tokens and duplicate local backups.
5. A legacy unused mail dependency had high-severity advisories.
6. GitHub Actions used mutable action tags; repository secret scanning and branch protection were unavailable or disabled.
7. Pages lacked a true 404 response and a complete Content Security Policy.

8. The contact proxy lacked bounded streaming input, complete validation, honeypot handling, safe upstream errors, and dynamic-response security headers.
9. The GitHub Cloudflare deploy token was stale, causing repeated authentication failures.
10. Wrangler debug logs contained local proxy shared-secret material and were too broadly readable.

Remediation completed

Repository and source

- Changed the GitHub repository to **private**; anonymous raw access now returns 404.
- Removed tracked `CLAUDE.md`, `.claude/**`, obsolete credential-setup instructions, and legacy Vercel/mail runtime files.
- Removed expired Vercel token files, deprecated Vercel state/backups, vulnerable local dependencies, and ignored HTML backups.
- Moved legitimate non-runtime documentation and verification sources outside deployable asset roots.
- Removed an unrelated Azure DevOps remote from the local web repository.

Cloudflare Pages

- Added `.assetsignore` protection to both Pages roots.
- Added deterministic public-asset preflight validation and bypass regression tests.
- Added real `404.html` responses to both sites.
- Added CSP, HSTS, `nosniff`, clickjacking, permissions, referrer, and cross-origin headers.
- Removed Google-hosted font and analytics runtime dependencies instead of weakening CSP.
- Kept `ucenje` static-only by isolating its Wrangler working directory.
- Added edge tombstone redirects for the two stale cached sensitive paths; requests now resolve to 404.

Contact endpoint

- Enforced JSON content type and an 8 KiB streaming body limit.
- Added strict name/email/message validation and conservative email grammar.
- Activated the existing honeypot.
- Restricted browser origins and unsupported methods.
- Added a 10-second upstream timeout and generic upstream failure responses.
- Added `no-store` and complete security headers to dynamic responses.

CI and credentials

- Pinned GitHub Actions to immutable commit SHAs.
- Added Gitleaks, asset checks, Python regression tests, contact-function tests, and Dependabot.
- Restricted Actions to selected actions with mandatory SHA pinning and read-only defaults.
- Restored the valid scoped Cloudflare Pages token from the approved vault and updated GitHub Secrets without exposing the token.
- Verified canonical CI deployment of both Pages projects.
- Restricted Wrangler configuration/evidence permissions and removed debug logs containing proxy secrets.

Verification

- Production Playwright gate: **21/21 PASS**.
- Browser console errors: **0**.
- Gitleaks current tree/history: **0 findings**.
- Semgrep OWASP/JavaScript: **0 findings**.
- Open Dependabot alerts: **0**.
- Canonical GitHub Actions deployment: **SUCCESS**.
- Sensitive live paths: **404 after edge routing**.
- Repository visibility: **PRIVATE**.

Evidence

- `/Users/makinja/system/evidence/107285/final-security-sweep-report.json`
- `/Users/makinja/system/evidence/107285/browser-verification.json`
- `/Users/makinja/system/evidence/alai-web-security-sweep-20260816/FINAL-REPORT.md`

Evidence directories are restricted to user-only access. No credential values are recorded in this page or its evidence summaries.

Residual low risks

1. GitHub branch protection for a private repository requires a paid plan. Compensating controls are enabled: private visibility, selected SHA-pinned Actions, read-only workflow permissions, Gitleaks CI, web commit signoff, and merged-branch deletion.
2. DNSSEC and CAA remain separate registrar/certificate-issuer changes and require a dedicated controlled rollout.
3. The edge tombstone rules should remain until the old one-week cache lifetime has fully elapsed; then revalidate direct paths before considering rule removal.

Closure

Technical remediation and production verification are complete. This page is the task-specific BookStack record for MC #107285.

Revision #1
Created 2026-08-17 11:54:47 UTC by John
Updated 2026-08-17 11:54:47 UTC by John