LiftedVFO Security Remediation Report

Date: {{DATE}} Prepared by: {{PREPARED_BY}}

Scope

This report addresses the findings and acceptance criteria outlined in “LiftedVFO - Security Pass 1.1 - 2025.09.18.docx”. Each item includes remediation status, how it was addressed, and validation steps. Items not completed include next actions and any blockers.

Legend

- Status: Completed | In Progress | Needs Approval | Not Started | Needs Access

---

Priority 0

0.1 Replace browser tokens with secure cookie sessions

- Status: In Progress
- What we changed: Switched auth to HttpOnly cookie sessions; frontend uses withCredentials; removed Authorization header usage. Logged-in endpoints require cookie. Logout clears cookie.
- Notes/Follow-up: Confirm removal of any remaining token storage patterns; complete Google OAuth move fully server-side.
- Evidence: evidence/A1-browser-tokens.md
- Validation: {{VALIDATION_0_1}}
- Notes/Follow-up: {{NOTES_0_1}}

0.2 Encrypt provider refresh tokens at rest

- Status: In Progress
- What we changed: Added encrypted columns and admin backfill/drop endpoints. Awaiting APP_DEK and staging backfill run, then drop plaintext.
- Notes/Follow-up: Set APP_DEK (>=32 bytes) in Render; run backfill; verify; drop plaintext.
- Evidence: evidence/A2-token-encryption.md
- Validation: {{VALIDATION_0_2}}
- Notes/Follow-up: {{NOTES_0_2}}

0.3 Remove or sanitize raw HTML rendering

- Status: Completed
- What we changed: Replaced dangerouslySetInnerHTML with DOMPurify-powered SafeHtml in EditableSection/PublicBlog
- Validation: XSS payloads stripped in UI; unit tests to follow.
- Evidence: evidence/A3-xss-sanitization.md
- Validation: {{VALIDATION_0_3}}
- Notes/Follow-up: {{NOTES_0_3}}

0.4 Lock down uploads by size and type, stream safely

- Status: Completed
- What we changed: Enforced MIME allowlist and 20MB streaming guard in chat/legal endpoints
- Validation: >20MB -> 413; disallowed type -> 415; allowed under limit -> 200.
- Evidence: evidence/A4-upload-guards.md
- Validation: {{VALIDATION_0_4}}
- Notes/Follow-up: {{NOTES_0_4}}

0.5 CORS and secret key hardening

- Status: Completed
- What we changed: Restricted CORS, enumerated methods, and fail-fast SECRET_KEY/DATABASE_URL in prod
- Validation: Non-allowed origins blocked; app exits in prod if secrets missing/default.
- Evidence: evidence/A5-cors-secret.md
- Validation: {{VALIDATION_0_5}}
- Notes/Follow-up: {{NOTES_0_5}}

0.6 Replace admin header token with real RBAC

- Status: Completed
- What we changed: Removed X-Admin-Token, require session+admin role, added audit log + IP allowlist
- Validation: Admin routes 401/403 when not admin; audit logs present; optional IP allowlist enforced.
- Evidence: evidence/A6-admin-rbac.md
- Validation: {{VALIDATION_0_6}}
- Notes/Follow-up: {{NOTES_0_6}}

A7 Disable configuration probe endpoint in prod

- Status: Completed
- What we changed: Restricted /api/test/config to SuperAdmin only
- Validation: 403 for non-SuperAdmin; 200 for SuperAdmin.
- Evidence: evidence/A7-config-probe.md
- Validation: {{VALIDATION_A7}}
- Notes/Follow-up: {{NOTES_A7}}

A8 Remove hardcoded Google Client ID fallback

- Status: Completed
- What we changed: Removed literals, added prebuild env verification
- Validation: Frontend build fails without VITE_GOOGLE_CLIENT_ID.
- Evidence: evidence/A8-google-client-id.md
- Validation: {{VALIDATION_A8}}
- Notes/Follow-up: {{NOTES_A8}}

Priority 1

1.1 Brute force protection and admin 2FA

- Status: In Progress
- Changes: Added rate limiting on /api/token and TOTP enforcement when enabled; SuperAdmin enrollment endpoint; frontend OTP flow
- Notes: Complete admin enrollment UX; consider WebAuthn as next phase.
- Evidence: evidence/P1-1.1-bruteforce-2fa.md
- Validation: {{VALIDATION_1_1}}
- Notes: {{NOTES_1_1}}

1.2 RAG and AI safety guardrails

- Status: Not Started
- Changes: Planned: stricter prompt guardrails, tool allowlist enforcement, injection tests, source citation checks.
- Evidence: evidence/P1-1.2-rag-guardrails.md
- Validation: {{VALIDATION_1_2}}

- Notes: {{NOTES_1_2}}

1.3 Schema migrations via Alembic

- Status: Not Started
- Changes: Planned: Introduce Alembic versioned migrations and remove startup DDL.
- Evidence: evidence/P1-1.3-alembic.md
- Validation: {{VALIDATION_1_3}}
- Notes: {{NOTES_1_3}}

1.4 Security headers and CSP at the edge

- Status: Partial
- Changes: Added app-level security headers; edge CSP report-only ready with Render steps
- Notes: Apply CSP header in Render (report-only), monitor, then enforce.
- Evidence: evidence/P1-1.4-csp.md
- Validation: {{VALIDATION_1_4}}
- Notes: {{NOTES_1_4}}

1.5 Observability, health, and error reporting

- Status: Completed
- Changes: Added /healthz, DB-checked /readyz, request IDs, optional Sentry
- Validation: /healthz ok; /readyz returns ready; responses include X-Request-ID; Sentry captures errors when DSN set.
- Evidence: evidence/P1-1.5-observability.md
- Validation: {{VALIDATION_1_5}}
- Notes: {{NOTES_1_5}}

Priority 2

2.1 PII masking and selective encryption

- Status: In Progress
- Changes: Admin audit log redaction and global logging redaction filter; targeted encryption via 0.2.
- Notes: Extend masking coverage and lint checks; UI masking where appropriate.
- Evidence: evidence/P2-2.1-pii-masking.md
- Validation: {{VALIDATION_2_1}}
- Notes: {{NOTES_2_1}}

2.2 Dependency and image scanning in CI

- Status: In Progress
- Changes: Added Bandit, pip-audit, npm audit (prod), Trivy FS scan; fail on high/critical.
- Notes: Add container image scans and SBOM on releases.
- Evidence: evidence/P2-2.2-ci-scanning.md
- Validation: {{VALIDATION_2_2}}
- Notes: {{NOTES_2_2}}

2.3 Docker hardening

- Status: Completed
- Changes: Multi-stage builds; backend non-root user; nginx static serve for frontend.
- Evidence: evidence/P2-2.3-docker-hardening.md
- Validation: {{VALIDATION_2_3}}
- Notes: {{NOTES_2_3}}

Appendices

- Tracker: docs/security/Remediation-Tracker.csv
- Evidence pack (paths & excerpts): docs/security/evidence/
- Test plan: docs/security/Test-Plan.md

Appendix A: Full Remediation Tracker Table

ID	Priority	Title	Required Change (summary)	Acceptance Criteria (summary)	
0.1	P0	Replace browser tokens with secure cookie sessions	Move OAuth to backend, issue HttpOnly+Secure+SameSite cookie; remove localStorage tokens; withCredentials on frontend	No localStorage tokens; cookie set with HttpOnly+Secure; API requires cookie; server-side logout clears cookie	frontend/ frontend/ frontend/ backend/ backend/
0.2	P0	Encrypt provider refresh tokens at rest	App-layer encryption (DEK/KMS) for provider tokens; add enc+iv columns; backfill; drop plaintext	Encrypted columns present; rotation documented; no raw tokens in logs	backend/ backend/ admin ba
0.3	P0	Remove or sanitize raw HTML rendering	Replace dangerouslySetInnerHTML with sanitizer (DOMPurify) or markdown	No direct dangerouslySetInnerHTML for user content; tests strip	