Strataflows

Security Scanner Findings — False Positive & Accepted Risk Documentation

CASA Tier 2 DAST Scan | TAC Security ESOF AppSec ADA | Score: 9.7/10 | All Findings: Patched

Overview

Strataflows completed a CASA Tier 2 DAST security assessment conducted by TAC Security using ESOF AppSec ADA. The assessment returned a score of 9.7/10. All eight findings are now marked as Patched. This document provides detailed justification for each finding, explaining the technical context, the remediation applied (where applicable), and — for infrastructure-level findings — why they represent accepted risks rather than exploitable vulnerabilities.

Finding Summary

#	Finding	Severity	Status	Disposition
1	Cross-Domain Misconfiguration	Low	Patched	Accepted — Vercel CDN public static assets
2	Proxy Disclosure	Low	Patched	Accepted — Vercel edge infrastructure
3	Sub Resource Integrity Missing	Low	Patched	Accepted — Dynamic third-party CMP (Termly)
4	Permissions Policy Header Not Set	Info	Patched	Fixed — header added in next.config.mjs
5	Modern Web Application	Info	Patched	Informational only — no action required
6	Storable but Non-Cacheable Content	Info	Patched	Informational — correct Next.js cache behavior
7	Retrieved from Cache	Info	Patched	Informational — Vercel CDN Age header behavior
8	User Agent Fuzzer	Info	Patched	Informational — consistent responses, no leakage

Detailed Justifications

Finding 1 — Cross-Domain Misconfiguration (Low) — Patched

Field	Detail
CWE ID	CWE-264
Affected URLs	/_next/static/chunks/*.css, /_next/static/chunks/*.js, /_next/static/media/*.woff2, /manifest.json, /sitemap.xml
Evidence	Access-Control-Allow-Origin: * header present on above URLs
Root Cause	Vercel CDN sets wildcard CORS headers by default on public static assets. This behavior is not configurable at the application layer.
Risk Assessment	These are immutable, content-addressed static assets (CSS, JS bundles, fonts). They contain no sensitive data. Wildcard CORS on public fingerprinted assets is standard CDN behavior across all Vercel-hosted Next.js applications. No user data is served from these paths. Application code sets zero Access-Control-Allow-Origin headers — confirmed by full codebase audit.
Remediation	Not feasible at application layer. Vercel CDN headers for static assets are not configurable. All sensitive API endpoints use restrictive CORS via Next.js headers configuration. Risk accepted as infrastructure limitation.

Finding 2 — Proxy Disclosure (Low) — Patched

Field	Detail
CWE ID	CWE-204
Evidence	TRACE, OPTIONS, and TRACK methods identify Vercel as hosting infrastructure

Field	Detail
Root Cause	Vercel edge infrastructure responds to TRACE/OPTIONS/TRACK with server identification. X-Powered-By header is suppressed in Strataflows (poweredByHeader: false in next.config.mjs).
Risk Assessment	Vercel is a publicly known, widely used, and reputable hosting platform. Knowledge that Strataflows runs on Vercel provides no meaningful attack surface. Vercel maintains SOC 2 compliance and a dedicated security team. TRACE/TRACK method responses are controlled entirely by Vercel infrastructure and cannot be disabled at the application layer.
Remediation	X-Powered-By header suppressed in next.config.mjs. TRACE/OPTIONS/TRACK method responses are Vercel infrastructure behavior and not controllable by the application. Risk accepted as infrastructure limitation.

Finding 3 — Sub Resource Integrity Attribute Missing (Low) — Patched

Field	Detail
CWE ID	CWE-345
Evidence	link rel=preload tag loading https://app.termly.io/resource-blocker/... without integrity attribute
Root Cause	Termly is a third-party consent management platform (CMP) used for GDPR/CCPA cookie compliance. Termly's resource-blocker script is dynamically updated by Termly to implement evolving cookie compliance requirements.
Risk Assessment	Pinning an SRI integrity hash to this script would cause it to silently fail (browser refuses to execute on hash mismatch) the next time Termly pushes any update — breaking cookie consent functionality and potentially creating GDPR/CCPA compliance violations. This is a known and accepted limitation of all third-party CMP integrations. Termly does not publish official integrity hashes for dynamic scripts for this exact reason. Industry-standard practice for CMP integrations.
Remediation	SRI pinning is not feasible for dynamically-updated CMP scripts without breaking legal compliance functionality. Termly is a trusted, established CMP vendor. Risk accepted as necessary for legal compliance operation.

Finding 4 — Permissions Policy Header Not Set (Info) — FIXED

Field	Detail
CWE ID	CWE-693
Remediation Applied	Permissions-Policy header added globally in next.config.mjs headers() configuration.
Header Value	Permissions-Policy: camera=(), microphone=(), geolocation=(), interest-cohort=()
Result	All unused browser features explicitly disabled. Header present on all application responses.

Findings 5–8 — Informational Findings (Info Severity) — Patched

All four informational findings require no remediation per scanner documentation. Each is documented below for completeness.

#	Finding	Justification
5	Modern Web Application	Informational alert indicating the scanner identified a modern JavaScript SPA framework (Next.js/React). Per OWASP ZAP documentation, this alert is informational only. No action required.
6	Storable but Non-Cacheable Content	Authenticated application pages use Cache-Control: no-store. Static assets use max-age=31536000 (immutable CDN caching for content-addressed files). This is correct and intentional caching behavior for a Next.js application on Vercel.
7	Retrieved from Cache	Vercel CDN Age: 0 header is present on responses. Age: 0 indicates content was freshly fetched — not stale. No sensitive data is served from cached endpoints. Authenticated routes use no-store. This is standard Vercel CDN behavior.
8	User Agent Fuzzer	Scanner detected consistent response behavior across different User-Agent strings. This confirms the application does not leak different data or expose different functionality based on User-Agent. No information leakage detected.

Security Headers Implemented

The following security headers are set globally on all Strataflows responses via next.config.mjs:

Header	Value	Purpose
X-Content-Type-Options	nosniff	Prevents MIME type sniffing attacks
X-Frame-Options	SAMEORIGIN	Prevents clickjacking via iframe embedding
Referrer-Policy	strict-origin-when-cross-origin	Controls referrer information sent with requests
Permissions-Policy	camera=(), microphone=(), geolocation=(), interest-cohort=()	Disables all unused browser features
Content-Security-Policy	default-src 'self'; script-src 'self' + Termly + Stripe allowlist	Restricts resource loading to trusted sources only

SAQ Compliance Summary

Strataflows completed the full 54-requirement Self-Assessment Questionnaire (SAQ) as part of the CASA Tier 2 assessment. All 54 requirements were addressed. The table below summarizes key compliance areas:

Area	Requirements	Status
Architecture Documentation	1	Documented in ARCHITECTURE.md, SYSTEM_LAW.md, FILE_RESPONSIBILITIES.md
Authentication & Session Mgmt	10	Supabase Auth with JWT, bcrypt password hashing, single-use tokens, session invalidation on logout
Access Control	8	RLS on all tables, server-side enforcement, principle of least privilege
Cryptography	4	AES-256 at rest (Supabase), TLS in transit (Vercel), CSPRNG UUIDs (gen_random_uuid)
Input Validation & Encoding	7	React built-in XSS protection, parameterized Supabase queries, no eval() usage
Data Protection	7	PII encrypted at rest, no credentials logged, no sensitive data in URLs or localStorage
Build & Deployment	4	Vercel CI/CD, automated deployments, infrastructure-as-code, OCSP stapling via Vercel
Anti-Automation	2	Supabase rate limiting, founding member redemption cap, Stripe abuse prevention
Configuration	6	Debug mode off in production, no default accounts, security headers configured
Other Requirements	5	No LDAP, no client-side access control, no SVG injection, HTTP method restrictions