VEXERA

SECURITY ASSESSMENT · PHASE 2 · EXECUTIVE EDITION

Security App LLC

Glacier Infrastructure · Phase 2 External Service Review (Executive Edition)

October 24, 2026

INFRASTRUCTURE | EXTERNAL RED TEAM | EXECUTIVE SUMMARY

PREPARED FOR

Security App LLC
Glacier infrastructure

PREPARED BY

David De Jesus
Vexera Consulting LLC
david@vexeraconsulting.com

PHASE 2 · EXECUTIVE EDITION

Table of Contents

01 Executive Summary 2
02 Assessment Scope at a Glance 3
03 Assessment Outcomes 4
04 Engineering Follow-up 6
05 Remaining Limits and Next Phase 7
06 Notices and Remarks 8

SECTION 01

Executive Summary

Vexera Consulting LLC completed a Phase 2 external red team review of Glacier's infrastructure on 24 October 2026. Testing was unauthenticated and read-only against production and staging hosts derived from the mobile apps, console JavaScript, DNS, and certificate transparency. **No vulnerabilities were found at this time.**

Every sampled API path required authentication or did not exist: 18 of 21 app-derived GET paths returned HTTP 401 and three returned 404 in each environment, and all read-only POST lookups and the WireGuard preset-config operation returned 401. No customer records, account details, WireGuard configuration URL, or AWS credentials were returned. The public Cognito identity pool refused to issue an unauthenticated identity, conventional secret and configuration paths returned only the public web shell, browser security headers were in place, and no cross-site scripting executed on the tested pre-login routes.

No severity or CVSS score is assigned because no vulnerability was confirmed. Two conditions are recorded as observations, not vulnerabilities: production and staging share the same public Cognito pool and client configuration, and the web app stores session tokens in browser localStorage when available. Neither was shown to enable unauthorized access or token theft. The remaining validation needs an authenticated session and is described below.

RESULT	API PATHS PROBED	ANONYMOUS RECORDS	XSS EXECUTIONS
0	21	0	0
Vulnerabilities found · This assessment	GET, each environment	None returned	Pre-login routes

> What this means for leadership: the public attack surface held up to unauthenticated testing, with no vulnerability found and no customer data reachable without a token. Two configuration observations are flagged for owner review, not as flaws. Closing the last questions, cross-environment access and PKCE enforcement, needs an authenticated-session test in a follow-up phase.

SECTION 02

Assessment Scope at a Glance

What was tested, how, and where the unauthenticated boundary sits.

TARGET

Scope	Glacier infrastructure, production and staging
Hosts	Console, auth, API gateway, and support hosts from app config, DNS, and CT
Access	Unauthenticated, read-only; no customer session used

METHOD

Approach	External HTTP, API, OAuth, TLS, and browser checks
Tooling	httpx, Nmap, Nuclei, Gitleaks, and an in-app browser
Change	No state-changing request; no data modified

COVERED THIS PHASE

- Unauthenticated API, OAuth, CORS, and response-header checks against production and staging.
- TLS and limited port scans of the console A records, plus static review of 50 JavaScript chunks.
- Browser tests of pre-authentication routes for cross-site scripting.

NOT COVERED · NEEDS AN AUTHENTICATED SESSION

- Authenticated API traffic and customer-data endpoints (no token was used)
- A cross-environment test from a signed-in production session
- PKCE enforcement at code redemption (no authorization code was issued)
- The signed-in mobile device, which was not used for this pass

This phase deliberately stayed unauthenticated and read-only. The results describe what an anonymous attacker could reach; they are not a statement about authenticated or internal exposure, which a later phase should cover.

SECTION 03

Assessment Outcomes

Each test area, its Phase 2 result, and what remains open.

AREA	PHASE 2 RESULT	WHAT'S STILL OPEN
Anonymous API access	18 of 21 GET paths returned 401 and three returned 404 per environment; all POST lookups and the WireGuard preset-config operation returned 401. No records or secrets were returned.	Repeat the data-access checks from an authenticated session to confirm per-user authorization.
Cognito identity pool	A direct unauthenticated GetId returned HTTP 400 and issued no identity or temporary AWS credentials.	No further action; the behavior is as expected.
OAuth and Hosted UI	The implicit flow and an unregistered redirect were rejected; a code-flow request without PKCE reached the login page but issued no code.	Verify PKCE enforcement at code redemption in an authenticated flow.
Browser security controls	HSTS, CSP (script-src 'self', no unsafe-inline), frame, content-type, and referrer protections were present, with no permissive CORS.	Maintain the current headers; consider Trusted Types.
Cross-site scripting	No application sink was found across 50 chunks; pre-login probes rendered as inert text with no DOM marker.	Exercise authenticated pages and API-backed content in a later phase.
Secret and config exposure	Conventional secret paths returned only the public HTML shell; Gitleaks and source-map checks found nothing.	No action; no secret file was exposed.

These are assessment outcomes, not scored findings. No severity or CVSS score is assigned in this phase. Full evidence, exact requests, and raw responses are in the technical report (Appendices A to D).

OBSERVATIONS TO REVIEW · NOT VULNERABILITIES

Two conditions are recorded as observations, not vulnerabilities. Production and staging expose the same public Cognito pool and client configuration, and the staging build's redirect list includes the production console origin; owner validation across environments is appropriate. Separately, the web app stores access, ID, and refresh tokens in browser localStorage when available, which would be reachable by JavaScript if a same-origin XSS were ever found. Neither condition was shown to enable unauthorized access in this assessment.

What Testing Confirmed

- Unauthenticated API requests required a token: sampled reads returned HTTP 401 or 404 with no customer data.
- The public Cognito identity pool refused to issue an anonymous identity or AWS credentials.
- The OAuth client rejected the implicit flow and unregistered redirect URIs.
- Browser security headers (HSTS, CSP, frame and content-type protections) were present on the production console.
- No cross-site scripting executed on the tested pre-authentication routes; payloads rendered as inert text.
- Conventional secret and configuration paths returned only the public application shell, not secret files.

SECTION 04

Engineering Follow-up

The order reflects the largest open questions and the quickest hardening wins; it is not a severity rating.

ORDER	ENGINEERING FOLLOW-UP AND EVIDENCE GATE
1	Run the data-access and cross-environment checks from an authenticated production session to confirm per-user and per-environment authorization.
2	Verify PKCE enforcement at code redemption, since no authorization code was issued during unauthenticated testing.
3	Review the shared production/staging Cognito configuration and the staging redirect list that includes the production origin.
4	Move refresh tokens out of JavaScript-readable storage (Secure, HttpOnly, SameSite cookies via a backend-for-frontend), keep access tokens in memory, and consider Trusted Types alongside the current CSP.

SECTION 05

Remaining Limits and Next Phase

The strongest remaining questions need an authenticated session. This pass was unauthenticated and read-only by design, so customer-data endpoints, per-user authorization, and any cross-environment access from a signed-in production session were not exercised. PKCE enforcement at code redemption could not be tested because no authorization code was issued, and authenticated pages were not available for cross-site scripting review.

What the Next Phase Needs

- An authenticated production session to re-run the data-access and authorization checks.
- A controlled cross-environment test to confirm whether a production session can reach staging-only resources.
- An authenticated OAuth flow to verify PKCE enforcement at code redemption.

Effort

Header and configuration hardening can begin now. Closing the authorization and PKCE questions needs a follow-up phase with an authenticated account session.

SECTION 06

Notices and Remarks

Copyright and Distribution

© 2026 Vexera Consulting LLC. All rights reserved.

This executive edition is prepared for Security App LLC and designated Business Confidential. Distribution, publication, and reuse are governed by the engagement agreement and Security App LLC approval.

Reference for this executive edition: **VEX-GLCR-2026-INF2E-1024-01**. It summarizes the Phase 2 infrastructure technical report; where the two differ, the technical report governs.

Assessment Basis and Limits

Findings reflect the hosts, methods, and conditions of an unauthenticated, read-only Phase 2 external review on 24 October 2026. The observations are not a comprehensive inventory of every possible defect, and several questions remained open under the unauthenticated scope described above.

No vulnerabilities were found at this time. That result reflects what this phase could observe from outside an authenticated session; it is not a guarantee for authenticated paths, internal services, or future changes, which should be reassessed.

Assessor

SIGNATURE

DATE

David De Jesus
Penetration Tester / Red Team Operator
Vexera Consulting LLC
david@vexeraconsulting.com | (253) 341-1781