Security Sweep — bilko.cloud HR — MC #107298 (2026-08-18)

bilko.cloud Security Sweep — MC #107298

Verdict: PASS
Date: 2026-08-18
Scope: `bilko.cloud` HR landing only (`apps/landing-hr`); separate verdict from bilko.io and bilko.company.

Baseline findings

1. **P1 — mixed Cloudflare Pages asset root:** production served exact `wrangler.toml` and `package.json` with HTTP 200; unknown/sensitive paths returned the homepage as HTTP 200.
2. **P1 — stale removed-asset cache:** after the first production asset-root fix, exact config URLs remained cached with `s-maxage=604800`. A successful zone purge did not evict the Pages asset cache. A Pages middleware deny guard was added and independently passed CI before the final deploy.
3. **P2 — missing browser controls:** no CSP, HSTS, frame-deny or Permissions-Policy on the baseline homepage.
4. **P2 — public Function hardening gaps:** request bodies and several fields were unbounded; Turnstile accepted any successful hostname and had no timeout.
5. **P2 — blanket SAST exclusion:** `apps/landing-hr/` was excluded from Semgrep.

Remediation

- Physically isolated all 52 unchanged runtime assets under `apps/landing-hr/public/`; byte-integrity check: 52/52 identical.

- `wrangler.toml` now deploys `public`; workflow/docs use app cwd plus `pages deploy public`, preserving sibling Functions.
- Added `.assetsignore`, asset preflight, real `404.html`, CSP/HSTS/frame/referrer/permissions/COOP/CORP headers and immutable asset caching.
- Added Pages `_middleware.js` fail-closed guard for config/source/hidden/backup paths before cache lookup.
- Bounded request body at 16 KiB and lead fields; unsupported media returns 415.
- Turnstile now fails closed without a secret, uses a 5-second timeout, checks HTTP success and requires hostname `bilko.cloud`.
- Sanitized storage failure response codes; internal details remain server-side.
- Added 12 focused HR Function/middleware tests and updated canonical landing tests for the Fetch Request/public-root contract.
- Removed HR blanket Semgrep exclusion.

Verification

- Local HR tests: **12/12 PASS**.
- Canonical landing suite: **29/29 PASS**.
- Asset preflight: PASS; local Wrangler: Functions compiled and sensitive paths 404.
- Configured landing Gitleaks: **0**; Semgrep: **0**; pnpm production audit: **0 at all severities**.
- Raw shared-repo Gitleaks findings were adjudicated as documented synthetic test values/placeholders; no landing secret finding. Existing unrelated credential work is not duplicated here.
- Preview Playwright: **5/5 PASS**, desktop and mobile screenshots.
- AzDO PR #352 → build #1129 PASS → merge `41383beefeaeccb8725c7ef897d8280d4935bf92`.
- Stale-cache follow-up PR #353 → build #1131 PASS → merge `6c75e5c45141c59a01586351d157aa56eae11edf`.
- Production deployment: `d5dbe05b-0c1e-42c3-b15d-5fd6dfdb7525`, source `6c75e5c`.
- Final production Playwright: **6/6 PASS** (desktop/mobile, security headers, Turnstile source, submit click geometry, legal pages, sensitive 404s, non-mutating Function guards).
- Final exact-path probes: **15/15 HTTP 404**, `Cache-Control: no-store` for guarded paths.
- Homepage bytes/hash exactly match merged `public/index.html`.
- TLS valid for `bilko.cloud`; HSTS/CSP and all required browser headers live.
- All three #107298 preview deployments deleted; no matching preview branch deployment remains.

Linked finding reconciliation

- **#106408:** current production/source uses live Turnstile sitekey `0x4AAAAAADmvPOAvTZjn4gU9`; deleted key absent. No real lead was submitted.

- **#106413:** current source and production contain no cookie-banner overlay; Playwright proves the submit button owns its center hit point. This sweep does not fabricate an end-to-end lead mutation.
- **#106358:** IO/BA task is outside this HR verdict. HR `BILKO_LEADS` production/preview bindings remain in `wrangler.toml`, and both production deployments logged `Compiled Worker`.
- Canonical main's more conservative MC #107052 landing claims are now live; this intentionally supersedes the previously deployed unmerged #106980 branch copy.

Residual / accepted constraints

- CSP retains `'unsafe-inline'` because the legacy static page embeds inline script/style. Migration to hashes/nonces is recommended but not required for this closure.
- No valid Turnstile/real-lead submission was made, by explicit non-mutation/privacy constraint. Verification covers live widget identity, DOM geometry, invalid/hostile requests, Function unit contracts and compiled production Functions.
- Bilko monorepo/application risks outside `apps/landing-hr` are not inherited as a PASS for bilko.io, bilko.company or authenticated Bilko SaaS surfaces.

Evidence anchors

- `final-live-security-summary.json`
- `production-playwright-final-report.json`
- `production-cache-guard-deploy.log`
- `azdo-build-1129.json`, `azdo-build-1131.json`
- `azdo-pr-completed.json`, `cache-guard-pr-completed.json`
- `remediation-local/`
- `screenshots/production-final-desktop.png`, `screenshots/production-final-mobile.png`

Revision #1
Created 2026-08-18 06:02:04 UTC by John
Updated 2026-08-18 06:02:04 UTC by John