PTworker.me Authorized External Security Assessment

External security assessment and Up to Code software audit for PTworker.me

Target: https://ptworker.me

Tested (UTC): 2026-11-06T04:18:22.068Z

Executive summary

External read-only probes against https://ptworker.me found no critical or high issues. 26 controls verified. The bundled Up to Code software audit scored 100/100 (60 of 60 scored checks passed).

Scope ? in scope

? HTTPS web application at ptworker.me (staff app, patient portal, public pages)

? Anonymous REST API boundary (auth required on sensitive routes)

? Security response headers and static file exposure

? Public /api/public information disclosure

Scope ? out of scope

? Authenticated IDOR / cross-practice access (requires test accounts and written rules)

? Claim.MD, Stedi, PayPal, Stripe, and SMS provider infrastructure

? Denial-of-service or brute-force attacks

? Real patient PHI

? Mobile native apps (portal APK uses same web backend)

Methodology

? Authorized external probing from PTworker maintainers (no exploitation of live patient data).

? Safe automated checks: sensitive path probes, header review, unauthenticated API samples, CORS spot-check, injection-shaped kiosk input.

? Production smoke and deploy audit scripts against the live host.

? Up to Code software audit (sandbox sample office, API role checks, backup crypto, outbound fetch logging)?see up-to-code.html.

External findings

None on this run.

Controls verified

? HSTS present on /

? X-Content-Type-Options on /

? Clickjacking mitigation signal on /

? HSTS present on /app.html

? X-Content-Type-Options on /app.html

? Clickjacking mitigation signal on /app.html

? HSTS present on /api/public

? X-Content-Type-Options on /api/public
? Clickjacking mitigation signal on /api/public
? Protected or absent: /.env (404)
? Protected or absent: /.git/HEAD (404)
? Protected or absent: /data/pt.db (404)
? Protected or absent: /api/settings (401)
? Protected or absent: /api/billing/desk (401)
? Protected or absent: /api/patients (401)
? Protected or absent: /wp-login.php (404)
? Protected or absent: /server.mjs (404)
? Protected or absent: /src/db.mjs (404)
? Protected or absent: /var/data/pt-me.db (404)
? /api/public has no API keys or Stripe secrets
? PayPal client ID only (expected for checkout JS; not the secret)
? No demo password in public API (or demo off on prod)
? PUT /api/settings requires auth
? Disk audit gated (404)
? Kiosk lookup rejects injection-shaped input safely
? CORS does not reflect evil.example on /api/public

Up to Code software audit

Score 100/100 ? 60 of 60 scored checks passed

Full audit: https://ptworker.me/up-to-code.html