Tucker Payment Processing - Independent Security Scan

Mozilla HTTP Observatory

Site tested: **https://tuckerpaymentprocessing.com** | Scan date: **2026-11-24** | Scanner: Mozilla HTTP Observatory (MDN)

BEFORE FIXES	FINAL
n/a	**A+**
run after the fixes only	2026-11-25 about 01:35 UTC

A+ with a score of 140 out of 100 and 12 of 12 tests passed (120 in the afternoon round). The bonus points come from a strict Content-Security-Policy, Referrer-Policy, Subresource Integrity, frame protection and, added that evening, Cross-Origin-Opener-Policy and Cross-Origin-Resource-Policy (+10 each).

Checks

Check	Before	After	Detail
Content Security Policy		PASS	+5: implemented without 'unsafe-inline' or 'unsafe-eval'
Cookies		PASS	No cookies detected
Cross-Origin Resource Sharing		PASS	Content not visible via CORS
Redirection		PASS	HTTP redirects to HTTPS on the same host
Referrer Policy		PASS	+5: strict-origin-when-cross-origin
Strict Transport Security		PASS	Two years (max-age 63072000), includeSubDomains, preload; preload listing pending
Subresource Integrity		PASS	+5: all scripts loaded securely (self-hosted)
X-Content-Type-Options		PASS	nosniff
X-Frame-Options		PASS	+5: via CSP frame-ancestors 'none' and DENY
Cross-Origin-Embedder-Policy		INFO	Not set on purpose: it would break the Turnstile human check (no score impact)
Cross-Origin-Opener-Policy		PASS	+10: same-origin
Cross-Origin-Resource-Policy		PASS	+10: same-origin

Notes

• Remaining optional suggestions: default-src 'none' in the CSP, and the HSTS preload bonus once the browser preload list includes the domain (submitted 2026-11-24). Cross-Origin-Embedder-Policy is left off on purpose (see Known limits).

Verify it yourself

Run the same scan live:
https://developer.mozilla.org/en-US/observatory/analyze?host=tuckerpaymentprocessing.com

Method: each scanner was run against the live site from a normal web browser on 2026-11-24 (US Eastern; the evening round is dated 2026-11-25 in UTC). Grades, times (UTC) and check results are recorded exactly as shown on each scanner's result page; the 'Verify it yourself' links run the same scan again live. Scans run by Michael Cunningham with AI assistance (Claude).