Tucker Payment Processing - Independent Security Scan

Security Scan Summary

Site tested: **https://tuckerpaymentprocessing.com** | Scan date: **2026-11-24**

Tucker Payment Processing was tested by independent, public security scanners. The first round found three gaps (old TLS versions still accepted, DNS not signed with DNSSEC, and no security.txt or CAA record). All were fixed the same afternoon and every scanner was run again. That evening the site was hardened further (email spoofing lockdown, HSTS preload, cross-origin isolation headers, ping disabled) and the scanners were run a third time. This summary shows the first round and the latest results.

Scanner	What it checks	Before	Final
Qualys SSL Labs SSL Server Test	HTTPS/TLS configuration: protocols, certificates, key exchange, cipher strength, HSTS	**B**	**A+**
Internet.nl Website Test	Modern standards: IPv6, DNSSEC, HTTPS/TLS, security headers, security.txt, route security (RPKI)	**75%**	**96%**
Mozilla HTTP Observatory	Web security best practices: CSP, cookies, CORS, redirects, HSTS, SRI, framing, cross-origin policies	**n/a**	**A+**
SecurityHeaders.com	HTTP security headers that protect visitors' browsers (XSS, clickjacking, sniffing, downgrade)	**A+**	**A+**
Sucuri SiteCheck	Malware, defacement and website blocklists	**Clean**	**Clean**

Fixes made on 2026-11-24

• Cloudflare minimum TLS version raised from 1.0 to 1.2: TLS 1.0 and 1.1 are now refused (SSL Labs B to A+).
• DNSSEC enabled: the domain's DNS records are cryptographically signed and the DS record is published at the .com registry.
• CAA records added: only approved certificate authorities may issue certificates for the domain.
• security.txt published at /.well-known/security.txt (RFC 9116), pointing to a private GitHub vulnerability-reporting channel and SECURITY.md.
• Email spoofing lockdown: the domain sends no email, so SPF (-all), DMARC (p=reject), an empty DKIM key and a null MX record tell every mail server to reject anything claiming to be from it.
• HSTS strengthened to two years with includeSubDomains and preload, Cloudflare 'Always Use HTTPS' turned on, and the domain submitted to the browser HSTS preload list (pending).
• Cross-Origin-Opener-Policy and Cross-Origin-Resource-Policy headers added (Mozilla Observatory +20).
• Ping (ICMP) to the server disabled at the Google Cloud firewall; web traffic still only accepted from Cloudflare.
• Rate limits count an IPv6 visitor by their whole /64 network, so rotating addresses can't dodge them.
• Dependabot security update merged (dnspython 2.9.2).

Known limits

• internet.nl still marks two TLS 1.2 details (cipher suites; hash function for key exchange) because Cloudflare keeps some older-style options for compatibility. Choosing exact cipher suites is not available on Cloudflare's Free plan. TLS 1.3 is preferred and post-quantum key exchange is supported.
• Sucuri SiteCheck's malware scan was refused (HTTP 403) by Cloudflare's bot defense, which blocks automated scanners by design. Its blocklist check (9 lists) ran and is clean.
• Cross-Origin-Embedder-Policy is deliberately not set: it would break Cloudflare Turnstile, the human check that protects Cipher's Lair.

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).