CheckoutProof

PCI 6.4.3 / 11.6.1 readiness report

Scanned May 5, 2026 at 05:32 PM UTC
4318 ms

SCANNED URL

https://yourstore.example/checkout

28

of 100

Grade F

COMPONENT	SCORE
SRI coverage 1 of 6 external scripts have an integrity hash.	8/50
Content-Security-Policy No CSP header is set on the checkout page.	0/30
Script-count hygiene 7 scripts loaded — within the healthy range for a focused checkout.	10/10
Known-bad-script detection Detection module not yet in production; full credit until it lands.	10/10

Script inventory

SCRIPT	SRI	TYPE
https://js.stripe.com/v3/	OK	ext
https://yourstore.example/themes/storefront/main.min.js	—	ext
https://yourstore.example/plugins/woocommerce/checkout.min.js	—	ext
https://www.googletagmanager.com/gtm.js?id=GTM-PR0OFXX	—	ext
https://www.googletagmanager.com/gtag/js?id=G-PR0OFXXXXX · dynamic	—	ext
https://static.klaviyo.com/onsite/js/klaviyo.js?company_id=ABCDEF	—	ext
(inline)	—	inline

Recommendations

1. Add SRI integrity hashes to the 5 external scripts that don't have them. Pin to versioned URLs where the vendor publishes them.
2. Add a Content-Security-Policy header on your checkout page with script-src restricted to specific domains and report-to wired to a violation endpoint.
3. Maintain a written script inventory with a business justification and named approver for each entry. Required by PCI 6.4.3.
4. Set up automated weekly tamper detection that alerts on changes to scripts, SRI hashes, or your CSP header. Required by PCI 11.6.1.