Web Scanner Header Findings

Illustrative two-page PDF showing how header-related findings can be packaged inside the knowledge base.

Scanner	w3af
Target	https://staging.app.example.com
Profile	authenticated crawl plus lightweight plugin checks
Focus	browser-exposed transport and response-header posture

Findings overview

Finding	Severity	Why a tester cares
Strict-Transport-Security header missing	Medium	Users can still begin on HTTP and lose first-request upgrade protection.
Content-Security-Policy header missing	Medium	No browser-side containment for script and frame sources on authenticated pages.
X-Content-Type-Options missing	Low	Browsers may MIME-sniff script or style responses unexpectedly.
Referrer-Policy not set	Low	Cross-origin requests may leak more URL detail than intended.
Clickjacking protection inconsistent	Medium	Legacy or admin routes may still be embeddable.

Operator notes

• Treat header findings as **route-specific review prompts**, not automatic severity truth.

• If the affected origin is authenticated, admin-capable, or serves active content, header debt deserves quicker remediation.

• Confirm whether the fix belongs in the CDN, reverse proxy, Apache/Nginx vhost, or application layer.

Header and Delivery Findings - Example View

Illustrative second page modeled on a lightweight web-scanner summary for web-server owned controls.

Scanner	Skipfish
Target	https://app.example.com
Run mode	focused crawl against login, account, admin, and export routes
Primary concern	transport, caching, CORS, and active-content delivery posture

Route summary

Route class	Observed issue	Suggested owner
/login and /account	HSTS absent on one legacy hostname alias	edge / vhost owner
/admin	CSP present but broader than intended for third-party script sources	product + reverse-proxy owner
/download/export	No-store missing on personalized export responses	application + delivery owner
/api/public/*	OPTIONS handling inconsistent for credentialed browser clients	API gateway / Nginx owner

Recommended next steps

• Normalize header policy across the canonical origin and any legacy aliases before enabling preload expectations.

• Review CORS only on the browser-facing routes that need it; remove broad wildcard rules from unrelated paths.

• Keep scanner output attached to the release evidence pack, but add a short human interpretation so the finding is not read out of context.