Security headers

The question

A header needs a useful policy

Browser security headers create boundaries for a page. The policy values determine how much those boundaries restrict.

01 Understand

02 Observe

03 Verify

A practical briefing for the people who own your domain.

Security headers

The mechanism

Different headers do different jobs

CSP controls content. Framing rules control embedding. nosniff respects content types. Referrer policy limits referring information.

01 Website response headers

↓

02 Browser interprets each policy

↓

03 Resource, framing and referrer boundaries

The scanner recognises selected header forms. Policy effectiveness requires application-aware testing.

Security headers

The evidence

Our check recognises four controls

> It measures selected header forms on the observed HTTPS response. Presence cannot establish effectiveness or application security.

PUT THE OBSERVATION IN CONTEXT

Public signal

Service context

Operational validation

Use the finding to start an owned review.

Security headers

The handoff

Match policy to the application

Have developers inventory scripts and integrations. Observe CSP reports, then test critical journeys before and after enforcement.

BRING THE RIGHT OWNERS TOGETHER

01 Application security and development owners

02 Web platform owner

Security headers

Your checklist

Keep a browser policy checklist

- ✓ Review actual values
- ✓ Test key routes
- ✓ Confirm legitimate embeds
- ✓ Assign maintenance ownership

> Read the security headers explainer with your development team.
>
> **/learn/security-headers**