

Website configuration

Subscore 39

HTTP / Security Headers

39

- **Reachability** Required

The site is reachable over HTTPS.

- **IPv6 reachability** Recommended

The web server is reachable over IPv6 (2606:4700:10::ac42:9ded).

- **Same website over IPv6** Recommended

IPv6 and IPv4 serve the same website (text similarity 100%).

- **HTTPS redirect** Recommended · Medium

Plain HTTP is not redirected to HTTPS.

Recommendation: Configure a permanent redirect from http:// to https:// for the same host.

- **HSTS** Recommended · Medium

Your web server does not send an HSTS policy.

Recommendation: HSTS requires that your site works fully over HTTPS, including a valid certificate from a publicly trusted authority.

Proceed step by step:

1. Make sure your site works fully over HTTPS now and permanently (e.g. with a reliable certificate-rollover process).
2. Raise the HSTS lifetime gradually. After each step, check carefully for reachability problems and wait out the full `max-age` before moving to the next.
3. Repeat steps 1–2 for every subdomain you want to protect. Only use `includeSubDomains` once you are sure that all (nested) subdomains support HTTPS reliably.
4. Use `preload` only with great care — it is hard to undo and can break reachability of the whole domain and its subdomains.

- **Content-Security-Policy** Recommended · Medium

No Content-Security-Policy header is set.

Recommendation: Define a Content-Security-Policy that only allows the sources your site actually needs.

- **X-Frame-Options** Recommended · Low

No X-Frame-Options header is set.

Recommendation: Send X-Frame-Options: DENY or SAMEORIGIN, or an equivalent frame-ancestors CSP directive.

- **X-Content-Type-Options** Recommended · Low

The X-Content-Type-Options header is missing or not set to nosniff.

Recommendation: Send X-Content-Type-Options: nosniff.

- **Referrer-Policy** Recommended · Low

No Referrer-Policy header is set.

Recommendation: Send a Referrer-Policy such as strict-origin-when-cross-origin or no-referrer.

- **HTTP compression** Optional · Low

HTTP compression (br) is active — a performance plus.

Recommendation: Enable HTTP compression (gzip or Brotli) for text responses to improve load time and bandwidth.

- **security.txt** Recommended · Low

No security.txt file is published.

Recommendation: Publish a signed `.well-known/security.txt` with at least a `Contact:` and an `Expires:` field.

- **HTTP/2** Recommended

The web server supports HTTP/2.

- **HTTP/3** Optional · Info

The web server does not advertise HTTP/3 (QUIC).

Recommendation: Optional: enable HTTP/3 in your web server/reverse proxy and make sure UDP port 443 is open in the firewall.

- **Cookie security** Recommended · Info

The homepage sets no cookies that could be assessed.

- **Mixed content** Required

The page loads no resources over unencrypted HTTP.

- **Subresource integrity** Recommended · Info

The page loads no external scripts/stylesheets where SRI would be relevant.