///\ mdn _

HTTP Observatory Report

Scan summary: www.tesla.com

| B |

Score: 70 / 100

Scan Time: 1 minute ago

Tests Passed: 8 / 10

↗ since

last scan

| Rescan |

Scan another website

Scan results

Scoring   CSP analysis   Raw server headers   Cookies   Scan history   Benchmark cor

Test   Content Security Policy (CSP)

Score   −25 ✖

Reason   Content Security Policy (CSP) header not implemented

Advice   Implement one, see MDN's Content Security Policy (CSP) documentation.

Test   Cookies

Score   −5 ✖

Reason   Cookies set without using the `Secure` flag, but transmission over HTTP prevented by HSTS.

Advice   Use `Secure` flag.

Test   Cross Origin Resource Sharing (CORS)

Score   0 ✔

Reason   Content is not visible via cross-origin resource sharing (CORS) files or headers.

Advice   None

Test   Redirection

Score   0 ✔

Reason   Initial redirection is to HTTPS on same host, final destination is HTTPS

Advice   None

Test   <u>Referrer Policy</u>

Score   -

Reason   `Referrer-Policy` header not implemented.

Advice   Set to `strict-origin-when-cross-origin` at a minimum.

Test   <u>Strict Transport Security (HSTS)</u>

Score   0 ✓

Reason   `Strict-Transport-Security` header set to a minimum of six months (15768000).

Advice   Consider preloading: this requires adding the `preload` and `includeSubDomains` directives and setting `max-age` to at least `31536000` (1 year), and submitting your site to <u>https://hstspreload.org/</u> .

Test   <u>Subresource Integrity</u>

Score   -

Reason   Subresource Integrity (SRI) not implemented, but all scripts are loaded from a similar origin.

Advice   Add SRI for bonus points.

Test   <u>X-Content-Type-Options</u>

Score   0 ✅

Reason   `X-Content-Type-Options` header set to `nosniff`.

Advice   None

Test   <u>X-Frame-Options</u>

Score   0 ✅

Reason   `X-Frame-Options` (XFO) header set to `SAMEORIGIN` or `DENY`.

Advice   Implement frame-ancestors CSP.

Test   <u>Cross Origin Resource Policy</u>

Score   -

Reason   Cross Origin Resource Policy (CORP) is not implemented (defaults to `cross-origin`).

Advice   None