



HTTP Observatory Report

[Report Feedback](#)

Scan summary: www.tesla.com



Score: 70 / 100
Scan Time: Just now
Tests Passed: 8 / 10

↗ since
last scan




Wait 32s to rescan

[Scan another website](#)

Scan results

- Scoring
- CSP analysis
- Raw server headers
- Cookies
- Scan history
- Benchmark ▲

Test	<u>Content Security Policy (CSP)</u>
Score	-25 ❌
Reason	Content Security Policy (CSP) header not implemented
Advice	Implement one, see <u>MDN's Content Security Policy (CSP) documentation</u> .
Test	<u>Cookies</u>
Score	-5 ❌

Reason	Cookies set without using the <code>secure</code> flag, but transmission over HTTP prevented by HSTS.
Advice	Use <code>secure</code> flag.
Test	<u>Cross Origin Resource Sharing (CORS)</u>
Score	0 
Reason	Content is not visible via cross-origin resource sharing (CORS) files or headers.
Advice	None
Test	<u>Redirection</u>
Score	0 
Reason	Initial redirection is to HTTPS on same host, final destination is HTTPS
Advice	None
Test	<u>Referrer Policy</u>
Score	-
Reason	<code>Referrer-Policy</code> header not implemented.
Advice	Set to <code>strict-origin-when-cross-origin</code> at a minimum.
Test	<u>Strict Transport Security (HSTS)</u>
Score	0 
Reason	<code>Strict-Transport-Security</code> header set to a minimum of six months (15768000).
Advice	Consider preloading: this requires adding the <code>preload</code> and <code>includeSubDomains</code> directives and setting <code>max-age</code> to at least 31536000 (1 year), and submitting your site to https://hstspreload.org/ .


Test Subresource Integrity

Score -

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

Advice Add SRI for bonus points.


Test X-Content-Type-Options

Score 0 

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

Advice None

Test X-Frame-Options

Score 0 

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

Advice Implement frame-ancestors CSP.

Test Cross Origin Resource Policy

Score -

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

Advice None