

# HTTP Observatory Report

[Report Feedback](#)

Scan summary: [www.apple.com](http://www.apple.com)

B

Score: 70 / 100

Scan Time: Just now

Tests Passed: 7 / 10


Wait 49s to rescan

[Scan another website](#)

## Scan results

[Scoring](#)
[CSP analysis](#)
[Cookies](#)
[Raw server headers](#)
[Scan history](#)
[Benchmark](#)

**Test** [Content Security Policy \(CSP\)](#)

**Score** -20 

**Reason** Content Security Policy (CSP) implemented unsafely. This includes `'unsafe-inline'` or `data:` inside `script-src`, overly broad sources such as `https:` inside `object-src` or `script-src`, or not restricting the sources for `object-src` or `script-src`.

**Advice** Remove `unsafe-inline` and `data:` from `script-src`, overly broad sources from `object-src` and `script-src`, and ensure `object-src` and `script-src` are set.

**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** Referrer Policy

**Score** -5 

**Reason** `Referrer-Policy` header set unsafely to `origin`, `origin-when-cross-origin`, `unsafe-url` or `no-referrer-when-downgrade`.

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

**Test** Strict Transport Security (HSTS)

**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 <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