

**Humble HTTP headers analyzer**  
(<https://github.com/rfc-st/humble>)

[0. Info]

Date : 2021/09/03 - 18:42:02  
Domain : <https://facebook.com>

[1. Missing HTTP Response Headers]

Clear-Site-Data

Clears browsing data (cookies, storage, cache) associated with the requesting website.  
Ref: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Clear-Site-Data>

Cross-Origin-Embedder-Policy

Prevents documents and workers from loading non-same-origin requests unless allowed.  
Ref: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cross-Origin-Embedder-Policy>

Cross-Origin-Opener-Policy

Prevent other websites from gaining arbitrary window references to a page.  
Ref: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cross-Origin-Opener-Policy>

Cross-Origin-Resource-Policy

Allows a resource owner to specify who can load the resource.  
Ref: [https://developer.mozilla.org/en-US/docs/Web/HTTP/Cross-Origin\\_Resource\\_Policy\\_\(CORP\)](https://developer.mozilla.org/en-US/docs/Web/HTTP/Cross-Origin_Resource_Policy_(CORP))

Expect-CT

Prevents the use of misissued certificates from going unnoticed.  
Ref: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Expect-CT>

NEL

Enables web applications to declare a reporting policy to report errors.  
Ref: <https://scotthelme.co.uk/network-error-logging-deep-dive/>

Permissions-Policy

Previously called "Feature-Policy", allow and deny the use of browser features.  
Ref: <https://scotthelme.co.uk/goodbye-feature-policy-and-hello-permissions-policy/>

Referrer-Policy

Controls how much referrer information should be included with requests.  
Ref: <https://scotthelme.co.uk/a-new-security-header-referrer-policy/>

[2. Fingerprint HTTP Response Headers]

Remove these headers (or modify their values), if they refer to actual software/versions:

Nothing to report, all seems OK!

**Humble HTTP headers analyzer**  
(<https://github.com/rfc-st/humble>)

[3. Insecure HTTP Response Headers Values]

All, or any, of the values in these headers could be considered insecure:

Content-Security-Policy

Remove 'unsafe-inline' and/or 'unsafe-eval' whenever possible.

Strict-Transport-Security

Add 'includeSubDomains' and define 'max-age' equal or greater than 31536000 (1 year).

[4. Empty HTTP Response Headers Values]

The following headers have no value (could be equivalent to as if they were not enabled):

Nothing to report, all seems OK!

.:

Analysis done in 0.65 seconds!.

.: