Humble HTTP headers analyzer

(https://github.com/rfc-st/humble)

[0. Info]

 Date : 2023/01/20 - 19:48:57
 URL : https://tesla.com

[1. Missing HTTP Security 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
 Protect servers against certain cross-origin or cross-site embedding of the returned source.
 Ref: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cross-Origin_Resource_Policy_(CORP)

 Content-Security-Policy
 Detect and mitigate Cross Site Scripting (XSS) and data injection attacks, among others.
 Ref: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy

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

 Pragma
 Used for backwards compatibility with HTTP/1.0 clients.
 Ref: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Pragma

 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]

 These headers can leak information about software, versions, hostnames or IP addresses:

 X-Drupal-Cache [Drupal Content Management System]

 MISS

 X-Drupal-Dynamic-Cache [Drupal Content Management System]
 MISS

 X-Generator [Generic Publishing Software]
 Drupal 9 (https://www.drupal.org)

 X-Varnish [Varnish HTTP accelerator]
 889464481 889495398

[3. Deprecated HTTP Response Headers/Protocols and Insecure Values]

 The following headers/protocols are deprecated or their values may be considered unsafe:

 Cache-Control (Recommended Values)
 Enable 'no-cache', 'no-store', and 'must-revalidate' if there are sensitive data.
 Ref: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control

 Etag (Potentially Unsafe Header)
 Although unlikely to be exploited, this header should not include inode information.
 Ref: https://www.pentestpartners.com/security-blog/vulnerabilities-that-arent-etag-headers/

 Set-Cookie (Insecure Attributes)
 Enable 'secure' and 'httponly': to send it via HTTPS and not be accessed by client APIs.
 Ref: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie

 Strict-Transport-Security (Recommended Values)
 Add 'includeSubDomains' and set 'max-age' to at least 31536000 (one year).
 Ref: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
 Ref: https://https.cio.gov/hsts/

 X-UA-compatible (Deprecated Header)
 Unless you need compatibility with very old versions of Internet Explorer (e.g. 6 to 8),
 remove this header and declare correctly the doctype.
 Ref: https://getoutofmyhead.dev/x-ua-compatible/

[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!

[5. Browser Compatibility for Enabled HTTP Security Headers]

Cache-Control: https://caniuse.com/?search=Cache-Control

Content-Type: https://caniuse.com/?search=Content-Type

Permissions-Policy: https://caniuse.com/?search=Permissions-Policy

Strict-Transport-Security: https://caniuse.com/?search=Strict-Transport-Security

X-Content-Type-Options: https://caniuse.com/?search=X-Content-Type-Options

X-Frame-Options: https://caniuse.com/?search=X-Frame-Options

.:

Analysis done in 2.71 seconds!.

  Missing headers: 8
  Fingerprint headers: 4
  Deprecated/Insecure headers: 5
  Empty headers: 0

.: