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

[0. Info]

Date : 2023/11/10 - 18:59:26
URL : https://www.spacex.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/

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/

X-Content-Type-Options
Indicate that MIME types in the "Content-Type" headers should be followed.
Ref: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options

X-Permitted-Cross-Domain-Policies

Limit which data external resources (e.g. Adobe Flash/PDF documents), can access on the domain.
Ref: https://owasp.org/www-project-secure-headers/#div-headers

X-Frame-Options
Prevents clickjacking attacks, limiting sources of embedded content.
Ref: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

[2. Fingerprint HTTP Response Headers]

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

Server [Generic HTTP Server/Content Delivery Network]
whydoyoucare?

Via [Generic Proxy server]
1.1 varnish, 1.1 varnish

X-Served-By [Generic HTTP Server/Content Delivery Network]
cache-bur-kbur8200135-BUR, cache-mad22080-MAD

[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/

Expires (Ignored Header)
Header ignored by the directives 'max-age' or 's-maxage' in in the header that controls the cache.
Ref: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Expires

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/

[4. Empty HTTP Response Headers Values]

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

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

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

.:

Analysis done in 0.38 seconds! (changes with respect to the last analysis in parentheses)

Missing headers:	11 (First Analysis)
Fingerprint headers:	3 (First Analysis)
Deprecated/Insecure headers:	4 (First Analysis)
Empty headers:	0 (First Analysis)
Warnings to review:	18 (First Analysis)