

[0. Info]

Date : 2026/06/13 - 18:36:11
URL : <https://samsung.com>
File : humble_https_samsung.com_20260613_183612_en.pdf

[1. Enabled HTTP Security Headers]

Content-Type: text/html; charset=UTF-8
Server-Timing: cdn-cache; desc=HIT, edge; dur=1, ak_p; desc="1781368573334_34893008_3930321228_248_14353_18_0_-";dur=1
Set-Cookie: device_type=pc; path=/; domain=.samsung.com
Strict-Transport-Security: max-age=31536000
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 0

[2. Missing HTTP Security Headers]

Cache-Control

Directives for caching in both requests and responses.

Ref: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Cache-Control>

Clear-Site-Data

Clears browsing data (cookies, storage, cache) associated with the requesting website.

Ref: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Clear-Site-Data>

Cross-Origin-Embedder-Policy

Prevents documents and workers from loading non-same-origin requests unless allowed.

Ref: <https://mdn.io/Cross-Origin-Embedder-Policy>

Cross-Origin-Opener-Policy

Prevent other websites from gaining arbitrary window references to a page.

Ref: <https://mdn.io/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/Guides/Cross-Origin_Resource_Policy

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/Reference/Headers/Content-Security-Policy>

Integrity-Policy

Blocks certain resource types without Subresource Integrity metadata.

Ref: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Integrity-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://mdn.io/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>

[3. Fingerprint HTTP Response Headers]

These headers can expose IPs, hostnames, software or their versions:

X-Akamai-Transformed (Akamai Edge)

Value: '9 - 0 pmb=mRUM,3'

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

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

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/>

Server-Timing (Potentially Unsafe Header)

This header should not expose sensitive application or infrastructure information.

Ref: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Server-Timing>

Set-Cookie (Insecure Attributes)

Review the cookie 'device_type'.

'Secure' and 'HttpOnly' must be set on any cookie associated with sensitive data.

Ref: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Set-Cookie>

Strict-Transport-Security (Recommended Values)

Add 'includeSubDomains' and 'max-age' (with 31536000 -one year- as minimum).

Ref: <https://https.cio.gov/hts/>

Ref: <https://mdn.io/Strict-Transport-Security>

Vary (Potentially Unsafe Header)

The values of this header may expose others, facilitating attacks if user input is accepted.

Ref: <https://www.yeswehack.com/fr/learn-bug-bounty/http-header-exploitation>

Ref: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Vary>

X-XSS-Protection (Deprecated Header)

This header is deprecated in the major web browsers.

Instead, enforce a strict "Content-Security-Policy" header.

Ref: <https://web.dev/articles/strict-csp>

Ref: https://developer.mozilla.org/en-US/docs/Web/HTTP/Guides/CSP#strict_csp

Ref: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/X-XSS-Protection>

Ref: https://developer.mozilla.org/en-US/docs/Web/Security/Practical_implementation_guides/CSP

[5. Empty HTTP Response Headers Values]

Empty HTTP headers (and are therefore considered disabled):

Nothing to report, all seems OK!

[6. Browser Compatibility for Enabled HTTP Security Headers]

Content-Type: <https://caniuse.com/?search=Content-Type>
ETag: <https://caniuse.com/?search=ETag>
Server-Timing: <https://caniuse.com/?search=Server-Timing>
Set-Cookie: <https://caniuse.com/?search=Set-Cookie>
Strict-Transport-Security: <https://caniuse.com/?search=Strict-Transport-Security>
Vary: <https://caniuse.com/?search=Vary>
X-Frame-Options: <https://caniuse.com/?search=X-Frame-Options>
X-XSS-Protection: <https://caniuse.com/?search=X-XSS-Protection>

[7. Analysis Results]

Done in 1.47 seconds! (changes with respect to the last analysis in parentheses)

Enabled headers: 6 (First Analysis)

Missing headers: 12 (First Analysis)

Fingerprint headers: 1 (First Analysis)

Deprecated/Insecure headers: 6 (First Analysis)

Empty headers: 0 (First Analysis)

Findings to review: 19 (First Analysis)

Analysis Grade: D (Review 'Deprecated/Insecure headers')

'(*)' meaning: Experimental HTTP response directive or header

'(*)' ref: https://mdn.io/Experimental_deprecated_obsolete

'(Not available)' meaning: The history file, analysis_h.txt, could not be accessed