# Wolf-Agents Security Report

## Web Security Check

Output: en / fr / 2026-10-05.2 · EU background and French CNIL guidance on data security; French rules implementing NIS/NIS2 are not covered. · Selected general source information; applicability has not been assessed. · Information checked: 2026-10-05

### Target

https://wolf-agents.com/
Scan time: 06 Oct 2026, 22:31 GMT+2 (Europe/Berlin)
Document generated on: 06 Oct 2026, 22:55 GMT+2 (Europe/Berlin)
The explanations in this report were created using AI. Available measurements were collected automatically; assessments follow fixed rules. About their creation: https://wolf-agents.com/ki-hinweis/#english
Measurement catalogue version: 1.9
Report presentation: 2026-10-05.legal-2
Scan ID: e6e4f987-06f1-473d-9a35-0ec5076cf172
Report model: 1.4
Confidentiality: for the recipient and third parties named by the recipient
Issued by: Wolf-Agents.com - kontakt@wolf-agents.com

### Overall picture

**A** 138 of 166 points - Very good

133 checks: 93 passed, 3 failed, 1 not assessable, 14 informational, 22 not applicable.
1 of 133 checks cannot be assessed conclusively from the saved findings. Unmeasured features do not count as confirmed protection. Unmeasured list features earn no points; the scoring scale stays unchanged. Header observations are assessed separately.

## Start here

Informational, not applicable and passed checks remain in the complete catalogue below. The IDs also identify sections in print.

**Confirmed negative findings**

cross-origin-opener-policy · failed · Cross-Origin Isolation (COOP)
cross-origin-embedder-policy · failed · Cross-Origin Embedder (COEP)
csp-unsafe-inline-style · failed · Inline CSS in style source lists

**Open / not assessable**

hsts_preload_pending · not assessable · HSTS preload application pending

**Additional legal information**

### Scope limits

- The check is unauthenticated and is performed exclusively from outside the system.
- Conservative passive check of this single address: measurements cover its HTTP response headers and redirect chain, TLS certificate, domain DNS records, the HSTS preload list and external resources embedded in the delivered HTML. No crawling of further pages, no login, no port scan and no active exploitation.
- This is not a penetration test. No vulnerability was actively exploited.
- No source code, infrastructure or process audit.
- A snapshot at the stated time. Subsequent changes are not captured.
- False findings are possible. Upstream CDN, WAF or rate-limiting systems may distort the result.
- Checks without evaluable measurement evidence, for example because a system was unreachable or unresponsive, are shown as “not assessable”, not as “passed”.

- This classification is general information and does not replace legal advice.
- Chromium reference list dated 2026-09-25 (revision 92802374ec24). Covered by the direct entry for wolf-agents.com. Pending inclusion and pending removal are not measured. Browser versions may use different lists; header observations are separate.
- Requested origin: https://wolf-agents.com. Final response origin: https://wolf-agents.com. Response headers, cookies, TLS, CSP and content observations apply to the final response; DNS and security.txt measurements apply to the requested host wolf-agents.com. The path did not change; path and query values are not duplicated in this scope record. Final response context: GET, status 200, media type text/html, measured at 2026-10-06T20:31:28.904Z.

Automated snapshot within the documented scope. Not an audit, certification or legal advice. Statutory rights remain unaffected. Measured on: 06 Oct 2026.

Evidence notation e1: original backslashes are doubled; \u{HEX} represents exactly one Unicode codepoint. Raw evidence explicitly represents every space, control, combining or unsupported character this way. No normalisation. Layout line breaks add no original character. CSV raw fields additionally preserve the complete evidence text; cookie values and local parts of email addresses are hidden as *** there as everywhere.

## Assessment scheme

The following scale applies only to failed checks, not to information, checks that cannot be assessed or non-applicable checks. The terms used for potential impact and response priority follow the BSI practical guide, version 1.2, section 4.1.3. The classification of scanner findings, points and grade follows our documented assessment method. These do not set legal deadlines. high = immediate, medium = short-term, low = medium-term, for information = long-term. Web finding interpretation 1.5, separate from the measurement catalogue. The corrected finding balance can differ from the saved rating. Inputs, scan time, points, denominator and stored grade remain unchanged; missing maximum points alone do not demonstrate a security defect. The Wolf-Agents methodology starts with 100 base points for eight selected headers and adds up to 66 bonus points. These are our own weights, not a general requirement under a standard, certification or a measured probability of harm. Optional measures depend on the application context. Bonuses count only from 80 base points. Deprecated headers and software disclosures may cause additional deductions. Unmeasured features are not treated as implemented protection. Comparisons require the same catalogue version and check scope; historical scores are not recalculated. Deliberately NO CVSS score is assigned - there is no authoritative CVSS rating for configuration findings, and a self-calculated number in the notation of a standard would claim a precision that does not exist.

BSI – Practical guide to information security penetration testing · v1.2 (2016-11), section 4.1.3, pp. 25–26 · checked 2026-10-05 · https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/Pentest_Webcheck/Leitfaden_Penetrationstest.pdf?__blob=publicationFile&v=3

**Status values per check:**

[+] passed - confirmed within the stated scope; no deviation demonstrated. [!] failed - finding present. [?] not assessable - no evaluable measurement evidence is available for this check; that is neither a positive nor a negative finding. The individual finding identifies a documented measurement limit or missing saved information. [i] Information - observed configuration signal without a demonstrated security defect. [-] not applicable - not applicable to the observed response context; not a passed security check.

# Baseline headers (Wolf-Agents assessment)

92 of 100 points

8 selected headers with a total of 100 base points.

### [+] content-security-policy · Protection against injected malicious code (XSS)

Status: passed | ID: content-security-policy | Rule weighting (not a current negative finding): Critical | Damage potential: high | Weight: 25 points

What is checked: Whether the response carries a Content-Security-Policy header, whether it is enforced or runs in report-only mode, and which directives it sets.

References: BSI APP.3.1.A21

References: W3C Content Security Policy Level 3 · https://www.w3.org/TR/CSP3/

References: BSI APP.3.1.A21 · Secure HTTP configuration, standard (S), module p. 5 · IT-Grundschutz, Edition 2023 (2023-02) · checked 5 October 2026 · https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium/IT_Grundschutz_Kompendium_Edition2023.pdf?__blob=publicationFile&v=4

## [+] strict-transport-security · Enforced encryption (HSTS)

Status: passed | ID: strict-transport-security | Rule weighting (not a current negative finding): Critical | Damage potential: high | Weight: 20 points

What is checked: Whether the response carries a Strict-Transport-Security header and which validity period, subdomain and preload settings it contains.

**Finding: After receiving a valid policy, supporting browsers can be required to use HTTPS by HSTS. The detailed analysis checks max-age and additional directives. A header request demonstrates neither coverage of all subdomains nor inclusion in every browser's preload list. Chromium reference list dated 2026-09-25 (revision 92802374ec24). Covered by the direct entry for wolf-agents.com. Pending inclusion and pending removal are not measured. Browser versions may use different lists; header observations are separate.**

Evidence:\u{20}max-age=63072000;\u{20}includeSubDomains;\u{20}preload

References: BSI APP.3.1.A21

References: RFC 6797: HTTP Strict Transport Security · https://www.rfc-editor.org/rfc/rfc6797

References: BSI APP.3.1.A21 · Secure HTTP configuration, standard (S), module p. 5 · IT-Grundschutz, Edition 2023 (2023-02) · checked 5 October 2026 · https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium/IT_Grundschutz_Kompendium_Edition2023.pdf?__blob=publicationFile&v=4

## [+] x-frame-options · Protection against clickjacking attacks

Status: passed | ID: x-frame-options | Rule weighting (not a current negative finding): Medium | Damage potential: medium | Weight: 15 points

What is checked: Which X-Frame-Options values are present, interpreted according to HTML and the precedence of enforced CSP frame-ancestors. No browser embedding test.

## [+] x-content-type-options · MIME type protection

Status: passed | ID: x-content-type-options | Rule weighting (not a current negative finding): Low | Damage potential: low | Weight: 10 points

What is checked: Whether the response carries an X-Content-Type-Options header and whether its value is nosniff — any other value has no effect.

References: BSI APP.3.1.A21

References: BSI APP.3.1.A21 · Secure HTTP configuration, standard (S), module p. 5 · IT-Grundschutz, Edition 2023 (2023-02) · checked 5 October 2026 · https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium/IT_Grundschutz_Kompendium_Edition2023.pdf?__blob=publicationFile&v=4

## [+] referrer-policy · Control over URL disclosure

Status: passed | ID: referrer-policy | Rule weighting (not a current negative finding): Low | Damage potential: low | Weight: 10 points

What is checked: Whether the response carries a Referrer-Policy header and how much of the originating URL its value passes on to third-party destinations.

## [+] permissions-policy · Browser API restrictions

Status: passed | ID: permissions-policy | Rule weighting (not a current negative finding): Low | Damage potential: low | Weight: 10 points

What is checked: Whether Permissions-Policy has valid dictionary syntax and empty or self-only allowlists for selected features. Browser enforcement, script inventory and required features are not measured.



Technical snapshot within the stated scope; no compliance attestation.

### [!] cross-origin-opener-policy · Cross-Origin Isolation (COOP)

Status: failed | ID: cross-origin-opener-policy | Severity: Low | Damage potential: low | Response: medium-term | Weight: 4 points

What is checked: Whether the response carries a Cross-Origin-Opener-Policy header and whether its value severs the connection to third-party windows that opened the page.

**Finding: The header is set but does not reach the full number of points — its configuration leaves gaps. What is missing is set out in the check aspects of this section.**

Evidence:\u{20}same-origin,\u{20}same-origin

Recommendation [cross-origin-opener-policy]: Consider COOP: same-origin when window relationships should be separated. Test SSO, payments and popups before enabling it; same-origin-allow-popups can preserve required integrations but does not establish cross-origin isolation.

### [!] cross-origin-embedder-policy · Cross-Origin Embedder (COEP)

Status: failed | ID: cross-origin-embedder-policy | Severity: Low | Damage potential: low | Response: medium-term | Weight: 4 points

What is checked: Whether the response carries a Cross-Origin-Embedder-Policy header and whether its value requires embedded resources to grant explicit permission.

**Finding: The header is set but does not reach the full number of points — its configuration leaves gaps. What is missing is set out in the check aspects of this section.**

Evidence:\u{20}credentialless,\u{20}credentialless

Recommendation [cross-origin-embedder-policy]: Set COEP only after assessing the need for isolation and all resource integrations: require-corp requires suitable CORS/CORP permissions; credentialless permits certain requests without credentials. Check the result in the browser together with COOP.

## Content Security Policy

7 of 19 points

12 hardening features with a total of 19 bonus points, plus 15 checks assessing the content of the configuration.

### [i] csp_strict_dynamic · CSP strict-dynamic

Status: Information | ID: csp_strict_dynamic | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 2 points

What is checked: CSP strict-dynamic

**Finding: This hardening feature is not implemented. It is not a defect in the narrow sense, but an additional measure that is still open.**

Recommendation [csp_strict_dynamic]: If appropriate for this application: Use script-src 'strict-dynamic'

### [i] csp_nonces · CSP nonces

Status: Information | ID: csp_nonces | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 2 points

What is checked: CSP nonces

**Finding: This hardening feature is not implemented. It is not a defect in the narrow sense, but an additional measure that is still open.**

Recommendation [csp_nonces]: If appropriate for this application: Use nonces for inline scripts

### [i] csp_hashes · CSP hashes

Status: Information | ID: csp_hashes | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 2 points

What is checked: CSP hashes

**Finding: This hardening feature is not implemented. It is not a defect in the narrow sense, but an additional measure that is still open.**

Recommendation [csp_hashes]: If appropriate for this application: SHA hashes for inline scripts



Technical snapshot within the stated scope; no compliance attestation.

### [+] csp_default_none · CSP default-src: none

Status: passed | ID: csp_default_none | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 2 points

What is checked: CSP default-src: none

### [+] csp_object_none · CSP object-src: none

Status: passed | ID: csp_object_none | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 1 point

What is checked: CSP object-src: none

### [+] csp_base_uri · CSP base-uri restricted

Status: passed | ID: csp_base_uri | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 1 point

What is checked: CSP base-uri restricted

### [+] csp_frame_ancestors · CSP frame-ancestors

Status: passed | ID: csp_frame_ancestors | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 1 point

What is checked: CSP frame-ancestors

### [+] csp_form_action · CSP form-action

Status: passed | ID: csp_form_action | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 1 point

What is checked: CSP form-action

### [+] csp_upgrade_insecure · CSP upgrade-insecure-requests

Status: passed | ID: csp_upgrade_insecure | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 1 point

What is checked: CSP upgrade-insecure-requests

### [i] csp_reporting · CSP reporting (report-uri)

Status: Information | ID: csp_reporting | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 1 point

What is checked: CSP reporting (report-uri)

**Finding: This hardening feature is not implemented. It is not a defect in the narrow sense, but an additional measure that is still open.**

Recommendation [csp_reporting]: If appropriate for this application: report-uri directive for violation reports

### [i] csp_report_to · Modern CSP reporting (report-to)

Status: Information | ID: csp_report_to | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 2 points

What is checked: Modern CSP reporting (report-to)

**Finding: This hardening feature is not implemented. It is not a defect in the narrow sense, but an additional measure that is still open.**

Recommendation [csp_report_to]: If appropriate for this application: report-to directive (Reporting API v1)

### [i] csp_trusted_types · Trusted Types

Status: Information | ID: csp_trusted_types | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 3 points

What is checked: Trusted Types

**Finding: This hardening feature is not implemented. It is not a defect in the narrow sense, but an additional measure that is still open.**

Recommendation [csp_trusted_types]: If appropriate for this application: require-trusted-types-for 'script' restricts supported DOM interfaces; safe Trusted Type policies remain necessary



Technical snapshot within the stated scope; no compliance attestation.

### [+] csp-nur-report-only · Enforcement mode of the policy

Status: passed | ID: csp-nur-report-only | Rule weighting (not a current negative finding): Flagged | Damage potential: medium | Weight: 0 points

What is checked: Enforcement mode of the policy

### [+] csp-unsafe-inline-script · Inline scripts in script-src

Status: passed | ID: csp-unsafe-inline-script | Rule weighting (not a current negative finding): High | Damage potential: high | Weight: 0 points

What is checked: Inline scripts in script-src

### [+] csp-unsafe-eval · Dynamic code evaluation in script-src

Status: passed | ID: csp-unsafe-eval | Rule weighting (not a current negative finding): Medium | Damage potential: medium | Weight: 0 points

What is checked: Dynamic code evaluation in script-src

### [+] csp-wasm-unsafe-eval · WebAssembly compilation in script-src

Status: passed | ID: csp-wasm-unsafe-eval | Rule weighting (not a current negative finding): Low | Damage potential: low | Weight: 0 points

What is checked: WebAssembly compilation in script-src

### [+] csp-unsafe-hashes · Hash allowance for event handler attributes

Status: passed | ID: csp-unsafe-hashes | Rule weighting (not a current negative finding): Medium | Damage potential: medium | Weight: 0 points

What is checked: Hash allowance for event handler attributes

### [+] csp-breite-quelle-script · Broad source entries in script-src

Status: passed | ID: csp-breite-quelle-script | Rule weighting (not a current negative finding): High | Damage potential: high | Weight: 0 points

What is checked: Broad source entries in script-src

### [+] csp-default-src-wildcard · Wildcard as default-src

Status: passed | ID: csp-default-src-wildcard | Rule weighting (not a current negative finding): Critical | Damage potential: high | Weight: 0 points

What is checked: Wildcard as default-src

### [+] csp-http-schema · Unencrypted http: scheme as a source

Status: passed | ID: csp-http-schema | Rule weighting (not a current negative finding): High | Damage potential: high | Weight: 0 points

What is checked: Unencrypted http: scheme as a source

### [+] csp-data-uri-script · data: URIs in script-src

Status: passed | ID: csp-data-uri-script | Rule weighting (not a current negative finding): Medium | Damage potential: medium | Weight: 0 points

What is checked: data: URIs in script-src



Technical snapshot within the stated scope; no compliance attestation.

### [!] csp-unsafe-inline-style · Inline CSS in style source lists

Status: failed | ID: csp-unsafe-inline-style | Severity: Low | Damage potential: low | Response: medium-term | Weight: 0 points

What is checked: Inline CSS in style source lists

**Finding: The saved enforced policies permit arbitrary inline CSS in: style-src-elem, style-src-attr. An effective 'unsafe-inline' allowance was recorded. This is a header configuration finding, not evidence of an attack. It does not establish whether attacker-controlled HTML or CSS can enter this application.**

Evidence:\u{20}Content-Security-Policy\u{20}[1]:\u{20}style-src-elem\u{20}->\u{20}style-src:\u{20}'self'\u{20}'unsafe-inline'\u{A}Content-Security-Policy\u{20}[1]:\u{20}style-src-attr\u{20}->\u{20}style-src:\u{20}'self'\u{20}'unsafe-inline'

Recommendation [csp-unsafe-inline-style]: If arbitrary inline CSS is unnecessary, remove 'unsafe-inline' from the effective style source lists after testing the application. For required <style> elements, use an unpredictable nonce generated for each response or an exact content hash. Nonces do not authorise style attributes: prefer CSS classes; consider exact attribute hashes with 'unsafe-hashes' only after assessing compatibility and reuse risks. Configure style-src-elem and style-src-attr deliberately; changing a default-src fallback also affects other resource types. Check all enforced policies together. Report-Only policies only report; test behaviour before deliberately enforcing a policy.

### [+] csp-blob-uri-script · blob: URIs in script-src

Status: passed | ID: csp-blob-uri-script | Rule weighting (not a current negative finding): Low | Damage potential: low | Weight: 0 points

What is checked: blob: URIs in script-src

### [+] csp-default-src-fehlt · Script restrictions through script-src, script-src-elem or default-src

Status: passed | ID: csp-default-src-fehlt | Rule weighting (not a current negative finding): Medium | Damage potential: medium | Weight: 0 points

What is checked: Script restrictions through script-src, script-src-elem or default-src

### [+] csp-object-src-offen · Embedding via object-src

Status: passed | ID: csp-object-src-offen | Rule weighting (not a current negative finding): Low | Damage potential: low | Weight: 0 points

What is checked: Embedding via object-src

### [+] csp-base-uri-fehlt · Restriction of base-uri

Status: passed | ID: csp-base-uri-fehlt | Rule weighting (not a current negative finding): Low | Damage potential: low | Weight: 0 points

What is checked: Restriction of base-uri

### [+] csp-frame-ancestors-wirkungslos · Effectiveness of frame-ancestors

Status: passed | ID: csp-frame-ancestors-wirkungslos | Rule weighting (not a current negative finding): Medium | Damage potential: medium | Weight: 0 points

What is checked: Effectiveness of frame-ancestors

## HTTP Strict Transport Security

5 of 5 points

5 hardening features with a total of 5 bonus points, plus 8 checks assessing the content of the configuration.

### [+] hsts_max_age · HSTS max-age >= 1 year

Status: passed | ID: hsts_max_age | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 1 point

What is checked: HSTS max-age >= 1 year



Technical snapshot within the stated scope; no compliance attestation.

### [+] hsts_subdomains · HSTS includeSubDomains

Status: passed | ID: hsts_subdomains | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 1 point

What is checked: HSTS includeSubDomains

### [+] hsts_preload_flag · HSTS preload flag

Status: passed | ID: hsts_preload_flag | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 1 point

What is checked: HSTS preload flag

### [+] hsts_preload_list · HSTS preload list

Status: passed | ID: hsts_preload_list | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 2 points

What is checked: HSTS preload list

**Finding: Chromium reference list dated 2026-09-25 (revision 92802374ec24). Covered by the direct entry for wolf-agents.com. Pending inclusion and pending removal are not measured. Browser versions may use different lists; header observations are separate.**

### [?] hsts_preload_pending · HSTS preload application pending

Status: not assessable | ID: hsts_preload_pending | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 1 point

What is checked: HSTS preload application pending

Chromium reference list dated 2026-09-25 (revision 92802374ec24). Covered by the direct entry for wolf-agents.com. Pending inclusion and pending removal are not measured. Browser versions may use different lists; header observations are separate.

### [+] hsts-max-age-fehlt · Valid HSTS syntax and max-age

Status: passed | ID: hsts-max-age-fehlt | Rule weighting (not a current negative finding): Critical | Damage potential: high | Weight: 0 points

What is checked: Valid HSTS syntax and max-age

### [+] hsts-max-age-null · max-age=0 as an opt-out from HSTS protection

Status: passed | ID: hsts-max-age-null | Rule weighting (not a current negative finding): Critical | Damage potential: high | Weight: 0 points

What is checked: max-age=0 as an opt-out from HSTS protection

### [+] hsts-max-age-zu-kurz · Length of the HSTS validity period

Status: passed | ID: hsts-max-age-zu-kurz | Rule weighting (not a current negative finding): High | Damage potential: high | Weight: 0 points

What is checked: Length of the HSTS validity period

### [+] hsts-subdomains-fehlt · Coverage of subdomains

Status: passed | ID: hsts-subdomains-fehlt | Rule weighting (not a current negative finding): Medium | Damage potential: medium | Weight: 0 points

What is checked: Coverage of subdomains

### [+] hsts-preload-status-ungeprueft · Usability of the local reference snapshot

Status: passed | ID: hsts-preload-status-ungeprueft | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 0 points

What is checked: Usability of the local reference snapshot

### [+] hsts-preload-max-age-zu-kurz · Preload requirement: validity period

Status: passed | ID: hsts-preload-max-age-zu-kurz | Rule weighting (not a current negative finding): High | Damage potential: high | Weight: 0 points

What is checked: Preload requirement: validity period

### [+] hsts-preload-subdomains-fehlt · Preload requirement: subdomains

Status: passed | ID: hsts-preload-subdomains-fehlt | Rule weighting (not a current negative finding): High | Damage potential: high | Weight: 0 points

What is checked: Preload requirement: subdomains



Technical snapshot within the stated scope; no compliance attestation.

### [+] hsts-preload-ohne-header · Header while a preload entry exists

Status: passed | ID: hsts-preload-ohne-header | Rule weighting (not a current negative finding): Flagged | Damage potential: medium | Weight: 0 points

What is checked: Header while a preload entry exists

## Cookie security

4 of 4 points

5 hardening features with a total of 4 bonus points, plus 10 checks assessing the content of the configuration.

Cookie observations cover the captured HTTP redirect and final responses. Other pages, JavaScript, consent and login workflows, and browser storage were not checked.

### [-] cookies_all_secure · All cookies Secure

Status: not applicable | ID: cookies_all_secure | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 1 point

What is checked: All cookies Secure

No cookies were identified in the captured HTTP redirect and final responses. Cookie attributes are therefore not applicable to this observation; no attribute check was passed. There is no recommendation to create cookies.

### [-] cookies_all_httponly · All cookies HttpOnly

Status: not applicable | ID: cookies_all_httponly | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 1 point

What is checked: All cookies HttpOnly

No cookies were identified in the captured HTTP redirect and final responses. Cookie attributes are therefore not applicable to this observation; no attribute check was passed. There is no recommendation to create cookies.

### [-] cookies_all_samesite_strict · All cookies SameSite=Strict

Status: not applicable | ID: cookies_all_samesite_strict | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 1 point

What is checked: All cookies SameSite=Strict

No cookies were identified in the captured HTTP redirect and final responses. Cookie attributes are therefore not applicable to this observation; no attribute check was passed. There is no recommendation to create cookies.

### [-] cookies_host_prefix · Cookie __Host- prefix

Status: not applicable | ID: cookies_host_prefix | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 1 point

What is checked: Cookie __Host- prefix

No cookies were identified in the captured HTTP redirect and final responses. Cookie attributes are therefore not applicable to this observation; no attribute check was passed. There is no recommendation to create cookies.

### [+] no_cookies_data_minimization · Data minimisation (no cookies)

Status: passed | ID: no_cookies_data_minimization | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 4 points

What is checked: Data minimisation (no cookies)

**Finding: No cookies were identified in the captured HTTP redirect and final responses. Cookie observations cover the captured HTTP redirect and final responses. Other pages, JavaScript, consent and login workflows, and browser storage were not checked.**

### [-] cookie-session-ohne-secure · Secure flag on session cookies

Status: not applicable | ID: cookie-session-ohne-secure | Rule weighting (not a current negative finding): Critical | Damage potential: high | Weight: 0 points

What is checked: Secure flag on session cookies

No cookies were identified in the captured HTTP redirect and final responses. Cookie attributes are therefore not applicable to this observation; no attribute check was passed. There is no recommendation to create cookies.

### [-] cookie-session-ohne-httponly · HttpOnly flag on session cookies

Status: not applicable | ID: cookie-session-ohne-httponly | Rule weighting (not a current negative finding): High | Damage potential: high | Weight: 0 points

What is checked: HttpOnly flag on session cookies

No cookies were identified in the captured HTTP redirect and final responses. Cookie attributes are therefore not applicable to this observation; no attribute check was passed. There is no recommendation to create cookies.

### [-] cookie-session-ohne-samesite · SameSite attribute on session cookies

Status: not applicable | ID: cookie-session-ohne-samesite | Rule weighting (not a current negative finding): Medium | Damage potential: medium | Weight: 0 points

What is checked: SameSite attribute on session cookies

No cookies were identified in the captured HTTP redirect and final responses. Cookie attributes are therefore not applicable to this observation; no attribute check was passed. There is no recommendation to create cookies.

### [-] cookie-session-samesite-none-ohne-secure · SameSite=None on session cookies without Secure

Status: not applicable | ID: cookie-session-samesite-none-ohne-secure | Rule weighting (not a current negative finding): High | Damage potential: high | Weight: 0 points

What is checked: SameSite=None on session cookies without Secure

No cookies were identified in the captured HTTP redirect and final responses. Cookie attributes are therefore not applicable to this observation; no attribute check was passed. There is no recommendation to create cookies.

### [-] cookie-ohne-secure · Secure flag on the remaining cookies

Status: not applicable | ID: cookie-ohne-secure | Rule weighting (not a current negative finding): Low | Damage potential: low | Weight: 0 points

What is checked: Secure flag on the remaining cookies

No cookies were identified in the captured HTTP redirect and final responses. Cookie attributes are therefore not applicable to this observation; no attribute check was passed. There is no recommendation to create cookies.

### [-] cookie-samesite-none-ohne-secure · SameSite=None on the remaining cookies without Secure

Status: not applicable | ID: cookie-samesite-none-ohne-secure | Rule weighting (not a current negative finding): Medium | Damage potential: medium | Weight: 0 points

What is checked: SameSite=None on the remaining cookies without Secure

No cookies were identified in the captured HTTP redirect and final responses. Cookie attributes are therefore not applicable to this observation; no attribute check was passed. There is no recommendation to create cookies.



Technical snapshot within the stated scope; no compliance attestation.

### [-] cookie-host-prefix-ohne-secure · __Host- prefix: Secure flag

Status: not applicable | ID: cookie-host-prefix-ohne-secure | Rule weighting (not a current negative finding): Medium | Damage potential: medium | Weight: 0 points

What is checked: __Host- prefix: Secure flag

No cookies were identified in the captured HTTP redirect and final responses. Cookie attributes are therefore not applicable to this observation; no attribute check was passed. There is no recommendation to create cookies.

### [-] cookie-host-prefix-falscher-pfad · __Host- prefix: path setting

Status: not applicable | ID: cookie-host-prefix-falscher-pfad | Rule weighting (not a current negative finding): Low | Damage potential: low | Weight: 0 points

What is checked: __Host- prefix: path setting

No cookies were identified in the captured HTTP redirect and final responses. Cookie attributes are therefore not applicable to this observation; no attribute check was passed. There is no recommendation to create cookies.

### [-] cookie-host-prefix-mit-domain · __Host- prefix: Domain attribute

Status: not applicable | ID: cookie-host-prefix-mit-domain | Rule weighting (not a current negative finding): Low | Damage potential: low | Weight: 0 points

What is checked: __Host- prefix: Domain attribute

No cookies were identified in the captured HTTP redirect and final responses. Cookie attributes are therefore not applicable to this observation; no attribute check was passed. There is no recommendation to create cookies.

### [-] cookie-secure-prefix-ohne-secure · __Secure- prefix: Secure flag

Status: not applicable | ID: cookie-secure-prefix-ohne-secure | Rule weighting (not a current negative finding): Medium | Damage potential: medium | Weight: 0 points

What is checked: __Secure- prefix: Secure flag

No cookies were identified in the captured HTTP redirect and final responses. Cookie attributes are therefore not applicable to this observation; no attribute check was passed. There is no recommendation to create cookies.

## Subresource Integrity

3 of 3 points

3 hardening features with a total of 3 bonus points, plus 7 checks assessing the content of the configuration.

### [-] sri_all_cdn · All CDN resources with SRI

Status: not applicable | ID: sri_all_cdn | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 2 points

What is checked: All CDN resources with SRI

No external scripts or stylesheets were identified in the analysed HTML. Resource integrity and integration criteria are not applicable to this observation; no resource attribute check was passed. Dynamic loading was not checked.

### [-] sri_all_external · SRI configuration on identified third-party resources

Status: not applicable | ID: sri_all_external | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 1 point

What is checked: SRI configuration on identified third-party resources

No external scripts or stylesheets were identified in the analysed HTML. Resource integrity and integration criteria are not applicable to this observation; no resource attribute check was passed. Dynamic loading was not checked.

### [+] sri_self_hosted · No third-party scripts/styles in the HTML examined

Status: passed | ID: sri_self_hosted | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 3 points

What is checked: No third-party scripts/styles in the HTML examined

### [-] sri-cdn-ungeschuetzt · Integrity protection of embedded CDN files

Status: not applicable | ID: sri-cdn-ungeschuetzt | Rule weighting (not a current negative finding): High | Damage potential: high | Weight: 0 points

What is checked: Integrity protection of embedded CDN files

No external scripts or stylesheets were identified in the analysed HTML. Resource integrity and integration criteria are not applicable to this observation; no resource attribute check was passed. Dynamic loading was not checked.

### [-] sri-integrity-ohne-crossorigin · Effectiveness of the integrity attributes that are set

Status: not applicable | ID: sri-integrity-ohne-crossorigin | Rule weighting (not a current negative finding): High | Damage potential: high | Weight: 0 points

What is checked: Effectiveness of the integrity attributes that are set

No external scripts or stylesheets were identified in the analysed HTML. Resource integrity and integration criteria are not applicable to this observation; no resource attribute check was passed. Dynamic loading was not checked.

### [-] sri-ohne-cdn-zuordnung · External embeds outside known CDN domains

Status: not applicable | ID: sri-ohne-cdn-zuordnung | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 0 points

What is checked: External embeds outside known CDN domains

No external scripts or stylesheets were identified in the analysed HTML. Resource integrity and integration criteria are not applicable to this observation; no resource attribute check was passed. Dynamic loading was not checked.

### [-] sri-host-ohne-sri · Hosts flagged for SRI compatibility review

Status: not applicable | ID: sri-host-ohne-sri | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 0 points

What is checked: Hosts flagged for SRI compatibility review

No external scripts or stylesheets were identified in the analysed HTML. Resource integrity and integration criteria are not applicable to this observation; no resource attribute check was passed. Dynamic loading was not checked.

### [+] sri-html-gekuerzt · Completeness of the page source that was evaluated

Status: passed | ID: sri-html-gekuerzt | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 0 points

What is checked: Completeness of the page source that was evaluated

### [+] sri-einbindungen-gekuerzt · Completeness of the embeds that were assessed

Status: passed | ID: sri-einbindungen-gekuerzt | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 0 points

What is checked: Completeness of the embeds that were assessed

### [+] sri-quelltext-fehlt · Availability of the page source for the SRI check

Status: passed | ID: sri-quelltext-fehlt | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 0 points

What is checked: Availability of the page source for the SRI check

---



Technical snapshot within the stated scope; no compliance attestation.

## HTTPS redirects

3 of 3 points

4 hardening features with a total of 3 bonus points, plus 7 checks assessing the content of the configuration.

### [+] redirect_https_only · Direct HTTPS

Status: passed | ID: redirect_https_only | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 1 point

What is checked: Direct HTTPS

### [+] redirect_single · Clean HTTP-to-HTTPS redirect

Status: passed | ID: redirect_single | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 1 point

What is checked: Clean HTTP-to-HTTPS redirect

### [+] redirect_www_normalized · WWW normalisation

Status: passed | ID: redirect_www_normalized | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 1 point

What is checked: WWW normalisation

### [-] redirect_www_not_applicable · No www alias present

Status: not applicable | ID: redirect_www_not_applicable | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 1 point

What is checked: No www alias present

A normalised www alias was recorded. The no-alias bonus is an alternative, not an additional missing measure.

### [+] redirect-kein-https-upgrade · Automatic redirect from HTTP to HTTPS

Status: passed | ID: redirect-kein-https-upgrade | Rule weighting (not a current negative finding): High | Damage potential: high | Weight: 0 points

What is checked: Automatic redirect from HTTP to HTTPS

### [+] redirect-http-ohne-weiterleitung · Reachability over unencrypted HTTP

Status: passed | ID: redirect-http-ohne-weiterleitung | Rule weighting (not a current negative finding): High | Damage potential: high | Weight: 0 points

What is checked: Reachability over unencrypted HTTP

### [+] redirect-http-hop · Encryption of every intermediate step in the redirect chain

Status: passed | ID: redirect-http-hop | Rule weighting (not a current negative finding): High | Damage potential: high | Weight: 0 points

What is checked: Encryption of every intermediate step in the redirect chain

### [+] redirect-temporaer · Permanence of the HTTPS redirect

Status: passed | ID: redirect-temporaer | Rule weighting (not a current negative finding): Low | Damage potential: low | Weight: 0 points

What is checked: Permanence of the HTTPS redirect

### [+] redirect-kette-zu-lang · Length of the redirect chain

Status: passed | ID: redirect-kette-zu-lang | Rule weighting (not a current negative finding): Low | Damage potential: low | Weight: 0 points

What is checked: Length of the redirect chain

### [+] redirect-kette-mehrfach · Number of redirects below the deduction threshold

Status: passed | ID: redirect-kette-mehrfach | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 0 points

What is checked: Number of redirects below the deduction threshold

### [+] redirect-kette-abgeschnitten · Completeness of the redirect chain recorded

Status: passed | ID: redirect-kette-abgeschnitten | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 0 points

What is checked: Completeness of the redirect chain recorded



Technical snapshot within the stated scope; no compliance attestation.

## Cross-Origin Headers

0 of 7 points

6 hardening features with a total of 7 bonus points.

Header configuration only: crossOriginIsolated, resource and embedding success, and separate processes were not measured.

### [i] cross_origin_coop · Cross-Origin-Opener-Policy

Status: Information | ID: cross_origin_coop | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 2 points

What is checked: Cross-Origin-Opener-Policy

**Finding: This hardening feature is not implemented. It is not a defect in the narrow sense, but an additional measure that is still open.**

Recommendation [cross_origin_coop]: If appropriate for this application: COOP: same-origin

### [i] cross_origin_coep · Cross-Origin-Embedder-Policy

Status: Information | ID: cross_origin_coep | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 2 points

What is checked: Cross-Origin-Embedder-Policy

**Finding: This hardening feature is not implemented. It is not a defect in the narrow sense, but an additional measure that is still open.**

Recommendation [cross_origin_coep]: If appropriate for this application: COEP: require-corp

### [i] cross_origin_corp_same_origin · CORP: same-origin

Status: Information | ID: cross_origin_corp_same_origin | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 2 points

What is checked: CORP: same-origin

**Finding: The saved CORP header does not contain one valid CORP value.**

Evidence:\u{20}same-origin,\u{20}same-origin

Recommendation [cross_origin_corp_same_origin]: If CORP is appropriate for these resources, choose one value that permits the required no-cors integrations: same-origin, same-site or cross-origin. Do not combine these values; test the required integrations.

### [i] cross_origin_corp_same_site · CORP: same-site

Status: Information | ID: cross_origin_corp_same_site | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 1 point

What is checked: CORP: same-site

**Finding: The saved CORP header does not contain one valid CORP value.**

Evidence:\u{20}same-origin,\u{20}same-origin

Recommendation [cross_origin_corp_same_site]: If CORP is appropriate for these resources, choose one value that permits the required no-cors integrations: same-origin, same-site or cross-origin. Do not combine these values; test the required integrations.

### [i] cross_origin_corp_cross_origin · CORP: cross-origin

Status: Information | ID: cross_origin_corp_cross_origin | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 1 point

What is checked: CORP: cross-origin

**Finding: The saved CORP header does not contain one valid CORP value.**

Evidence:\u{20}same-origin,\u{20}same-origin

Recommendation [cross_origin_corp_cross_origin]: If CORP is appropriate for these resources, choose one value that permits the required no-cors integrations: same-origin, same-site or cross-origin. Do not combine these values; test the required integrations.



Technical snapshot within the stated scope; no compliance attestation.

### [i] cross_origin_isolated · Headers for cross-origin isolation

Status: Information | ID: cross_origin_isolated | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 1 point

What is checked: Headers for cross-origin isolation

**Finding: This hardening feature is not implemented. It is not a defect in the narrow sense, but an additional measure that is still open.**

Recommendation [cross_origin_isolated]: If appropriate for this application: If cross-origin isolation is required, configure suitable COOP/COEP values and check crossOriginIsolated and integrations in the browser.

## Security Reporting

4 of 5 points

4 hardening features with a total of 5 bonus points.

Configuration bonuses record non-empty Report-To, NEL or Reporting-Endpoints headers and Origin-Agent-Cluster: ?1. Endpoint syntax, delivery, browser state and process separation were not measured.

### [+] reporting_report_to · Report-To header

Status: passed | ID: reporting_report_to | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 1 point

What is checked: Report-To header

### [+] reporting_nel · Network Error Logging

Status: passed | ID: reporting_nel | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 2 points

What is checked: Network Error Logging

### [i] reporting_endpoints · Reporting-Endpoints header

Status: Information | ID: reporting_endpoints | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 1 point

What is checked: Reporting-Endpoints header

**Finding: This hardening feature is not implemented. It is not a defect in the narrow sense, but an additional measure that is still open.**

Recommendation [reporting_endpoints]: If appropriate for this application: Modern reporting standard (W3C Reporting API)

### [+] origin_agent_cluster · Origin-Agent-Cluster

Status: passed | ID: origin_agent_cluster | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 1 point

What is checked: Origin-Agent-Cluster

## DNSSEC

5 of 5 points

4 hardening features with a total of 5 bonus points, plus 10 checks assessing the content of the configuration.

CAA quality describes the assessed records, not specific CA authorisation. issuewild applies only to wildcard certificates and overrides issue for that scope. Issuer-specific parameters and full alias/parent paths were not evaluated.

### [+] dnssec_validated · DNSSEC validated

Status: passed | ID: dnssec_validated | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 2 points

What is checked: DNSSEC validated



Technical snapshot within the stated scope; no compliance attestation.

### [-] dnssec_enabled · DNSSEC enabled (partially)

Status: not applicable | ID: dnssec_enabled | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 1 point

What is checked: DNSSEC enabled (partially)

DNSSEC was validated. The partial DNSSEC bonus is an alternative and is not an additional missing improvement.

### [+] caa_records · CAA issue/issuewild records

Status: passed | ID: caa_records | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 2 points

What is checked: CAA issue/issuewild records

### [+] caa_iodef · CAA iodef reporting

Status: passed | ID: caa_iodef | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 1 point

What is checked: CAA iodef reporting

### [+] caa-keine-records · CAA records restricting certificate issuance

Status: passed | ID: caa-keine-records | Rule weighting (not a current negative finding): Low | Damage potential: low | Weight: 0 points

What is checked: CAA records restricting certificate issuance

### [+] caa-nicht-parsebar · Formal validity of the CAA records

Status: passed | ID: caa-nicht-parsebar | Rule weighting (not a current negative finding): Flagged | Damage potential: medium | Weight: 0 points

What is checked: Formal validity of the CAA records

### [+] caa-syntax-ungueltig · Syntax of the assessed CAA properties

Status: passed | ID: caa-syntax-ungueltig | Rule weighting (not a current negative finding): Flagged | Damage potential: medium | Weight: 0 points

What is checked: Syntax of the assessed CAA properties

### [+] caa-kritische-eigenschaft · Assessment of critical CAA properties

Status: passed | ID: caa-kritische-eigenschaft | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 0 points

What is checked: Assessment of critical CAA properties

### [i] caa-kein-issuewild · Separate rule for wildcard certificates

Status: Information | ID: caa-kein-issuewild | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 0 points

What is checked: Separate rule for wildcard certificates

**Finding: Wildcard issuance follows the issue policy (no separate issuewild record present)**

### [+] caa-kein-iodef · Reporting address for rejected certificate requests

Status: passed | ID: caa-kein-iodef | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 0 points

What is checked: Reporting address for rejected certificate requests

### [+] caa-nicht-pruefbar · Reachability of the CAA query

Status: passed | ID: caa-nicht-pruefbar | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 0 points

What is checked: Reachability of the CAA query

### [+] dnssec-nicht-aktiviert · Signing of the DNS records (DNSSEC)

Status: passed | ID: dnssec-nicht-aktiviert | Rule weighting (not a current negative finding): Low | Damage potential: low | Weight: 0 points

What is checked: Signing of the DNS records (DNSSEC)



Technical snapshot within the stated scope; no compliance attestation.

### [+] dnssec-validierung-unvollstaendig · Completeness of the DNSSEC chain of trust

Status: passed | ID: dnssec-validierung-unvollstaendig | Rule weighting (not a current negative finding): Flagged | Damage potential: medium | Weight: 0 points

What is checked: Completeness of the DNSSEC chain of trust

### [+] dnssec-nicht-pruefbar · Reachability of the DNSSEC query

Status: passed | ID: dnssec-nicht-pruefbar | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 0 points

What is checked: Reachability of the DNSSEC query

## SSL/TLS encryption

2 of 2 points

1 hardening feature with a total of 2 bonus points.

Certificate validity at scan time 2026-10-06T20:31:28.405Z: notBefore 2026-09-12T13:23:06.000Z; notAfter 2026-12-11T13:23:05.000Z.

Remaining validity at measurement: 65 days 16 hours. Renewal was not observed.

CA/B conformity was not determined: issuance time and public-PKI scope were not verified. The staged limits apply to newly issued public TLS certificates; they are not a general private-PKI rule.

The listed TLS protocol criterion was met. Additional certificate findings and measurement limits are stated above.

### [+] ssl_tls13 · TLS 1.3

Status: passed | ID: ssl_tls13 | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 2 points

What is checked: TLS 1.3

## Cache-Control (BSI)

8 of 8 points

5 hardening features with a total of 8 bonus points, plus 5 checks assessing the content of the configuration.

The sensitivity and intended cache behaviour of this response were not determined. Public/CDN content does not generally require no-store, private; the existing bonuses describe selected directives, not universal obligations.

All checks in the “Cache-Control (BSI)” group were met; no deficiency was found in this area.

### [+] cache_present · Cache-Control header

Status: passed | ID: cache_present | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 3 points

What is checked: Cache-Control header

### [+] cache_no_store · no-store directive

Status: passed | ID: cache_no_store | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 2 points

What is checked: no-store directive

### [+] cache_private · private directive

Status: passed | ID: cache_private | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 1 point

What is checked: private directive

### [+] cache_must_revalidate · must-revalidate directive

Status: passed | ID: cache_must_revalidate | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 1 point

What is checked: must-revalidate directive



Technical snapshot within the stated scope; no compliance attestation.

### [+] cache_excellent · Cache-Control directive combination

Status: passed | ID: cache_excellent | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 1 point

What is checked: Cache-Control directive combination

### [+] cache-control-fehlt · Presence of the Cache-Control header

Status: passed | ID: cache-control-fehlt | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 0 points

What is checked: Presence of the Cache-Control header

### [+] cache-pragma-wirkungslos · Pragma: no-cache as a substitute setting

Status: passed | ID: cache-pragma-wirkungslos | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 0 points

What is checked: Pragma: no-cache as a substitute setting

### [+] cache-public-ohne-schutz · public without no-store or private

Status: passed | ID: cache-public-ohne-schutz | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 0 points

What is checked: public without no-store or private

### [+] cache-ohne-no-store-oder-no-cache · no-store or no-cache set

Status: passed | ID: cache-ohne-no-store-oder-no-cache | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 0 points

What is checked: no-store or no-cache set

### [+] cache-max-age-ohne-revalidierung · Very long max-age without must-revalidate

Status: passed | ID: cache-max-age-ohne-revalidierung | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 0 points

What is checked: Very long max-age without must-revalidate

## Clear-Site-Data

3 of 3 points

1 hardening feature with a total of 3 bonus points.

All checks in the “Clear-Site-Data” group were met; no deficiency was found in this area.

### [+] clear_site_data_stateless · No session cookies identified in this response

Status: passed | ID: clear_site_data_stateless | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 3 points

What is checked: No session cookies identified in this response

## security.txt (RFC 9116)

2 of 2 points

2 hardening features with a total of 2 bonus points, plus 11 checks assessing the content of the configuration.

Contact URIs were not opened. Signature structure does not establish cryptographic validity. The recommendation to expire within one year is not a hard validity limit.

All checks in the “security.txt (RFC 9116)” group were met; no deficiency was found in this area.

### [+] security_txt_present · security.txt present

Status: passed | ID: security_txt_present | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 1 point

What is checked: security.txt present

### [+] security_txt_complete · security.txt complete

Status: passed | ID: security_txt_complete | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 1 point

What is checked: security.txt complete



Technical snapshot within the stated scope; no compliance attestation.

### [+] security-txt-fehlt · Presence of a security.txt

Status: passed | ID: security-txt-fehlt | Rule weighting (not a current negative finding): Low | Damage potential: low | Weight: 0 points

What is checked: Presence of a security.txt

### [+] security-txt-contact-ungueltig · Contact URI syntax

Status: passed | ID: security-txt-contact-ungueltig | Rule weighting (not a current negative finding): Flagged | Damage potential: medium | Weight: 0 points

What is checked: Contact URI syntax

### [+] security-txt-expires-nicht-pruefbar · Evaluability of the Expires date

Status: passed | ID: security-txt-expires-nicht-pruefbar | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 0 points

What is checked: Evaluability of the Expires date

### [+] security-txt-contact-fehlt · Mandatory field "Contact" of the security.txt

Status: passed | ID: security-txt-contact-fehlt | Rule weighting (not a current negative finding): Flagged | Damage potential: medium | Weight: 0 points

What is checked: Mandatory field "Contact" of the security.txt

### [+] security-txt-expires-fehlt · Mandatory field "Expires" of the security.txt

Status: passed | ID: security-txt-expires-fehlt | Rule weighting (not a current negative finding): Flagged | Damage potential: medium | Weight: 0 points

What is checked: Mandatory field "Expires" of the security.txt

### [+] security-txt-expires-ungueltig · Formal validity of the Expires date

Status: passed | ID: security-txt-expires-ungueltig | Rule weighting (not a current negative finding): Flagged | Damage potential: medium | Weight: 0 points

What is checked: Formal validity of the Expires date

### [+] security-txt-abgelaufen · Currency of the security.txt

Status: passed | ID: security-txt-abgelaufen | Rule weighting (not a current negative finding): Flagged | Damage potential: medium | Weight: 0 points

What is checked: Currency of the security.txt

### [+] security-txt-expires-zu-weit · Distance of the Expires date from the present

Status: passed | ID: security-txt-expires-zu-weit | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 0 points

What is checked: Distance of the Expires date from the present

### [+] security-txt-expires-mehrfach · Uniqueness of the Expires field

Status: passed | ID: security-txt-expires-mehrfach | Rule weighting (not a current negative finding): Flagged | Damage potential: medium | Weight: 0 points

What is checked: Uniqueness of the Expires field

### [+] security-txt-signatur-aufbau · Structure of the signature block as the rules require

Status: passed | ID: security-txt-signatur-aufbau | Rule weighting (not a current negative finding): Flagged | Damage potential: medium | Weight: 0 points

What is checked: Structure of the signature block as the rules require

### [+] security-txt-signatur-ohne-canonical · Binding of the signature to this location via the Canonical field

Status: passed | ID: security-txt-signatur-ohne-canonical | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 0 points

What is checked: Binding of the signature to this location via the Canonical field



Technical snapshot within the stated scope; no compliance attestation.

## Additional legal information

Output: en / fr / 2026-10-05.2 · EU background and French CNIL guidance on data security; French rules implementing NIS/NIS2 are not covered. · Selected general source information; applicability has not been assessed. · Information checked: 2026-10-05

The following general information relates to your selected context. Several legal systems may be relevant at the same time. Whether these provisions apply to your processing activities or organisation has not been assessed.

This information is separate from the technical findings. It does not assess your specific processing activities, organisation or applicable rules. A measurement or grade establishes neither compliance with nor a breach of a legal obligation.

## Security of personal data

Where the GDPR applies to processing, Article 32 requires technical and organisational security measures appropriate to the risk. These may include encryption to protect personal data in transit.

Observations about transport and application security can inform one part of that assessment. The scan identifies neither all data and risks involved nor whether all safeguards are appropriate.

European Union – GDPR: security of processing · Article 32; scope: Articles 2–3 · EU 2016/679 · checked 2026-10-05 · effective from 2018-05-25: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

## Cybersecurity risks and NIS2

For covered entities, NIS2 describes comprehensive technical, operational and organisational risk management. The relevant national implementation, scope and sector-specific rules must be considered. This technical check assesses neither whether an organisation is covered nor its overall risk management.

Implementing Regulation (EU) 2024/2690 specifies requirements for certain digital services, such as DNS, cloud and managed services. Running a website or using such a service does not by itself establish that an organisation is one of those types of entity.

European Union – NIS2: cybersecurity risk management · Article 21; scope: Articles 2–4 and 26; Directive in force since 16 January 2023, national implementation is a separate matter · EU 2022/2555 · checked 2026-10-05: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

European Commission – requirements for specified digital services · Articles 1–2 and Annex; entry into force: Article 16 · EU 2024/2690 · checked 2026-10-05 · effective from 2024-11-07: https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj/eng

## CNIL guidance on data transmission

For file transfers involving personal data, the CNIL recommends protocols that authenticate the receiving server and protect confidentiality in transit. It also recommends encrypting sensitive files and sending keys or passwords through a separate channel. A TLS finding does not establish that all these measures are in place.

France, CNIL – Security of external data transmission · Fiche 13, ‘Sécuriser les échanges avec l’extérieur’, ‘Les précautions élémentaires’ section · CNIL, fiche 13, 2024-03-14 · checked 2026-10-05: https://www.cnil.fr/fr/securite-securiser-les-echanges-avec-lexterieur

## CNIL guidance on websites

The CNIL recommends TLS to protect web connections and restricting access to administration interfaces to authorised people. An external scan does not establish appropriate implementation across all pages, roles and internal systems.

France, CNIL – Website security · Guide pratique RGPD – Sécurité des données personnelles, Fiche 10, ‘Les précautions élémentaires’ section · CNIL, version 2024, mise à jour 2026 · checked 2026-10-05: https://www.cnil.fr/sites/default/files/2026-05/cnil_guide_securite_personnelle.pdf



Technical snapshot within the stated scope; no compliance attestation.