

Wolf-Agents Security Report

Web Security Check

Output: en / none / 2026-10-05.1 · Technical results, explanations and sources without additional legal context. · Information checked: 2026-10-05

Example target

<https://synthetic-review.app/start>

Example time: 21 Sept 2026, 10:02 GMT+2 (Europe/Berlin)

Document generated on: 05 Oct 2026, 14:00 GMT+2 (Europe/Berlin)

Synthetic example: example data, no measurement performed. Explanations created using AI. About its creation: <https://wolf-agents.com/ki-hinweis/#english>

Example catalogue: 1.6

Report presentation: 2026-10-05.legal-1

Example ID: W1

Report model: 1.4

Synthetic product example W1; not a customer report.

Issued by: Wolf-Agents.com - kontakt@wolf-agents.com

Illustrative assessment; not an assessment of a measured system.

Illustrative assessment

B

103 of 166 points - Reasonable

133 checks: 43 passed, 4 failed, 28 not assessable, 38 informational, 20 not applicable.

28 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)

[caa-keine-records](#) · failed · CAA records restricting certificate issuance

[security-txt-fehlt](#) · failed · Presence of a security.txt

Open / not assessable

[csp-unsafe-inline-style](#) · not assessable · Inline CSS in style source lists

[hsts_preload_pending](#) · not assessable · HSTS preload application pending

[hsts-max-age-fehlt](#) · not assessable · Valid HSTS syntax and max-age

[hsts-max-age-null](#) · not assessable · max-age=0 as an opt-out from HSTS protection

[hsts-max-age-zu-kurz](#) · not assessable · Length of the HSTS validity period

[hsts-subdomains-fehlt](#) · not assessable · Coverage of subdomains

[hsts-preload-max-age-zu-kurz](#) · not assessable · Preload requirement: validity period

[hsts-preload-subdomains-fehlt](#) · not assessable · Preload requirement: subdomains

[redirect_www_normalized](#) · not assessable · WWW normalisation

[redirect_www_not_applicable](#) · not assessable · No www alias present

[caa-nicht-parsebar](#) · not assessable · Formal validity of the CAA records

[caa-syntax-ungueltig](#) · not assessable · Syntax of the assessed CAA properties

[caa-kritische-eigenschaft](#) · not assessable · Assessment of critical CAA properties

caa-kein-issuewild · not assessable · Separate rule for wildcard certificates
caa-kein-iodef · not assessable · Reporting address for rejected certificate requests
dnssec-nicht-aktiviert · not assessable · Signing of the DNS records (DNSSEC)
dnssec-validierung-unvollstaendig · not assessable · Completeness of the DNSSEC chain of trust
ssl_tls13 · not assessable · TLS 1.3
security-txt-contact-ungueltig · not assessable · Contact URI syntax
security-txt-expires-nicht-pruefbar · not assessable · Evaluability of the Expires date
security-txt-contact-fehlt · not assessable · Mandatory field "Contact" of the security.txt
security-txt-expires-fehlt · not assessable · Mandatory field "Expires" of the security.txt
security-txt-expires-ungueltig · not assessable · Formal validity of the Expires date
security-txt-abgelaufen · not assessable · Currency of the security.txt
security-txt-expires-zu-weit · not assessable · Distance of the Expires date from the present
security-txt-expires-mehrfach · not assessable · Uniqueness of the Expires field
security-txt-signatur-aufbau · not assessable · Structure of the signature block as the rules require
security-txt-signatur-ohne-canonical · not assessable · Binding of the signature to this location via the Canonical field

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 2026-09-20 (revision 546be746859e). Covered by inherited include_subdomains from app. Pending inclusion and pending removal are not measured. Browser versions may use different lists; header observations are separate.
 - Requested origin: https://synthetic-review.app. Final response origin: https://synthetic-review.app. Response headers, cookies, TLS, CSP and content observations apply to the final response; DNS and security.txt measurements apply to the requested host synthetic-review.app. 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 2026-09-21T08:02:23.369Z.
Synthetic example; no measurement performed. Not an audit, certification or legal advice.
- 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)

85 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.

Finding: A Content Security Policy was delivered. The detailed analysis assesses the restrictions it can identify; the presence of the header alone does not demonstrate effective protection against XSS.

Evidence: `\u{20}default-src\u{20}'self';\u{20}object-src\u{20}'none';\u{20}base-uri\u{20}'self';\u{20}frame-ancestor s\u{20}'none'`

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-Kompodium/IT_Grundschutz_Kompodium_Edition2023.pdf?__blob=publicationFile&v=4

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

Status: Information | ID: strict-transport-security | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 0 points

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

Finding: No HSTS response header was measured. Chromium reference list dated 2026-09-20 (revision 546be746859e). Covered by inherited include_subdomains from app. Pending inclusion and pending removal are not measured. Browser versions may use different lists; header observations are separate.

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-Kompodium/IT_Grundschutz_Kompodium_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-Kompodium/IT_Grundschutz_Kompodium_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.

[i] permissions-policy · Browser API restrictions

Status: Information | ID: permissions-policy | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 5 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.

Finding: The saved Permissions-Policy has valid dictionary syntax and received 5/10 product points. The point gap alone does not demonstrate a security defect; the application's required browser features were not established.

Evidence: \u{20}camera=(),\u{20}microphone=()

Recommendation [permissions-policy]: Review which browser features and embeds the application needs. Apply additional restrictions only where appropriate and test the affected workflows.

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

Status: failed | ID: cross-origin-opener-policy | Severity: Low | Damage potential: low | Response: medium-term | Weight: 5 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: No explicit COOP policy was observed. It provides additional protection for window relationships and is relevant to certain isolated browser features. Its absence alone does not demonstrate a side-channel attack.

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: 5 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: COEP is an optional prerequisite for cross-origin isolation. Its absence does not demonstrate an exploitable vulnerability. Enabling it may block existing third-party resources.

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

3 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

[i] csp_default_none · CSP default-src: none

Status: Information | 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

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_default_none]: If appropriate for this application: Restrictive default-src: 'none' policy

[+] 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

[i] csp_form_action · CSP form-action

Status: Information | 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

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_form_action]: If appropriate for this application: Restrict form targets

[i] csp_upgrade_insecure · CSP upgrade-insecure-requests

Status: Information | 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

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_upgrade_insecure]: If appropriate for this application: Upgrade HTTP to HTTPS automatically

[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

[+] 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

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

Status: not assessable | ID: csp-unsafe-inline-style | Rule weighting (not a current negative finding): Low | Damage potential: low | Weight: 0 points

What is checked: Inline CSS in style source lists

The saved snapshot has no separate element/attribute and multi-policy assessment. The historical analyser directive label does not reliably identify a fallback. The affected contexts cannot be confirmed from that label; no new analysis was run.

[+] 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

2 of 5 points

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

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

Status: Information | 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

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 [hsts_max_age]: If appropriate for this application: max-age=31536000 or higher

[i] hsts_subdomains · HSTS includeSubDomains

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

What is checked: HSTS includeSubDomains

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 [hsts_subdomains]: If appropriate for this application: Enable includeSubDomains only when all affected subdomains can support HTTPS for as long as browsers may apply the HSTS policy.

[i] hsts_preload_flag · HSTS preload flag

Status: Information | 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

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 [hsts_preload_flag]: If appropriate for this application: Do not add preload by default. Assess the long-term HTTPS commitment for every subdomain and the slow removal process first.

[+] 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 2026-09-20 (revision 546be746859e). Covered by inherited include_subdomains from app. 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 2026-09-20 (revision 546be746859e). Covered by inherited include_subdomains from app. 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: not assessable | 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

The header in which this aspect would be checked is not set, so the aspect can be neither met nor violated. The missing header is listed as a separate check in this section.

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

Status: not assessable | 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

The header in which this aspect would be checked is not set, so the aspect can be neither met nor violated. The missing header is listed as a separate check in this section.

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

Status: not assessable | 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

The header in which this aspect would be checked is not set, so the aspect can be neither met nor violated. The missing header is listed as a separate check in this section.

[?] hsts-subdomains-fehlt · Coverage of subdomains

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

What is checked: Coverage of subdomains

The header in which this aspect would be checked is not set, so the aspect can be neither met nor violated. The missing header is listed as a separate check in this section.

[+] 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: not assessable | 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

The header in which this aspect would be checked is not set, so the aspect can be neither met nor violated. The missing header is listed as a separate check in this section.

[?] hsts-preload-subdomains-fehlt · Preload requirement: subdomains

Status: not assessable | 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

The header in which this aspect would be checked is not set, so the aspect can be neither met nor violated. The missing header is listed as a separate check in this section.

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

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

What is checked: Header while a preload entry exists

Finding: No HSTS header was measured in this response. The separate reference-list match is not a header observation. A valid header can also protect browsers without this list entry; review HTTPS coverage before enabling it.

Evidence:\u{20}key:\u{20}preloadedWithoutHeader

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.

[-] 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

HTTPS redirects

1 of 2 assessable points (1 further point cannot be assessed)

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

[i] redirect_single · Clean HTTP-to-HTTPS redirect

Status: Information | 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

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 [redirect_single]: If appropriate for this application: Where a redirect is needed, use only 1 redirect in the chain.

[?] redirect_www_normalized · WWW normalisation

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

What is checked: WWW normalisation

No analysis is available for this check; it was not part of the result at the time of the scan. There is neither a positive nor a negative finding.

[?] redirect_www_not_applicable · No www alias present

Status: not assessable | 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

No analysis is available for this check; it was not part of the result at the time of the scan. There is neither a positive nor a negative finding.

[+] 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

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: No CORP header was observed in the measured response.

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: No CORP header was observed in the measured response.

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: No CORP header was observed in the measured response.

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.

[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

0 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.

[i] reporting_report_to · Report-To header

Status: Information | 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

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_report_to]: If appropriate for this application: Configure a suitable Report-To endpoint where required and check its syntax and delivery separately.

[i] reporting_nel · Network Error Logging

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

What is checked: Network Error Logging

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_nel]: If appropriate for this application: Configure NEL where needed; browser support and report delivery must be checked separately.

[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)

[i] origin_agent_cluster · Origin-Agent-Cluster

Status: Information | 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

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 [origin_agent_cluster]: If appropriate for this application: Origin-Agent-Cluster: ?1 requests origin-keyed agent clustering in supporting browsers; browser state and actual process isolation were not measured.

DNSSEC

2 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.

[i] dnssec_validated · DNSSEC validated

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

What is checked: DNSSEC validated

Finding: Historical configuration assessment (2 saved bonus points): trusted resolver validation metadata cannot be reconstructed under the corrected contract. This is no new successful check; the saved points and grade remain unchanged.

Recommendation [dnssec_validated]: Check DNSSEC through a trusted validating resolver; review signing, the chain of trust and ongoing key management with the DNS provider.

[i] dnssec_enabled · DNSSEC enabled (partially)

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

What is checked: DNSSEC enabled (partially)

Finding: Historical configuration assessment (0 saved bonus points): trusted resolver validation metadata cannot be reconstructed under the corrected contract. This is no new successful check; the saved points and grade remain unchanged.

Recommendation [dnssec_enabled]: If DNSSEC validation has not been confirmed, check signing and the chain of trust with the DNS provider.

[i] caa_records · CAA issue/issuewild records

Status: Information | 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

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 [caa_records]: If appropriate for this application: CAA records can specify issuer restrictions for the relevant certificate type. Neither a specific CA's authorisation to issue nor the prevention of misissuance was established.

[i] caa_iodef · CAA iodef reporting

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

What is checked: CAA iodef reporting

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 [caa_iodef]: If appropriate for this application: CAA iodef record for reports of certificate misuse

[!] caa-keine-records · CAA records restricting certificate issuance

Status: failed | ID: caa-keine-records | Severity: Low | Damage potential: low | Response: medium-term | Weight: 0 points

What is checked: CAA records restricting certificate issuance

Finding: No CAA records configured

[?] **caa-nicht-parsebar · Formal validity of the CAA records**

Status: not assessable | 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

The measurement on which this aspect depends could not be carried out, so the aspect can be neither met nor violated. The reason is listed as a separate check in this section.

[?] **caa-syntax-ungueltig · Syntax of the assessed CAA properties**

Status: not assessable | 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

The measurement on which this aspect depends could not be carried out, so the aspect can be neither met nor violated. The reason is listed as a separate check in this section.

[?] **caa-kritische-eigenschaft · Assessment of critical CAA properties**

Status: not assessable | 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

The measurement on which this aspect depends could not be carried out, so the aspect can be neither met nor violated. The reason is listed as a separate check in this section.

[?] **caa-kein-issuewild · Separate rule for wildcard certificates**

Status: not assessable | 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

The measurement on which this aspect depends could not be carried out, so the aspect can be neither met nor violated. The reason is listed as a separate check in this section.

[?] **caa-kein-iodef · Reporting address for rejected certificate requests**

Status: not assessable | 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

The measurement on which this aspect depends could not be carried out, so the aspect can be neither met nor violated. The reason is listed as a separate check in this section.

[+] **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: not assessable | 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)

The saved measurement does not document this corrected check. Its absence is not a successful check; no new measurement was performed.

[?] **dnssec-validierung-unvollstaendig · Completeness of the DNSSEC chain of trust**

Status: not assessable | 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

The saved measurement does not document this corrected check. Its absence is not a successful check; no new measurement was performed.

[+] 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

not assessable (2 possible points in this category)

1 hardening feature with a total of 2 bonus points.

[?] ssl_tls13 · TLS 1.3

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

What is checked: TLS 1.3

No analysis is available for this check; it was not part of the result at the time of the scan. There is neither a positive nor a negative finding.

Cache-Control (BSI)

0 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.

[i] cache_present · Cache-Control header

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

What is checked: Cache-Control 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 [cache_present]: If appropriate for this application: Set a Cache-Control policy appropriate to the response and its confidentiality.

[i] cache_no_store · no-store directive

Status: Information | 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

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 [cache_no_store]: If appropriate for this application: Prevents any caching of sensitive data

[i] cache_private · private directive

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

What is checked: private directive

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 [cache_private]: If appropriate for this application: Prevents caching on proxy servers

[i] cache_must_revalidate · must-revalidate directive

Status: Information | 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

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 [cache_must_revalidate]: If appropriate for this application: Forces revalidation after expiry

[i] cache_excellent · Cache-Control directive combination

Status: Information | 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

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 [cache_excellent]: If appropriate for this application: Review the combined use of no-store, private and must-revalidate for sensitive responses. Their combination is a scanner criterion, not a universal caching recommendation.

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

Status: Information | 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

Finding: Cache-Control is missing. Whether caching is unwanted depends on the content. no-store is useful for sensitive responses; public content may be cached.

[+] 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)

0 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.

[i] security_txt_present · security.txt present

Status: Information | 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

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 [security_txt_present]: If appropriate for this application: security.txt with Contact + Expires (RFC 9116)

[i] security_txt_complete · security.txt complete

Status: Information | 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

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 [security_txt_complete]: If appropriate for this application: With Encryption or Canonical (best practice)

[!] security-txt-fehlt · Presence of a security.txt

Status: failed | ID: security-txt-fehlt | Severity: Low | Damage potential: low | Response: medium-term | Weight: 0 points

What is checked: Presence of a security.txt

Finding: security.txt not found

[?] security-txt-contact-ungueltig · Contact URI syntax

Status: not assessable | 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

The measurement on which this aspect depends could not be carried out, so the aspect can be neither met nor violated. The reason is listed as a separate check in this section.

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

Status: not assessable | 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

The measurement on which this aspect depends could not be carried out, so the aspect can be neither met nor violated. The reason is listed as a separate check in this section.

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

Status: not assessable | 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

The measurement on which this aspect depends could not be carried out, so the aspect can be neither met nor violated. The reason is listed as a separate check in this section.

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

Status: not assessable | 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

The measurement on which this aspect depends could not be carried out, so the aspect can be neither met nor violated. The reason is listed as a separate check in this section.

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

Status: not assessable | 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

The measurement on which this aspect depends could not be carried out, so the aspect can be neither met nor violated. The reason is listed as a separate check in this section.

[?] security-txt-abgelaufen · Currency of the security.txt

Status: not assessable | 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

The measurement on which this aspect depends could not be carried out, so the aspect can be neither met nor violated. The reason is listed as a separate check in this section.

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

Status: not assessable | 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

The measurement on which this aspect depends could not be carried out, so the aspect can be neither met nor violated. The reason is listed as a separate check in this section.

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

Status: not assessable | 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

The measurement on which this aspect depends could not be carried out, so the aspect can be neither met nor violated. The reason is listed as a separate check in this section.

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

Status: not assessable | 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

The measurement on which this aspect depends could not be carried out, so the aspect can be neither met nor violated. The reason is listed as a separate check in this section.

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

Status: not assessable | 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

The measurement on which this aspect depends could not be carried out, so the aspect can be neither met nor violated. The reason is listed as a separate check in this section.