Wolf-Agents Security Report

API Security Check: CORS and security headers at the public endpoint

Output: en / it / 2026-10-05.2 · EU background and general information on risk management under Italy's Legislative Decree 138/2024. · Selected general source information; applicability has not been assessed. · Information checked: 2026-10-05

Target

https://wolf-agents.com/api/health
Scan time: 06 Oct 2026, 22:32 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: 1.4
Report presentation: 2026-10-05.legal-2
Scan ID: 52a62d29-3718-4c38-a3dc-d45bc6f8123d
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+ 100 of 100 points - Excellent

17 checks: 14 passed, 0 failed, 2 not assessable, 1 informational.
2 of 17 checks cannot be assessed conclusively from the saved findings. The stored product score is not recalculated from this finding summary. Checks that cannot be assessed do not count as passed. The rate-limit category is not assessed. The deduction model leaves the overall score unchanged but awards no confirmed 15/15 category points; the overall grade does not establish effective throttling.

Start here

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

Confirmed negative findings

No confirmed negative findings in the recorded scope.

Open / not assessable

known-cve · not assessable · Server version against known weaknesses
xst-vulnerability · not assessable · TRACE/TRACK methods

Additional legal information

Scope limits

- The check is unauthenticated and is performed exclusively from outside the system.
- Conservative configuration check for CORS, security headers and other visible signals at this single public API endpoint: no endpoint discovery, crawling, brute force, authentication bypass, authorisation or business-logic testing, or monitoring. The version comparison uses a local, incomplete CVE selection (most recent entry 2024-08-14); no match does not mean free from vulnerabilities. These explanations come from catalogue 1.4. Historical scores and grades are not recalculated.
- This is not a penetration test. No vulnerability was actively exploited.
- No source code, infrastructure or process audit.

Technical snapshot within the stated scope; no compliance attestation.

- 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.

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. The score starts at 100; assessed findings deduct points according to severity and base weight. Informational findings cause no deduction. Absent visible rate-limit signals cause no deduction, but are not shown as confirmed category points; the unchanged overall score does not establish effective throttling. Weights and grade caps are product methodology, not an official security standard or an overall CVSS score. 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.

CORS configuration

25 of 25 points

Cross-Origin Resource Sharing controls which browser origins may read a response. This check observes the headers of one public response without credentials; actual access to protected data is not tested.

The passive check recognised no risky CORS pattern at the URL entered. That is a good configuration signal, but it does not replace a check of the authentication or of further endpoints.

[+] cors-wildcard-credentials · CORS with credentials for the foreign test origin or null

Status: passed | ID: cors-wildcard-credentials | Rule weighting (not a current negative finding): Critical | Damage potential: high | Weight: 25 points

What is checked: Whether a GET response allows the foreign test origin or "null" together with exactly Access-Control-Allow-Credentials: true. No credentials are sent and no protected data are retrieved.

References: CWE-942 | OWASP API8:2023

References: OWASP API8:2023 · Security Misconfiguration · Is the API Vulnerable? / How To Prevent · checked 5 October 2026 · https://api-security.owasp.org/editions/2023/en/0xa8-security-misconfiguration/

[+] cors-wildcard-credentials-blocked · CORS: wildcard with credentials (blocked by the browser)

Status: passed | ID: cors-wildcard-credentials-blocked | Rule weighting (not a current negative finding): Low | Damage potential: low | Weight: 5 points

What is checked: Whether the server sends the literal "*" as the allowed origin and at the same time allows credentials — a combination that browsers refuse and that therefore concerns configuration hygiene, not exploitability.

References: CWE-942 | OWASP API8:2023

References: OWASP API8:2023 · Security Misconfiguration · Is the API Vulnerable? / How To Prevent · checked 5 October 2026 · https://api-security.owasp.org/editions/2023/en/0xa8-security-misconfiguration/

[+] cors-wildcard · CORS: wildcard origin

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

What is checked: Whether the server allows cross-origin requests from every domain (Access-Control-Allow-Origin: *), without credentials.

References: CWE-942 | OWASP API8:2023

References: OWASP API8:2023 · Security Misconfiguration · Is the API Vulnerable? / How To Prevent · checked 5 October 2026 · https://api-security.owasp.org/editions/2023/en/0xa8-security-misconfiguration/

[+] cors-origin-reflection · CORS: origin reflection

Status: passed | ID: cors-origin-reflection | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 0 points

What is checked: Whether the GET response returns the foreign test origin. One observation proves neither arbitrary reflection nor the absence of an internal allowlist.

References: CWE-942 | OWASP API8:2023

References: OWASP API8:2023 · Security Misconfiguration · Is the API Vulnerable? / How To Prevent · checked 5 October 2026 · https://api-security.owasp.org/editions/2023/en/0xa8-security-misconfiguration/

[+] cors-null-origin · CORS: null origin accepted

Status: passed | ID: cors-null-origin | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 0 points

What is checked: Whether the server accepts the origin "null" as an allowed origin — without credentials.

References: CWE-942 | OWASP API8:2023

References: OWASP API8:2023 · Security Misconfiguration · Is the API Vulnerable? / How To Prevent · checked 5 October 2026 · https://api-security.owasp.org/editions/2023/en/0xa8-security-misconfiguration/

API headers

18 of 18 points

Security-relevant headers such as X-Content-Type-Options and Cache-Control protect against MIME sniffing and unintended caching.

The API headers checked show a good signal: nosniff, Cache-Control and Content-Type appear plausibly configured within the passive scope.

[+] api-response-cacheable · Cookie-setting response and shared caching

Status: passed | ID: api-response-cacheable | Rule weighting (not a current negative finding): Medium | Damage potential: medium | Weight: 8 points

What is checked: Whether a response that sets a cookie may at the same time be stored by a shared cache (proxy/CDN).

References: CWE-524 | OWASP API8:2023

References: OWASP API8:2023 · Security Misconfiguration · Is the API Vulnerable? / How To Prevent · checked 5 October 2026 · https://api-security.owasp.org/editions/2023/en/0xa8-security-misconfiguration/

Technical snapshot within the stated scope; no compliance attestation.

[+] missing-nosniff · X-Content-Type-Options: nosniff

Status: passed | ID: missing-nosniff | Rule weighting (not a current negative finding): Low | Damage potential: low | Weight: 5 points

What is checked: Whether the response sets the header X-Content-Type-Options: nosniff and thereby stops MIME sniffing in the browser.

References: CWE-16

References: OWASP HTTP Headers Cheat Sheet · x-content-type-options · checked 5 October 2026 · https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Headers_Cheat_Sheet.html#x-content-type-options

[+] missing-content-type · Content-Type of the API response

Status: passed | ID: missing-content-type | Rule weighting (not a current negative finding): Low | Damage potential: low | Weight: 3 points

What is checked: Whether a response with a representation sends a syntactically valid media type. JSON, XML, text and binary data can all be legitimate API formats; responses without a representation do not need this header for this check.

References: CWE-16

References: OWASP HTTP Headers Cheat Sheet · content-type · checked 5 October 2026 · https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Headers_Cheat_Sheet.html#content-type

Error handling

17 of 17 points

Detailed error messages such as stack traces or database errors give attackers valuable information about your system architecture.

The single conservative error response check recognised no stack traces, database errors or internal paths. That is not fuzzing and not a complete error handling check.

[+] stack-trace-exposure · Stack traces in error responses

Status: passed | ID: stack-trace-exposure | Rule weighting (not a current negative finding): High | Damage potential: high | Weight: 15 points

What is checked: Whether an error response of the API contains stack traces and thereby reveals file names, functions and the technology in use.

References: CWE-209 | OWASP API8:2023

References: OWASP API8:2023 · Security Misconfiguration · Is the API Vulnerable? / How To Prevent · checked 5 October 2026 · https://api-security.owasp.org/editions/2023/en/0xa8-security-misconfiguration/

[+] database-error-exposure · Database error messages in responses

Status: passed | ID: database-error-exposure | Rule weighting (not a current negative finding): High | Damage potential: high | Weight: 12 points

What is checked: Whether an error response of the API contains database messages and thereby reveals table names, column names or SQL.

References: CWE-209 | OWASP API8:2023

References: OWASP API8:2023 · Security Misconfiguration · Is the API Vulnerable? / How To Prevent · checked 5 October 2026 · https://api-security.owasp.org/editions/2023/en/0xa8-security-misconfiguration/

[+] debug-info-exposure · Debug information in responses

Status: passed | ID: debug-info-exposure | Rule weighting (not a current negative finding): Medium | Damage potential: medium | Weight: 10 points

What is checked: Whether the API returns debug output that should only be visible in development environments.

References: CWE-489 | OWASP API8:2023

References: OWASP API8:2023 · Security Misconfiguration · Is the API Vulnerable? / How To Prevent · checked 5 October 2026 · https://api-security.owasp.org/editions/2023/en/0xa8-security-misconfiguration/

Technical snapshot within the stated scope; no compliance attestation.

[+] internal-path-exposure · Internal file paths in responses

Status: passed | ID: internal-path-exposure | Rule weighting (not a current negative finding): Medium | Damage potential: medium | Weight: 8 points

What is checked: Whether an error response contains absolute server paths and thereby reveals the operating system and the directory structure.

References: CWE-200 | OWASP API8:2023

References: OWASP API8:2023 · Security Misconfiguration · Is the API Vulnerable? / How To Prevent · checked 5 October 2026 · https://api-security.owasp.org/editions/2023/en/0xa8-security-misconfiguration/

Rate limiting

Partial findings available; no reliable category score. Aspects that cannot be assessed are identified individually.

Rate limiting reduces risks from overload, scraping and automated failed attempts. This check assesses only visible rate limit headers. This category was not assessed in this run: the absence of a visible signal proves neither protection nor the absence of throttling.

[i] no-rate-limiting · Rate limit headers

Status: Information | ID: no-rate-limiting | Rule weighting (not a current negative finding): Info | Damage potential: for information | Weight: 0 points

What is checked: Whether the response sends rate-limit signals (RateLimit, RateLimit-Policy, older RateLimit-*/X-RateLimit-* fields or HTTP 429). The check covers visibility, not enforcement; no load test is run.

Finding: No rate limit headers recognised

No supported rate-limit signal was recognised in the response. This does not establish that throttling is absent: limits can be invisible, user-dependent or visible only after a quota is exceeded.

Effect: Only if effective limits are absent can automated requests cause overload or cost. This scan does not demonstrate that such limits are absent.

Recommendation [no-rate-limiting]: Review and document existing quotas and client backoff. The active IETF draft draft-ietf-httpapi-ratelimit-headers-11 (23 May 2026) uses RateLimit and RateLimit-Policy; it is not yet an RFC. Retry-After can express a wait time on HTTP 429 as seconds or an HTTP date.

References: CWE-770 | OWASP API4:2023

References: OWASP API4:2023 · Unrestricted Resource Consumption · Is the API Vulnerable? / How To Prevent · checked 5 October 2026 · https://api-security.owasp.org/editions/2023/en/0xa4-unrestricted-resource-consumption/

Server information

Partial findings available; no reliable category score. Aspects that cannot be assessed are identified individually.

Server headers can reveal version information that attackers use to identify known weaknesses (CVEs).

[?] known-cve · Server version against known weaknesses

Status: not assessable | ID: known-cve | Rule weighting (not a current negative finding): High | Damage potential: high | Weight: 15 points

What is checked: Whether the version read from the Server header falls into the version range of publicly known weaknesses. Purely version-based — no proof of an active vulnerability.

No sufficiently precise product version, or no entries for this product in the local CVE selection. A vulnerability comparison could not be made.

References: CWE-1035 | OWASP API8:2023

References: OWASP API8:2023 · Security Misconfiguration · Is the API Vulnerable? / How To Prevent · checked 5 October 2026 · https://api-security.owasp.org/editions/2023/en/0xa8-security-misconfiguration/

Technical snapshot within the stated scope; no compliance attestation.

[+] server-version-exposed · Server header with a version number

Status: passed | ID: server-version-exposed | Rule weighting (not a current negative finding): Low | Damage potential: low | Weight: 5 points

What is checked: Whether the Server header names a product version and thereby makes a targeted search for weaknesses easier.

References: CWE-200

References: OWASP HTTP Headers Cheat Sheet · server · checked 5 October 2026 · https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Headers_Cheat_Sheet.html#server

[+] powered-by-exposed · X-Powered-By header

Status: passed | ID: powered-by-exposed | Rule weighting (not a current negative finding): Low | Damage potential: low | Weight: 5 points

What is checked: Whether the response sends an X-Powered-By header and thereby names the technology in use.

References: CWE-200

References: OWASP HTTP Headers Cheat Sheet · x-powered-by · checked 5 October 2026 · https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Headers_Cheat_Sheet.html#x-powered-by

HTTP methods

not assessable (10 possible points in this category)

The check reads the methods advertised by the target in the Allow header. It does not execute TRACE, TRACK, CONNECT or state-changing methods; permissions and actual usability remain untested.

[?] xst-vulnerability · TRACE/TRACK methods

Status: not assessable | ID: xst-vulnerability | Rule weighting (not a current negative finding): Medium | Damage potential: medium | Weight: 12 points

What is checked: Whether the server reports the HTTP methods TRACE or TRACK as enabled in the Allow header of an OPTIONS response.

The target did not answer this question, so the check could not reach a verdict. There is neither a positive nor a negative finding.

References: CWE-693 | OWASP API8:2023

References: OWASP API8:2023 · Security Misconfiguration · Is the API Vulnerable? / How To Prevent · checked 5 October 2026 · https://api-security.owasp.org/editions/2023/en/0xa8-security-misconfiguration/

Technical snapshot within the stated scope; no compliance attestation.

Additional legal information

Output: en / it / 2026-10-05.2 · EU background and general information on risk management under Italy’s Legislative Decree 138/2024. · 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.

This additional information does not cover detailed ACN requirements, individual implementation deadlines or specific sectoral or certified email (PEC) requirements.

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

Risk management in Italy

Article 24 of Italy’s Legislative Decree 138/2024 provides for appropriate and proportionate technical, operational and organisational measures for covered essential and important entities. These include policies and procedures on the use of cryptography and, where appropriate, encryption, as well as access control policies. The scan assesses neither this classification nor the full security programme and its implementation.

Italy, Gazzetta Ufficiale – Legislative Decree 138/2024: risk management · Article 24(1) and (2)(h)–(i); scope in particular: Articles 3–6 · D.Lgs. 138/2024; GU n. 230 del 01-10-2024 · checked 2026-10-05 · effective from 2024-10-16: https://www.gazzettaufficiale.it/eli/id/2024/10/01/24G00155/SG

Technical snapshot within the stated scope; no compliance attestation.