

Wolf-Agents Security Report

API-Security-Check: CORS & Sicherheitsheader am öffentlichen Endpunkt

Ausgabe: de / none / 2026-10-05.2 · Technische Ergebnisse, Erläuterungen und Fachquellen ohne zusätzliche rechtliche Einordnung. · Hinweise geprüft: 2026-10-05

Prüfgegenstand

<https://wolf-agents.com/api/health>

Prüfzeitpunkt: 06.10.2026, 22:32 Uhr (MESZ)

Dokument erzeugt am: 06.10.2026, 22:55 Uhr (MESZ)

Die Erläuterungen in diesem Bericht wurden mit KI erstellt. Vorhandene Messwerte wurden automatisiert erhoben; Bewertungen folgen festen Regeln. Zur Entstehung: <https://wolf-agents.com/ki-hinweis/>

Katalogstand der Messung: 1.4

Reportdarstellung: 2026-10-05.legal-2

Scan-Kennung: 52a62d29-3718-4c38-a3dc-d45bc6f8123d

Reportmodell: 1.4

Vertraulichkeit: für den Empfänger und von ihm benannte Dritte

Aussteller: Wolf-Agents.com - kontakt@wolf-agents.com

Gesamtbild

A+ 100 von 100 Punkten - Exzellent

17 Prüfpunkte: 14 bestanden, 0 nicht bestanden, 2 nicht auswertbar, 1 Hinweis.

2 von 17 Prüfpunkten sind mit den gespeicherten Befunden nicht abschließend auswertbar. Die gespeicherte Produktpunktzahl wird aus dieser Befundbilanz nicht neu berechnet. Nicht auswertbare Checks gelten nicht als bestanden. Die Rate-Limit-Kategorie ist unbewertet. Das Abzugsmodell lässt den Gesamtscore unverändert, vergibt dafür aber keine bestätigten 15/15 Kategorienpunkte; die Gesamtnote belegt keine wirksame Drosselung.

Schneller Einstieg

Hinweise, nicht anwendbare und bestandene Checks stehen im vollständigen Katalog unten. Die Kennungen bezeichnen die Abschnitte auch im Ausdruck.

Bestätigte negative Befunde

Im dokumentierten Prüfumfang sind keine bestätigten negativen Befunde enthalten.

Offen / nicht auswertbar

[known-cve](#) · nicht auswertbar · Server-Version gegen bekannte Schwachstellen

[xst-vulnerability](#) · nicht auswertbar · TRACE/TRACK-Methoden

Grenzen der Aussage

- Die Prüfung ist unauthentifiziert und erfolgt ausschließlich von außen.
- Konservativer Konfigurationscheck für CORS, Sicherheitsheader und weitere sichtbare Signale an genau diesem öffentlichen API-Endpunkt: keine Endpoint-Suche, kein Crawling, kein Brute Force, kein Auth-Bypass, keine Autorisierungs- oder Geschäftslogikprüfung und kein Monitoring. Der Versionsabgleich nutzt eine lokale, unvollständige CVE-Auswahl (jüngster Eintrag 2024-08-14); kein Treffer bedeutet nicht schwachstellenfrei. Die hier verwendeten Erläuterungen stammen aus Katalog 1.4. Historische Punktzahlen und Noten werden nicht neu berechnet.
- Dies ist kein Penetrationstest. Es wurde keine Schwachstelle aktiv ausgenutzt.
- Kein Quellcode-, Infrastruktur- oder Prozessaudit.

- Momentaufnahme zum genannten Zeitpunkt. Spätere Änderungen sind nicht erfasst.
- Falschmeldungen sind möglich. Vorgeschaltete CDN-, WAF- oder Ratenbegrenzungs-Systeme können das Ergebnis verfälschen.
- Prüfpunkte ohne auswertbaren Messbeleg, etwa bei nicht erreichbaren oder nicht antwortenden Systemen, erscheinen als „nicht auswertbar“ und nicht als „bestanden“.
- Diese Einordnung ist allgemein gehalten und ersetzt keine Rechtsberatung.

Automatisierte Momentaufnahme im dokumentierten Prüfumfang. Kein Audit, keine Zertifizierung und keine Rechtsberatung. Gesetzliche Rechte bleiben unberührt. Messstand: 06.10.2026.

Belegnotation e1: Originalbackslashes werden verdoppelt; \u{HEX} steht für genau einen Unicode-Codepoint. Rohbelege stellen so jedes Leer-, Steuer-, kombinierende oder nicht unterstützte Zeichen ausdrücklich dar. Keine Normalisierung.

Layoutumbrüche sind keine Originalzeichen. CSV-Rohfelder erhalten zusätzlich den vollständigen Belegtext; Cookie-Werte und Lokalteile von E-Mail-Adressen sind dort wie überall als *** ausgeblendet.

Bewertungsschema

Die folgende Skala gilt nur für nicht bestandene Prüfpunkte, nicht für Hinweise, nicht auswertbare oder nicht anwendbare Checks. Die Begriffe für Schadenspotenzial und Reaktionspriorität orientieren sich am BSI-Praxis-Leitfaden, Version 1.2, Abschnitt 4.1.3. Die Zuordnung der Scannerbefunde sowie Punkte und Note folgen unserer dokumentierten Bewertungsmethodik. Daraus entstehen keine gesetzlichen Fristen. hoch = sofort, mittel = kurzfristig, niedrig = mittelfristig, zur Information = langfristig. Die Punktzahl beginnt bei 100; bewertete Befunde ziehen entsprechend Schweregrad und Basisgewicht ab. Informationshinweise haben keinen Abzug. Fehlende sichtbare Rate-Limit-Signale lösen keinen Abzug aus, werden aber auch nicht als bestätigte Kategorienpunkte dargestellt; der unveränderte Gesamtscore belegt keine Drosselungswirkung. Gewichte und Notenkappen sind Produktmethodik, kein amtlicher Sicherheitsstandard und kein CVSS-Gesamtscore. Es wird bewusst KEIN CVSS-Wert vergeben - für Konfigurationsbefunde gibt es keine autoritative CVSS-Bewertung, und eine selbst gerechnete Zahl in der Notation eines Standards wäre eine Genauigkeit, die es nicht gibt.

BSI - Ein Praxis-Leitfaden für IS-Penetrationstests · v1.2 (2016-11), Kap. 4.1.3, S. 25-26 · geprüft 2026-10-05 ·

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/Pentest_Webcheck/Leitfaden_Penetrationstests.pdf?__blob=publicationFile&v=3

Zustände je Prüfpunkt:

[+] bestanden - im angegebenen Prüfumfang bestätigt; keine Abweichung belegt. [!] nicht bestanden - Befund vorhanden. [?] nicht auswertbar - für diesen Prüfpunkt liegt kein auswertbarer Messbeleg vor; das ist weder ein positiver noch ein negativer Befund. Der Einzelbefund nennt eine dokumentierte Messgrenze oder fehlende gespeicherte Angaben. [i] Hinweis - beobachtetes Konfigurationssignal ohne nachgewiesenen Sicherheitsmangel. [-] nicht anwendbar - für den beobachteten Antwortkontext nicht anwendbar; kein bestandener Sicherheitscheck.

CORS-Konfiguration

25 von 25 Punkten

Cross-Origin Resource Sharing steuert, welche Browser-Herkünfte eine Antwort lesen dürfen. Der Check beobachtet die Header einer öffentlichen Antwort ohne Anmeldedaten; tatsächlicher Zugriff auf geschützte Daten wird nicht geprüft.

Im passiven Check wurde kein riskantes CORS-Muster an der eingegebenen URL erkannt. Das ist ein gutes Konfigurationssignal, ersetzt aber keine Prüfung der Authentifizierung oder weiterer Endpoints.

[+] cors-wildcard-credentials · CORS mit Credentials für fremden Test-Origin oder null

Zustand: bestanden | Kennung: cors-wildcard-credentials | Regelgewichtung (kein aktueller negativer Befund): Kritisch | Schadenspotenzial: hoch | Gewicht: 25 Punkte

Geprüft wird: Ob eine GET-Antwort den fremden Test-Origin oder "null" zusammen mit exakt Access-Control-Allow-Credentials: true freigibt. Es werden keine Anmeldedaten gesendet und keine geschützten Daten abgerufen.

Referenzen: CWE-942 | OWASP API8:2023

Referenzen: OWASP API8:2023 · Fehlkonfiguration · Is the API Vulnerable? / How To Prevent · geprüft am 05.10.2026 · <https://api-security.owasp.org/editions/2023/en/0xa8-security-misconfiguration/>

[+] cors-wildcard-credentials-blocked · CORS: Wildcard mit Credentials (vom Browser blockiert)

Zustand: bestanden | Kennung: cors-wildcard-credentials-blocked | Regelgewichtung (kein aktueller negativer Befund): Niedrig | Schadenspotenzial: niedrig | Gewicht: 5 Punkte
Geprüft wird: Ob der Server das buchstäbliche "*" als erlaubte Herkunft sendet und gleichzeitig Credentials erlaubt — eine Kombination, die Browser verweigern und die deshalb Konfigurationshygiene betrifft, nicht Ausnutzbarkeit.

Referenzen: CWE-942 | OWASP API8:2023

Referenzen: OWASP API8:2023 · Fehlkonfiguration · Is the API Vulnerable? / How To Prevent · geprüft am 05.10.2026 · <https://api-security.owasp.org/editions/2023/en/0xa8-security-misconfiguration/>

[+] cors-wildcard · CORS: Wildcard-Origin

Zustand: bestanden | Kennung: cors-wildcard | Regelgewichtung (kein aktueller negativer Befund): Info | Schadenspotenzial: zur Information | Gewicht: 0 Punkte
Geprüft wird: Ob der Server Cross-Origin-Anfragen von jeder Domain erlaubt (Access-Control-Allow-Origin: *), ohne Credentials.

Referenzen: CWE-942 | OWASP API8:2023

Referenzen: OWASP API8:2023 · Fehlkonfiguration · Is the API Vulnerable? / How To Prevent · geprüft am 05.10.2026 · <https://api-security.owasp.org/editions/2023/en/0xa8-security-misconfiguration/>

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

Zustand: bestanden | Kennung: cors-origin-reflection | Regelgewichtung (kein aktueller negativer Befund): Info | Schadenspotenzial: zur Information | Gewicht: 0 Punkte
Geprüft wird: Ob die GET-Antwort einen fremden Test-Origin zurückgibt. Eine einzelne Beobachtung beweist weder beliebige Reflection noch das Fehlen einer internen Allowlist.

Referenzen: CWE-942 | OWASP API8:2023

Referenzen: OWASP API8:2023 · Fehlkonfiguration · Is the API Vulnerable? / How To Prevent · geprüft am 05.10.2026 · <https://api-security.owasp.org/editions/2023/en/0xa8-security-misconfiguration/>

[+] cors-null-origin · CORS: Null-Origin akzeptiert

Zustand: bestanden | Kennung: cors-null-origin | Regelgewichtung (kein aktueller negativer Befund): Info | Schadenspotenzial: zur Information | Gewicht: 0 Punkte
Geprüft wird: Ob der Server den Origin "null" als erlaubte Herkunft akzeptiert — ohne Credentials.

Referenzen: CWE-942 | OWASP API8:2023

Referenzen: OWASP API8:2023 · Fehlkonfiguration · Is the API Vulnerable? / How To Prevent · geprüft am 05.10.2026 · <https://api-security.owasp.org/editions/2023/en/0xa8-security-misconfiguration/>

API-Headers

18 von 18 Punkten

Sicherheitsrelevante Header wie X-Content-Type-Options und Cache-Control schützen vor MIME-Sniffing und ungewolltem Caching.

Die geprüften API-Header zeigen ein gutes Signal: nosniff, Cache-Control und Content-Type wirken im passiven Scope plausibel konfiguriert.

[+] api-response-cacheable · Cookie-setzende Antwort und geteiltes Caching

Zustand: bestanden | Kennung: api-response-cacheable | Regelgewichtung (kein aktueller negativer Befund): Mittel | Schadenspotenzial: mittel | Gewicht: 8 Punkte
Geprüft wird: Ob eine Antwort, die ein Cookie setzt, gleichzeitig von einem geteilten Cache (Proxy/CDN) gespeichert werden darf.

Referenzen: CWE-524 | OWASP API8:2023

Referenzen: OWASP API8:2023 · Fehlkonfiguration · Is the API Vulnerable? / How To Prevent · geprüft am 05.10.2026 · <https://api-security.owasp.org/editions/2023/en/0xa8-security-misconfiguration/>

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

Zustand: bestanden | Kennung: missing-nosniff | Regelgewichtung (kein aktueller negativer Befund): Niedrig | Schadenspotenzial: niedrig | Gewicht: 5 Punkte

Geprüft wird: Ob die Antwort den Header X-Content-Type-Options: nosniff setzt und damit MIME-Sniffing im Browser unterbindet.

Referenzen: CWE-16

Referenzen: OWASP HTTP Headers Cheat Sheet · x-content-type-options · geprüft am 05.10.2026 ·

https://cheatsheetseries.owasp.org/cheatsheets/HTTP-Headers_Cheat_Sheet.html#x-content-type-options

[+] missing-content-type · Content-Type der API-Antwort

Zustand: bestanden | Kennung: missing-content-type | Regelgewichtung (kein aktueller negativer Befund): Niedrig | Schadenspotenzial: niedrig | Gewicht: 3 Punkte

Geprüft wird: Ob eine Antwort mit Repräsentation einen syntaktisch gültigen Medientyp sendet. JSON, XML, Text und Binärdaten können legitime API-Formate sein; Antworten ohne Repräsentation benötigen hierfür keinen Header.

Referenzen: CWE-16

Referenzen: OWASP HTTP Headers Cheat Sheet · content-type · geprüft am 05.10.2026 ·

https://cheatsheetseries.owasp.org/cheatsheets/HTTP-Headers_Cheat_Sheet.html#content-type

Error-Handling

17 von 17 Punkten

Detaillierte Fehlermeldungen wie Stack Traces oder Datenbankfehler geben Angreifern wertvolle Informationen über Ihre Systemarchitektur.

Der einzelne konservative Fehlerantwort-Check hat keine Stack Traces, Datenbankfehler oder internen Pfade erkannt. Das ist kein Fuzzing und keine vollständige Error-Handling-Prüfung.

[+] stack-trace-exposure · Stack Traces in Fehlerantworten

Zustand: bestanden | Kennung: stack-trace-exposure | Regelgewichtung (kein aktueller negativer Befund): Hoch | Schadenspotenzial: hoch | Gewicht: 15 Punkte

Geprüft wird: Ob eine Fehlerantwort der API Stack Traces enthält und damit Dateinamen, Funktionen und die eingesetzte Technologie preisgibt.

Referenzen: CWE-209 | OWASP API8:2023

Referenzen: OWASP API8:2023 · Fehlkonfiguration · Is the API Vulnerable? / How To Prevent · geprüft am 05.10.2026 ·

<https://api-security.owasp.org/editions/2023/en/0xa8-security-misconfiguration/>

[+] database-error-exposure · Datenbank-Fehlermeldungen in Antworten

Zustand: bestanden | Kennung: database-error-exposure | Regelgewichtung (kein aktueller negativer Befund): Hoch | Schadenspotenzial: hoch | Gewicht: 12 Punkte

Geprüft wird: Ob eine Fehlerantwort der API Datenbankmeldungen enthält und damit Tabellen-, Spaltennamen oder SQL preisgibt.

Referenzen: CWE-209 | OWASP API8:2023

Referenzen: OWASP API8:2023 · Fehlkonfiguration · Is the API Vulnerable? / How To Prevent · geprüft am 05.10.2026 ·

<https://api-security.owasp.org/editions/2023/en/0xa8-security-misconfiguration/>

[+] debug-info-exposure · Debug-Informationen in Antworten

Zustand: bestanden | Kennung: debug-info-exposure | Regelgewichtung (kein aktueller negativer Befund): Mittel | Schadenspotenzial: mittel | Gewicht: 10 Punkte

Geprüft wird: Ob die API Debug-Ausgaben liefert, die nur in Entwicklungsumgebungen sichtbar sein sollten.

Referenzen: CWE-489 | OWASP API8:2023

Referenzen: OWASP API8:2023 · Fehlkonfiguration · Is the API Vulnerable? / How To Prevent · geprüft am 05.10.2026 ·

<https://api-security.owasp.org/editions/2023/en/0xa8-security-misconfiguration/>

[+] internal-path-exposure · Interne Dateipfade in Antworten

Zustand: bestanden | Kennung: internal-path-exposure | Regelgewichtung (kein aktueller negativer Befund): Mittel | Schadenspotenzial: mittel | Gewicht: 8 Punkte
Geprüft wird: Ob eine Fehlerantwort absolute Serverpfade enthält und damit Betriebssystem und Verzeichnisstruktur preisgibt.
Referenzen: CWE-200 | OWASP API8:2023
Referenzen: OWASP API8:2023 · Fehlkonfiguration · Is the API Vulnerable? / How To Prevent · geprüft am 05.10.2026 · <https://api-security.owasp.org/editions/2023/en/0xa8-security-misconfiguration/>

Rate-Limiting

Teilbefunde vorhanden; keine belastbare Kategorienpunktzahl. Nicht auswertbare Aspekte sind einzeln gekennzeichnet.

Rate-Limiting reduziert Risiken durch Überlastung, Scraping und automatisierte Fehlversuche. Dieser Check bewertet nur sichtbare Rate-Limit-Header. In diesem Lauf blieb die Kategorie unbewertet: Ein fehlendes sichtbares Signal ist weder ein Schutzbeleg noch der Nachweis einer fehlenden Drosselung.

[i] no-rate-limiting · Rate-Limit-Header

Zustand: Hinweis | Kennung: no-rate-limiting | Regelgewichtung (kein aktueller negativer Befund): Info | Schadenspotenzial: zur Information | Gewicht: 0 Punkte
Geprüft wird: Ob die Antwort Rate-Limit-Signale sendet (RateLimit, RateLimit-Policy, ältere RateLimit-*/X-RateLimit-* oder HTTP 429). Geprüft wird die Sichtbarkeit des Schutzes, nicht seine Wirksamkeit — es läuft kein Belastungstest.

Befund: Keine Rate-Limit-Header erkannt

In der Antwort wurden keine unterstützten Rate-Limit-Signale erkannt. Daraus lässt sich nicht ableiten, ob eine Drosselung fehlt: Limits können unsichtbar, nutzerabhängig oder erst bei Überschreitung erkennbar sein.

Auswirkung: Nur falls wirksame Begrenzungen fehlen, können automatisierte Anfragen Kosten oder Überlastung verursachen. Dieser Scan weist das Fehlen solcher Begrenzungen nicht nach.

Empfehlung [no-rate-limiting]: Prüfen und dokumentieren Sie vorhandene Quoten und den Client-Backoff. Der aktive IETF-Entwurf draft-ietf-httpapi-ratelimit-headers-11 (23.05.2026) verwendet RateLimit und RateLimit-Policy; er ist noch kein RFC. Retry-After kann bei HTTP 429 die Wartezeit als Sekunden oder HTTP-Datum nennen.

Referenzen: CWE-770 | OWASP API4:2023

Referenzen: OWASP API4:2023 · Unbegrenzter Ressourcenverbrauch · Is the API Vulnerable? / How To Prevent · geprüft am 05.10.2026 · <https://api-security.owasp.org/editions/2023/en/0xa4-unrestricted-resource-consumption/>

Server-Informationen

Teilbefunde vorhanden; keine belastbare Kategorienpunktzahl. Nicht auswertbare Aspekte sind einzeln gekennzeichnet.

Server-Header können Versionsinformationen preisgeben, die Angreifer zur Identifikation bekannter Schwachstellen (CVEs) nutzen.

[?] known-cve · Server-Version gegen bekannte Schwachstellen

Zustand: nicht auswertbar | Kennung: known-cve | Regelgewichtung (kein aktueller negativer Befund): Hoch | Schadenspotenzial: hoch | Gewicht: 15 Punkte
Geprüft wird: Ob die aus dem Server-Header gelesene Version in den Versionsbereich öffentlich bekannter Schwachstellen fällt. Rein versionsbasiert — kein Beweis einer aktiven Verwundbarkeit.
Keine ausreichend genaue Produktversion oder keine Einträge für dieses Produkt in der lokalen CVE-Auswahl. Ein Schwachstellenabgleich konnte nicht erfolgen.

Referenzen: CWE-1035 | OWASP API8:2023

Referenzen: OWASP API8:2023 · Fehlkonfiguration · Is the API Vulnerable? / How To Prevent · geprüft am 05.10.2026 · <https://api-security.owasp.org/editions/2023/en/0xa8-security-misconfiguration/>

[+] server-version-exposed · Server-Header mit Versionsangabe

Zustand: bestanden | Kennung: server-version-exposed | Regelgewichtung (kein aktueller negativer Befund): Niedrig | Schadenspotenzial: niedrig | Gewicht: 5 Punkte
Geprüft wird: Ob der Server-Header eine Produktversion nennt und damit gezielte Schwachstellensuche erleichtert.
Referenzen: CWE-200

Referenzen: OWASP HTTP Headers Cheat Sheet · server · geprüft am 05.10.2026 · <https://cheatsheetseries.owasp.org/cheatsheets/HTTP-Headers-Cheat-Sheet.html#server>

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

Zustand: bestanden | Kennung: powered-by-exposed | Regelgewichtung (kein aktueller negativer Befund): Niedrig | Schadenspotenzial: niedrig | Gewicht: 5 Punkte
Geprüft wird: Ob die Antwort einen X-Powered-By-Header sendet und damit die eingesetzte Technologie nennt.
Referenzen: CWE-200

Referenzen: OWASP HTTP Headers Cheat Sheet · x-powered-by · geprüft am 05.10.2026 · <https://cheatsheetseries.owasp.org/cheatsheets/HTTP-Headers-Cheat-Sheet.html#x-powered-by>

HTTP-Methoden

nicht auswertbar (10 mögliche Punkte in dieser Kategorie)

Der Check liest die vom Ziel im Allow-Header angekündigten Methoden. Er führt TRACE, TRACK, CONNECT und zustandsändernde Methoden nicht aus; Berechtigungen und tatsächliche Nutzbarkeit bleiben offen.

[?] xst-vulnerability · TRACE/TRACK-Methoden

Zustand: nicht auswertbar | Kennung: xst-vulnerability | Regelgewichtung (kein aktueller negativer Befund): Mittel | Schadenspotenzial: mittel | Gewicht: 12 Punkte
Geprüft wird: Ob der Server die HTTP-Methoden TRACE oder TRACK im Allow-Header einer OPTIONS-Antwort als aktiviert meldet.

Das Ziel hat die Frage nicht beantwortet - der Check konnte kein Urteil bilden. Es liegt weder ein positiver noch ein negativer Befund vor.

Referenzen: CWE-693 | OWASP API8:2023

Referenzen: OWASP API8:2023 · Fehlkonfiguration · Is the API Vulnerable? / How To Prevent · geprüft am 05.10.2026 · <https://api-security.owasp.org/editions/2023/en/Oxa8-security-misconfiguration/>