Premium API Security Audit Rapport

Analyse: https://jan-karel.nl

Opgesteld voor: **Test**

Door: **BasisHost**

Datum: **3 april 2026**

Inhoudsopgave

Management Samenvatting

Totaalscore: **70/100** (70%) — Cijfer: **B-**. Uw organisatie heeft een goed beveiligingsniveau. De meeste maatregelen zijn geïmplementeerd. Focus op de resterende aandachtspunten en continue verbetering.

Aandachtsgebieden: **Rate Limiting** (0%), **Authenticatie** (65%), **Security Headers** (70%).

Top aanbevelingen: Rate Limit Headers; Retry-After; Auth Vereist.

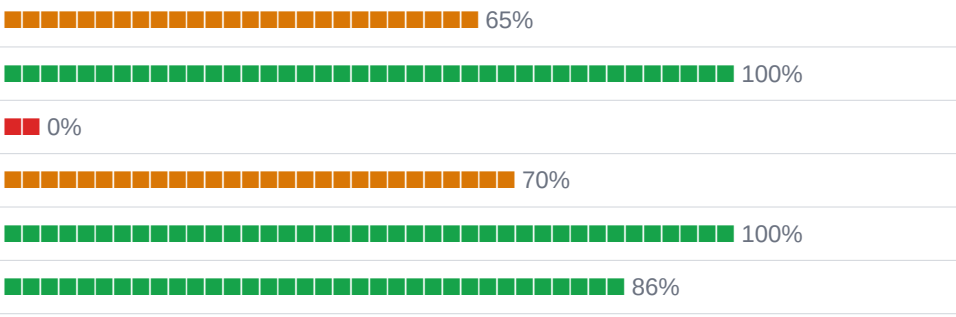
Totaalscore

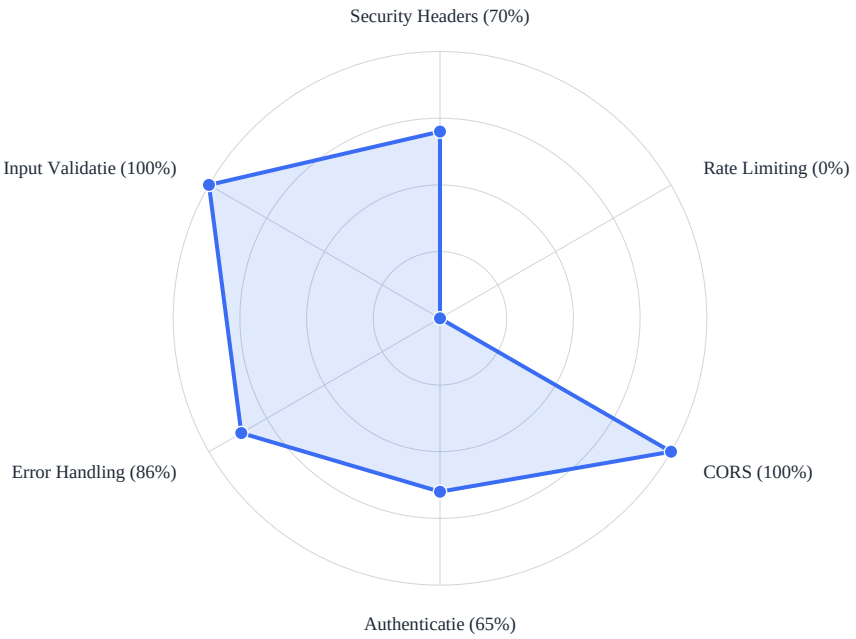
70 / 100

Cijfer: B-

Onderwerp	https://jan-karel.nl
Totaalscore	70/100 (70%)
Cijfer	B-
Rapportdatum	03-04-2026

Scores per Categorie




Security Headers (70%)
Rate Limiting (0%)
CORS (100%)
Authenticatie (65%)
Error Handling (86%)
Input Validatie (100%)

Authenticatie — 65%

Wat is dit? Authenticatie controleert of uw API verifieert wie er verbinding maakt. Zonder goede authenticatie kan iedereen bij uw data.

Wat betekent deze score? Uw authenticatie is voldoende, maar er zijn meerdere punten die verbeterd moeten worden om risico's te verkleinen.

Check	Status	Waarde	Advies
Auth Vereist	■ WARN	200 OK zonder credentials — mogelijk publiek	Overweeg authenticatie toe te voegen als dit geen publiek endpoint is.
Auth Scheme	■ WARN	Niet gedetecteerd	Implementeer token-gebaseerde authenticatie.
API Key in URL	✓ PASS	Geen credentials in URL	
HTTPS	✓ PASS	Endpoint gebruikt HTTPS	

CORS — 100%

Wat is dit? CORS bepaalt welke andere websites uw API mogen gebruiken. Verkeerde instellingen kunnen ertoe leiden dat kwaadwillende websites bij uw gegevens kunnen.

Wat betekent deze score? Uw cors is uitstekend ingericht. Er zijn geen dringende verbeterpunten gevonden.

Check	Status	Waarde	Advies
CORS Origin	✓ PASS	Geen CORS headers — standaard restrictief	
CORS Credentials	✓ PASS	Geen credentials header of uitgeschakeld	
CORS Methods	✓ PASS	Geen CORS methods header	

Rate Limiting — 0%

Wat is dit? Rate Limiting beperkt het aantal verzoeken dat iemand per tijdseenheid mag doen. Zonder limiet kan een aanvaller uw server overbelasten.

Wat betekent deze score? Uw rate limiting scoort kritiek laag. Directe actie is vereist om ernstige risico's te voorkomen.

Check	Status	Waarde	Advies
Rate Limit Headers	✗ FAIL	Geen rate limit headers gevonden	Implementeer rate limiting met X-RateLimit-* headers.
Retry-After	✗ FAIL	Niet aanwezig	Implementeer Retry-After header.
429 Status	■ WARN	Geen rate limiting gedetecteerd	Configureer 429 responses bij te veel verzoeken.

Security Headers — 70%

Wat is dit? Security Headers zijn extra beveiligingsinstructies die uw API meestuurt. Ze beschermen tegen veelvoorkomende aanvallen.

Wat betekent deze score? Uw security headers is goed op orde, maar er zijn enkele verbeterpunten die aandacht verdienen.

Check	Status	Waarde	Advies
Content-Type	■ WARN	text/html; charset=utf-8	APIs dienen application/json te gebruiken.
X-Content-Type-Options	✓ PASS	nosniff	
Cache-Control	■ WARN	public, max-age=0	Gebruik no-store of private voor API responses met gevoelige data.
Frame Protection	✓ PASS	SAMEORIGIN	
Server Info Leakage	■ WARN	nginx	Verberg server informatie in response headers.

Input Validatie — 100%

Wat is dit? Input Validatie controleert of uw API invoer van gebruikers goed controleert. Ongecontroleerde invoer is de meest voorkomende oorzaak van hacks.

Wat betekent deze score? Uw input validatie is uitstekend ingericht. Er zijn geen dringende verbeterpunten gevonden.

Check	Status	Waarde	Advies
SQL Injection	✓ PASS	Geen SQL foutmelding	
XSS Payload	✓ PASS	XSS payload wordt niet ongescaped weergegeven	
Path Traversal	✓ PASS	Geen path traversal gedetecteerd	

Error Handling — 86%

Wat is dit? Error Handling beoordeelt of foutmeldingen van uw API geen gevoelige technische informatie lekken die aanvallers kunnen misbruiken.

Wat betekent deze score? Uw error handling is uitstekend ingericht. Er zijn geen dringende verbeterpunten gevonden.

Check	Status	Waarde	Advies
404 Response	✓ PASS	Correcte 404 status code	
Stack Trace Leakage	✓ PASS	Geen stack traces in error responses	
Error Format	■ WARN	Kon error formaat niet bepalen	Gebruik JSON voor alle API responses.
Verbose Errors	✓ PASS	Geen verbose errors gedetecteerd	

Aanbevelingen

Geprioriteerde aanbevelingen op basis van de analyse.

Prio	Categorie	Titel	Beschrijving	Doorlooptijd
Hoog	Rate Limiting	**Rate Limit Headers**	Implementeer rate limiting met X-RateLimit-* headers.	2 uur
Hoog	Rate Limiting	**Retry-After**	Implementeer Retry-After header.	30 minuten
Middel	Authenticatie	**Auth Vereist**	Overweeg authenticatie toe te voegen als dit geen publiek endpoint is.	2 uur
Middel	Authenticatie	**Auth Scheme**	Implementeer token-gebaseerde authenticatie.	1 uur
Middel	Rate Limiting	**429 Status**	Configureer 429 responses bij te veel verzoeken.	1 uur
Middel	Security Headers	**Content-Type**	APIs dienen application/json te gebruiken.	15 minuten
Middel	Security Headers	**Cache-Control**	Gebruik no-store of private voor API responses met gevoelige data.	15 minuten
Middel	Security Headers	**Server Info Leakage**	Verberg server informatie in response headers.	15 minuten
Middel	Error Handling	**Error Format**	Gebruik JSON voor alle API responses.	1 uur

Bijlage: Invoergegevens

API URL	https://jan-karel.nl

Bijlage A: Begrippen en Afkortingen

Onderstaande lijst verklaart de belangrijkste termen en afkortingen die in dit rapport worden gebruikt.

Term	Betekenis
API	Application Programming Interface — een manier waarop computersystemen met elkaar communiceren, vergelijkbaar met een digitaal loket.
AVG	Algemene Verordening Gegevensbescherming — Europese privacywetgeving (ook wel GDPR).
BCP	Business Continuity Plan — plan om bedrijfsprocessen voort te zetten bij verstoringen.
BIA	Business Impact Analysis — analyse van de gevolgen van uitval van systemen of processen.
CISO	Chief Information Security Officer — eindverantwoordelijke voor informatiebeveiliging.
CORS	Cross-Origin Resource Sharing — beveiliging die bepaalt welke andere websites uw API mogen gebruiken.
CVE	Common Vulnerabilities and Exposures — gestandaardiseerd identificatiesysteem voor kwetsbaarheden.
DRP	Disaster Recovery Plan — plan voor herstel van IT-systemen na een calamiteit.
EDR	Endpoint Detection & Response — beveiligingssoftware die verdachte activiteit op werkstations en servers detecteert en blokkeert.
IAM	Identity & Access Management — beheer van digitale identiteiten en toegangsrechten.
IR-plan	Incident Response Plan — vastgelegde procedures voor het afhandelen van beveiligingsincidenten.
MFA	Multi-Factor Authenticatie — inloggen met twee of meer verificatiestappen (bijv. wachtwoord + app-code).
NIS2	Network and Information Security Directive 2 — Europese richtlijn die cybersecurity-eisen stelt aan essentiële en belangrijke entiteiten.
NIST CSF	National Institute of Standards and Technology Cyber Security Framework — internationaal raamwerk voor cybersecurity.
PAM	Privileged Access Management — beheer en beveiliging van accounts met verhoogde rechten.
Rate limiting	Beperking op het aantal verzoeken dat iemand mag doen in een bepaalde tijd, ter bescherming tegen misbruik.
RPO	Recovery Point Objective — maximaal acceptabel dataverlies, uitgedrukt in tijd.
RTO	Recovery Time Objective — maximaal acceptabele tijd om een systeem te herstellen na uitval.
SIEM	Security Information & Event Management — systeem dat beveiligingslogs verzamelt, correleert en alarmeert.
SOC	Security Operations Center — team dat 24/7 beveiligingsincidenten monitort en afhandelt.
XDR	Extended Detection & Response — geïntegreerde detectie over endpoints, netwerk en cloud.

Dit rapport is opgesteld door **BasisHost**.

Rapport gegenereerd op 3 april 2026. De resultaten zijn gebaseerd op door de klant verstrekte informatie. Dit rapport vervangt geen professionele security audit of pentest. BasisHost is niet aansprakelijk voor beslissingen genomen op basis van dit rapport zonder aanvullend professioneel advies.