LUCAS KIT

SITESTRESS / ANALYSIS / (v3.4.5)

22-02-2026 (cyberbrein.nl)

Algemene gegevens van scan

Domein:
cyberbrein.nl

IP:
Onbekend

Latency:
Onbekend

Server Header:
Onbekend

Executive Summary

In deze scan analyseert Lucas Kit het aangegeven doelwit op mogelijke blootstellingen en configuratiefouten. Binnen deze rapportage vindt u informatie over:
- DNS/Mail Configuratie Beveiliging
- HTTP Headers & Certificaat Validatie
- DDoS Volumetrische Resistentie
- Beheerders-poorten en datalek-paden.

Scope

- In scope: cyberbrein.nl en geidentificeerde gerelateerde subdomeinen.
- Out of scope: VPNs, Interne infrastructuren, Externe applicaties niet publiek georienteerd op dit domein.

Methodologie

Dit document is geunificeerd middels CLI tools (SiteStress & UltraDNS) en bevat exacte acties met timestamps. De onderliggende data is tevens als machine-leesbare JSON bestanden gegenereerd.

Tools & Environment

- SiteStress 3.4.5
- ultradns 3.4.5
- macOS / Linux

LUCAS
KIT

SITESTRESS / ANALYSIS / (v3.4.5)

22-02-2026 (cyberbrein.nl)

DNS Configuratie & Mail Security

Resolutie Data

Mail Security (DMARC, SPF, DKIM)

DKIM: map[]

DMARC: v=DMARC1; p=none; rua=mailto:support@itv360.net; adkim=s; rua=mailto:dmarc@inbound.flowmailer.net; ruf=mailto:dmarc@inbou

MTA-STS: Niet ingesteld

MX: map[mail.cyberbrein.nl:[188.68.47.56] mx2f38.netcup.net:[188.68.47.56]]

SPF: v=spf1 mx a include:_spf.webhosting.systems include:spf.flowmailer.net ~all

TLS-RPT: Niet ingesteld

LUCAS
KIT

SITESTRESS / ANALYSIS / (v3.4.5)

22-02-2026 (cyberbrein.nl)

Port Scans & Path Discovery

Open Poorten

Geidentificeerde open poorten via TLS TCP connecties: 8443, 80, 22, 53, 443

Path HTTP Status Responses

/robots.txt : HTTP 200
/sitemap.xml : HTTP 301
/.env : HTTP 404
/.git/config : HTTP 404
/.well-known/security.txt : HTTP 404

LUCAS KIT

SITESTRESS / ANALYSIS / (v3.4.5)

22-02-2026 (cyberbrein.nl)

Findings & Aanbevelingen

Finding #1: TLS Certificaat verloopt binnenkort

Severity: **MEDIUM**

Description:

Het certificaat is geldig voor minder dan 14 dagen.

Evidence:

Dagen resterend: 5

Recommendation:

Vernieuw het TLS certificaat zo snel mogelijk.

Finding #2: CSP ontbreekt

Severity: **MEDIUM**

Description:

Content-Security-Policy header is niet ingesteld.

Evidence:

CSP: MISSING

Recommendation:

Stel een CSP in om XSS-aanvallen te mitigeren.

Finding #3: Gevaarlijke poorten blootgesteld

Severity: **HIGH**

Description:

Er zijn direct toegankelijke beheer- of databasepoorten ontdekt via het publieke IP adres.

Evidence:

Open ports: 22

Recommendation:

Sluit deze poorten af via een firewall of beperk toegang uitsluitend tot vertrouwde (VPN) IPs.

Finding #4: Technologie & Frameworks Gedetecteerd

Severity: **INFO**

Description:

Er zijn specifieke CMS systemen of web-technologieen herkend via HTML body of Headers.

Evidence:

Detecies: Nginx

Recommendation:

Zorg ervoor dat alle gedetecteerde componenten up-to-date zijn ivm CVE risicos.

Finding #5: Interessante Fuzzing Directories Gevonden

Severity: **HIGH**

Description:
Via directory bruteforcing is directe toegang tot administratieve backends of database gerelateerde paden vastgesteld.
Evidence:
Positieve Fuzzing paden: /wp-admin (HTTP 200), /admin (HTTP 200), /dashboard (HTTP 200), /login (HTTP 200)
Recommendation:
Sluit deze paden direct af, minimaliseer error codes of verplaats authenticatie interfaces achter gesloten firewalls.

Finding #6: Geen AI Web-Crawler Beveiliging Gespot

Severity: **INFO**
Description:
De site verbiedt LLM aggregators (zoals GPTBot, ClaudeBot, Perplexity) niet via robots.txt, waardoor interne open data gebruikt kan worden voor AI model training.
Evidence:
Robots.txt mist specifieke Disallow regels voor bekende LLM user-agents.
Recommendation:
Indien data privacy en copyright extractie een zorg is, voeg LLM spiders toe aan robots.txt Disallow blokkades.

Risk Rating Overzicht

Issue	Severity	Status
TLS Certificaat verloopt binnenkort	MEDIUM	Open
CSP ontbreekt	MEDIUM	Open
Gevaarlijke poorten blootgesteld	HIGH	Open
Technologie & Frameworks Gedetecteerd	INFO	Open
Interessante Fuzzing Directories Gevonden	HIGH	Open
Geen AI Web-Crawler Beveiliging Gespot	INFO	Open

LUCAS
KIT

SITESTRESS / ANALYSIS / (v3.4.5)

22-02-2026 (cyberbrein.nl)

Legal / Appendix

Legal Notice

Dit document en de scanresultaten zijn uitsluitend bestemd voor gebruik door bevoegde personen. De Lucas Kit (ultradns / sitestress / lucaskit modules) en de auteur hiervan, Lucas Mangroelal, getoetst te worden door een gediplomeerde pentester alvorens beslissingen worden doorgevoerd.