# *Vooronderzoek Cybersecurity*

## Voorbeeld B.V.

**Opgesteld door:** Ethical Hacker Group International B.V. (EHGI)
in samenwerking met BOEM Cybersecurity B.V.

**Datum:** 18 maart 2026

**Classificatie:** Vertrouwelijk

**Referentie:** EHGI-2026-VBD-001

# 2. Management Samenvatting

Dit vooronderzoek brengt het externe aanvalsoppervlak van Voorbeeld B.V. in kaart. De resultaten tonen een **significant aanvalsoppervlak** met meerdere bevindingen die directe aandacht vereisen.

| | | | |
|---|---|---|---|
| **4** DOMEINEN ONDERZOCHT | **23** SUBDOMEINEN | **31** HTTP SERVICES | **18** TECHNOLOGIEËN |
| **12** CVE'S GEVONDEN | **2** KNOWN EXPLOITED (KEV) | **18** GELEKTE CREDENTIALS | **Hoog** RISICO-INDICATIE |

## TOP URGENTE ACTIEPUNTEN

### 1. Gelekte credentials met plaintext wachtwoorden

Er zijn 18 gelekte credentials gevonden waarvan 4 met plaintext wachtwoorden. Deze moeten direct worden gereset en de getroffen accounts moeten worden beveiligd met MFA.

### 2. Known Exploited Vulnerabilities (KEV) aanwezig

Er zijn 2 kwetsbaarheden gevonden die actief worden misbruikt door kwaadwillenden (CISA KEV). Deze moeten met de hoogste prioriteit worden gepatcht.

### 3. Verouderde webserver software

Meerdere services draaien op verouderde Apache en Nginx versies met bekende kwetsbaarheden. Update naar de laatste stabiele versies.

### 4. Ontbrekende e-mail authenticatie

Het domein mail.voorbeeld.nl heeft geen DMARC-beleid geconfigureerd, waardoor e-mail spoofing mogelijk is.

# 3. Extern Aanvalsoppervlak

## 3.1 Domein Portfolio

| DOMEIN | TYPE | BESCHRIJVING |
|---|---|---|
| voorbeeld.nl | Primair | Corporate website |
| mijn.voorbeeld.nl | Portaal | Klantenportaal |
| api.voorbeeld.nl | API | REST API |
| voorbeeld-intern.nl | Intern | Interne tooling |

## 3.2 Ontdekte Subdomeinen

In totaal **23 subdomeinen**. Selectie:

| SUBDOMEIN |
|---|
| www.voorbeeld.nl |
| mail.voorbeeld.nl |
| mijn.voorbeeld.nl |
| api.voorbeeld.nl |
| cdn.voorbeeld.nl |
| wiki.voorbeeld-intern.nl |
| gitlab.voorbeeld-intern.nl |
| jenkins.voorbeeld-intern.nl |
| ... +15 meer |

## 3.3 HTTP/HTTPS Services

**8 webservices** gedetecteerd:

| URL | IP | SERVER | TECH |
|---|---|---|---|
| https://www.voorbeeld.nl | 198.51.100.10 | Apache/2.4.49 | WordPress 6.4, PHP 8.1, jQuery 3.6 |
| https://mijn.voorbeeld.nl | 198.51.100.11 | Nginx/1.24 | React 18, Node.js |
| https://api.voorbeeld.nl | 198.51.100.12 | Nginx/1.24 | Express.js, Swagger UI |
| https://staging.voorbeeld.nl | 198.51.100.10 | Apache/2.4.49 | WordPress 6.2, PHP 8.0 |
| https://crm.voorbeeld.nl | 198.51.100.15 | Apache/2.4.58 | SuiteCRM 7.14, PHP 8.1 |

| | | | |
|---|---|---|---|
| https://webmail.voorbeeld.nl | 198.51.100.10 | Nginx/1.22 | Roundcube 1.6 |

… +2 meer

# 5. Kwetsbaarheden & CVE's

Op basis van de gedetecteerde software en versies zijn **12 unieke CVE's** geïdentificeerd.

| 3 | 4 | 5 |
|---|---|---|
| KRITIEK | HOOG | MIDDEL |

## KNOWN EXPLOITED VULNERABILITIES (KEV)

> **2 kwetsbaarheden worden actief misbruikt in het wild**
>
> De volgende CVE's staan op de CISA Known Exploited Vulnerabilities catalogus.

| CVE | CVSS | ERNST | EPSS | COMPONENT |
|---|---|---|---|---|
| CVE-2021-41773 | 9.8 | KRITIEK KEV | 97.2% | Apache 2.4.49 |
| CVE-2024-21762 | 9.8 | KRITIEK KEV | 94.1% | FortiOS SSL-VPN |

## TOP CVE'S

| CVE | CVSS | ERNST | EPSS | COMPONENT |
|---|---|---|---|---|
| CVE-2021-41773 | 9.8 | KRITIEK | 97.2% | Apache 2.4.49 |
| CVE-2024-21762 | 9.8 | KRITIEK | 94.1% | FortiOS SSL-VPN |
| CVE-2024-3400 | 9.1 | KRITIEK | 88.7% | Palo Alto PAN-OS |
| CVE-2023-44228 | 7.5 | HOOG | 45.3% | Apache Struts |
| CVE-2023-32315 | 7.5 | HOOG | 67.8% | Jenkins |
| CVE-2023-22518 | 7.2 | HOOG | 52.1% | SuiteCRM 7.14 |
| CVE-2023-0669 | 7.2 | HOOG | 41.9% | Grafana 10.1 |

# 6. Gelekte Credentials

In bekende datalek databases zijn **24 records** gevonden gekoppeld aan e-mailadressen van Voorbeeld B.V.. Van deze records bevatten **18 een blootgesteld wachtwoord of wachtwoord-hash**, waaronder **4 wachtwoorden in leesbare tekst**.

| 24 | 18 | 4 |
|---|---|---|
| TOTAAL RECORDS | MET WACHTWOORD / HASH | LEESBARE WACHTWOORDEN |

> **Directe dreiging: Leesbare wachtwoorden in datalekken**
>
> 4 accounts hebben wachtwoorden die in leesbare tekst beschikbaar zijn in datalek databases. Als deze wachtwoorden hergebruikt worden voor bedrijfsaccounts, kan een aanvaller direct inloggen.

## BLOOTGESTELDE CREDENTIALS (GEDEELTELIJK GEREDACTEERD)

| E-MAILADRES | TYPE | WACHTWOORD / HASH | BRON |
|---|---|---|---|
| j.jansen@voorbeeld.nl | PLAINTEXT | Welkom2024! | Data breach 2024 |
| admin@voorbeeld.nl | SHA-256 | a3f2b8c1d4... | Database dump 2023 |
| p.devries@voorbeeld.nl | PLAINTEXT | Voorbeeld#1 | Combolist 2024 |
| m.bakker@voorbeeld.nl | BCRYPT | $2b$10$xK9... | Credential stuffing DB |
| it-beheer@voorbeeld.nl | PLAINTEXT | Admin123! | Stealer log 2024 |
| r.smit@voorbeeld.nl | MD5 | 5d41402abc... | LinkedIn breach |
| h.degraaf@voorbeeld.nl | SHA-1 | aaf4c61ddc... | Data breach 2023 |
| s.vandam@voorbeeld.nl | PLAINTEXT | Zomer2023! | Stealer log 2024 |