VOORBEELD RAPPORT

Atlas Sentinel

Security Intelligence Rapport

Rapport voor:	**Testbedrijf B.V.**
Datum:	**4 april 2026**
Classificatie:	**VERTROUWELIJK**
Gegenereerd door:	**Atlas Sentinel**
Modules:	**E-mailbeveiliging, Infrastructuur, SSL / Certificaten, Aanvalsoppervlak, Website Hygiene**

GEMIDDELD

47

Dit rapport is gebaseerd op passieve analyse van publiek beschikbaar informatie.
Verspreiding buiten de ontvanger is niet toegestaan zonder schriftelijke toestemming.

Atlas Cybersecurity

www.atlas-cybersecurity.nl · rtsb@atlas-cybersecurity.nl

INTRODUCTIE

Introductie

Wat behelst dit rapport?

Dit rapport is opgesteld door Atlas Sentinel en biedt een extern risicoprofiel van testbedrijf.nl op basis van publiek beschikbare informatie. Er is geen toegang gevraagd tot interne systemen; alle bevindingen zijn afgeleid van bronnen die ook voor kwaadwillenden zichtbaar zijn.

Het rapport is geschreven in begrijpelijke taal voor eigenaren en directeuren, aangevuld met technische instructies in de bijlage voor IT-beheerders. Elke bevinding bevat een risicoclassificatie, een uitleg van de impact en concrete aanbevelingen met tijdsinschatting en kostenniveau.

Afgenomen modules

De volgende onderdelen zijn opgenomen in dit rapport:

• **E-mailbeveiliging** — Kunnen criminelen e-mails sturen namens uw bedrijf?

• **Infrastructuur** — Welke toegangen staan open naar uw systemen?

• **SSL / Certificaten** — Is communicatie met uw systemen beveiligd?

• **Aanvalsoppervlak** — Hoe groot is uw zichtbare digitale voetafdruk?

• **Website Hygiene** — Voldoet uw website aan moderne beveiligingsstandaarden?

Hoe leest u dit rapport?

Risicoscore per module	Elke module heeft een score van 0 tot 100. Een hogere score betekent meer risico. De algehele score is een gewogen gemiddelde van alle modules.
Ernst van bevindingen	Bevindingen zijn ingedeeld als KRITIEK, HOOG, GEMIDDELD of LAAG. Kritieke en hoge bevindingen vereisen de meeste aandacht.
Kans-indicator	Elke bevinding toont de kans op misbruik: GROOT, GEMIDDELD of KLEIN, gebaseerd op gangbare aanvalstechnieken en beschikbare gegevens.
Actieplan (bijlage)	De bijlage bevat stap-voor-stap instructies per bevinding, gesorteerd op urgentie. U kunt dit doorgeven aan uw hostingprovider of IT-partner.
Classificatie	Dit rapport is vertrouwelijk en uitsluitend bestemd voor de ontvanger. Rapport gegenereerd op 4 april 2026.

NAVIGATIE

Inhoudsopgave

METHODOLOGIE

Scoringstabel

Hoe wordt de risicoscore berekend?

Ernst (basispunten)	Kritiek 55 · Hoog 35 · Gemiddeld 20 · Laag 7
Exploiteerbaarheid	Actief misbruikt ×1.5 · Publieke exploit ×1.25 · Theoretisch ×1.0
Business impact	Kritiek ×1.3 · Hoog ×1.2 · Gemiddeld ×1.1 · Laag ×1.0
Eindscore	Ernst × Exploiteerbaarheid × Business impact
Modulescore	Som van alle bevindingen in de module, gemaximeerd op 100
Totaalscore	Gewogen gemiddelde van alle afgenomen modules

Risiconiveaus

Score	Niveau	Betekenis
0 – 25	**Laag**	Beperkte kwetsbaarheden
26 – 50	**Gemiddeld**	Aandacht aanbevolen
51 – 75	**Hoog**	Urgente aanpak noodzakelijk
76 – 100	**Kritiek**	Directe actie vereist

Bevindingen per module

Module	Bevinding	Ernst	Exploit.	Impact	Score
E-mailbeveiliging	DMARC ontbreekt — e-mail spoofing mogelijk	HOOG	Publieke exploit	Hoog ×1.2	**52.5**
	SPF staat op soft fail (~all)	GEMIDDELD	Theoretisch	Gem. ×1.1	**22.0**
Modulescore	(som gemaximeerd op 100)				**74**
SSL / Certificaten	Subdomain certificaat verloopt binnen 14 dagen	GEMIDDELD	Publieke exploit	Hoog ×1.2	**30.0**
Modulescore	(som gemaximeerd op 100)				**30**

Website Hygiene	HTTP zonder redirect naar HTTPS	HOOG	Publieke exploit	Hoog ×1.2	**52.5**
	Geen HSTS-header	GEMIDDELD	Theoretisch	Gem. ×1.1	**22.0**
	Geen CSP-header	GEMIDDELD	Theoretisch	Gem. ×1.1	**22.0**
Modulescore	(som gemaximeerd op 100)				**96**

REFERENTIE

Begrippen & Definities

In dit rapport worden technische termen gebruikt. Hieronder vindt u een verklaring van de belangrijkste begrippen in begrijpelijke taal.

CVE	Common Vulnerabilities and Exposures. Een internationaal genummerde lijst van bekende beveiligingslekken in software en systemen. Een CVE-nummer (bijv. CVE-2021-44228) verwijst naar een specifiek, publiek gedocumenteerd lek met bijbehorende ernst en impact.
CVSS	Common Vulnerability Scoring System. Een schaal van 0,0 tot 10,0 die de ernst van een beveiligingslek beoordeelt. Een score van 9,0 of hoger is kritiek; onder 4,0 is laag.
DMARC	Domain-based Message Authentication, Reporting and Conformance. Een e-mailstandaard die bepaalt wat er moet gebeuren met e-mails die de identiteitscontroles (SPF en DKIM) niet doorstaan. Zonder DMARC kunnen criminelen ongehinderd e-mails sturen alsof ze van uw organisatie komen.
SPF	Sender Policy Framework. Een DNS-instelling die bepaalt welke mailservers e-mail mogen versturen namens uw domein. Ontbreekt deze instelling, dan kunnen derden ongehinderd e-mails sturen die zogenaamd van uw adres afkomstig zijn.
DKIM	DomainKeys Identified Mail. Een digitale handtekening die wordt toegevoegd aan uitgaande e-mails, waarmee ontvangers kunnen verifiëren dat de e-mail daadwerkelijk van uw domein afkomstig is en onderweg niet is aangepast.
RDP	Remote Desktop Protocol. Een protocol van Microsoft voor het op afstand bedienen van een Windows-computer via het internet. Als RDP-toegang open staat zonder extra beveiliging, vormt dit een veelgebruikt aanvalspad voor ransomware-aanvallen.
MFA	Multi-Factor Authenticatie. Een beveiligingsmaatregel waarbij u naast uw wachtwoord een tweede verificatiestap doorloopt. Hierdoor is een gestolen wachtwoord alleen niet genoeg voor een aanvaller om in te loggen.
HSTS	HTTP Strict Transport Security. Een beveiligingsinstelling die browsers instrueert om uw website altijd via een beveiligde HTTPS-verbinding te laden. Dit beschermt bezoekers tegen man-in-the-middle aanvallen.
CSP	Content Security Policy. Een beveiligingsheader die bepaalt welke externe bronnen mogen laden op uw website. Dit verkleint sterk het risico op script-injectieaanvallen (XSS).
TLS / SSL	Transport Layer Security / Secure Sockets Layer. Protocollen die de verbinding tussen een browser en uw website versleutelen. Verlopen of zwakke certificaten betekenen dat de versleuteling niet gegarandeerd is.
DNSSEC	Domain Name System Security Extensions. Een uitbreiding op het DNS-systeem die DNS-antwoorden cryptografisch ondertekent. Dit voorkomt dat aanvallers uw bezoekers omleiden naar valse websites.

Phishing	Een aanvalstechniek waarbij criminelen zich voordoen als een betrouwbare partij om inloggegevens of geld te stelen, meestal via e-mail of een valse website.
Ransomware	Schadelijke software die bestanden op uw systemen versleutelt en een losgeld eist. Ransomware-aanvallen beginnen vaak via onbeveiligde toegangen of phishing-e-mails.
Darkweb	Een afgeschermd deel van het internet dat alleen toegankelijk is via speciale software. Criminelen verhandelen hier gestolen data, wachtwoorden en toegang tot gehackte systemen.

HOOFDSTUK 1

E-mailbeveiliging

Inleiding

Dit hoofdstuk analyseert de DNS-beveiligingsinstellingen van uw e-maildomein. Via publiek beschikbare DNS-records is vastgesteld of uw domein beschermd is tegen e-mailfraude en identiteitsvervalsing (spoofing).

Doel van dit hoofdstuk

Vaststellen of criminelen e-mails kunnen sturen namens uw organisatie, en of uw e-mailcommunicatie verplichte authenticatie vereist van alle verzenders.

Scope

DNS-records (SPF, DKIM, DMARC) van het domein testbedrijf.nl en bijbehorende subdomeinen.

Resultaten

[HOOG] DMARC ontbreekt — e-mail spoofing mogelijk

Kans: GEMIDDELD

Het domein testbedrijf.nl heeft geen DMARC-record. Hierdoor ontbreekt handhaving: e-mailadressen van dit domein kunnen worden nagebootst door aanvallers. Ontvangers van nep-e-mails hebben geen technisch middel om de echtheid te verifiëren.

Wat kan er gebeuren?	Criminelen sturen e-mails die er precies uitzien als berichten van Testbedrijf B.V.. Medewerkers, klanten of leveranciers worden misleid om betalingen te doen, inloggegevens te delen of bijlagen te openen.
Aanbeveling:	Stel een DMARC-record in via uw DNS-beheer. Begin met p=none (monitoring), daarna p=quarantine. Atlas helpt u bij de juiste configuratie.

[GEMIDDELD] SPF staat ingesteld op soft fail (~all)

Kans: KLEIN

Het SPF-record van testbedrijf.nl staat op ~all (soft fail). Dit betekent dat niet-geautoriseerde verzenders wel e-mails kunnen versturen, maar dat deze als verdacht worden gemarkeerd. Een harde afwijzing (-all) is aanbevolen.

Wat kan er gebeuren?	E-mails vanuit onbevoegde bronnen komen toch aan bij ontvangers. Sommige e-mailsystemen behandelen soft fail als acceptabel en bezorgen de e-mail gewoon.
Aanbeveling:	Wijzig het SPF-record van testbedrijf.nl van ~all naar -all. Test daarna met MXToolbox of alle legitieme verzenders nog correct werken.

Conclusie

De e-mailbeveiliging van testbedrijf.nl is onvolledig. DMARC ontbreekt volledig, waardoor e-mailadressen nagebootst kunnen worden. SPF is aanwezig maar niet streng geconfigureerd. Directe actie op DMARC is noodzakelijk. 2 maatregelen vereisen aandacht.

HOOFDSTUK 2

Infrastructuur & Open Toegangen

Inleiding

Dit hoofdstuk inventariseert de extern zichtbare netwerktoegang van uw systemen. Via openbare bronnen zijn de open poorten, diensten en bekende kwetsbaarheden van uw IP-adressen in kaart gebracht.

Doel van dit hoofdstuk

In kaart brengen welke netwerktoegang beschikbaar is voor buitenstaanders, en of er bekende kwetsbaarheden (CVE's) aanwezig zijn die misbruikt kunnen worden.

Scope

IP-adressen en open poorten van hosts gekoppeld aan het domein testbedrijf.nl. Geanalyseerde IP-adressen: 198.51.100.42, 198.51.100.87.

Resultaten

[HOOG] Verouderde webserver aangetroffen — CVE-2021-41773

Kans: GROOT

Op poort 8080 draait Apache 2.4.49, een versie met een kritieke kwetsbaarheid (CVE-2021-41773). Deze kwetsbaarheid maakt het mogelijk voor aanvallers om bestanden buiten de webroot te lezen en in sommige gevallen code uit te voeren op de server.

Wat kan er gebeuren?	Een aanvaller kan via een eenvoudige webaanvraag toegang krijgen tot vertrouwelijke bestanden op uw server, of in het ergste geval volledige controle overnemen. Actieve exploits voor deze kwetsbaarheid zijn publiek beschikbaar.
Aanbeveling:	Update Apache onmiddellijk naar de meest recente versie (2.4.62 of hoger). Schakel port 8080 af als het niet in gebruik is.

[GEMIDDELD] Databasepoort (3306) publiek bereikbaar

Kans: GEMIDDELD

Poort 3306 (MySQL) is bereikbaar vanaf het internet. Een database die direct toegankelijk is, vergroot het aanvalsoppervlak aanzienlijk. Brute-force aanvallen op databasewachtwoorden zijn eenvoudig uit te voeren.

Wat kan er gebeuren?	Aanvallers kunnen direct inlogpogingen doen op uw database. Bij een zwak wachtwoord of bekende kwetsbaarheid in de databasesoftware is volledige toegang tot bedrijfsdata mogelijk.

Aanbeveling: Blokkeer poort 3306 in uw firewall voor alle externe verbindingen. Databasetoegang moet uitsluitend intern of via VPN beschikbaar zijn.

Conclusie

De externe infrastructuur van testbedrijf.nl vertoont twee kwetsbaarheden die direct aandacht vereisen. De verouderde Apache-versie met bekende CVE vormt het grootste risico. 2 maatregelen vereisen aandacht.

HOOFDSTUK 3

SSL / TLS & Certificaten

Inleiding

Dit hoofdstuk beoordeelt de versleuteling van de communicatie met uw systemen. SSL/TLS-certificaten zorgen voor een beveiligde verbinding; verlopen of zwakke certificaten vormen een direct beveiligingsrisico.

Scope

SSL/TLS-certificaten en cipher suites van de hosts onder het domein testbedrijf.nl.

Resultaten

[GEMIDDELD] Subdomain certificaat verloopt binnen 14 dagen Kans: GEMIDDELD

Het SSL-certificaat van mail.testbedrijf.nl verloopt over 13 dagen. Na het verlopen van het certificaat tonen browsers een beveiligingswaarschuwing en weigeren sommige e-mailclients verbinding te maken.

Wat kan er gebeuren?	Bezoekers en medewerkers krijgen een "Uw verbinding is niet beveiligd" melding. E-mailverkeer via dit subdomain kan onderbroken worden. Het vertrouwen van klanten in uw organisatie wordt beschadigd.
Aanbeveling:	Vernieuw het certificaat van mail.testbedrijf.nl vóór de vervaldatum. Stel automatische verlenging in via uw hostingprovider of Let's Encrypt.

Conclusie

Het primaire domein testbedrijf.nl heeft een geldig certificaat met moderne TLS 1.3 configuratie. Het subdomain mail.testbedrijf.nl vereist urgente actie vanwege de naderende vervaldatum. 1 maatregel vereist aandacht.

HOOFDSTUK 4

Aanvalsoppervlak & Zichtbaarheid

Inleiding

Dit hoofdstuk inventariseert uw digitale voetafdruk: hoeveel subdomeinen, services en toegangen extern zichtbaar zijn. Hoe groter het aanvalsoppervlak, hoe meer aanvalsvectoren beschikbaar zijn.

Scope

Subdomeinen en publieke services van testbedrijf.nl. Gevonden subdomeinen: 4.

Resultaten

Subdomain	IP-adres	Services	Status
testbedrijf.nl	198.51.100.42	HTTP, HTTPS, SMTP	✓ Actief
mail.testbedrijf.nl	198.51.100.42	SMTP, IMAP, POP3	✓ Actief
www.testbedrijf.nl	198.51.100.42	HTTP, HTTPS	✓ Actief
old.testbedrijf.nl	198.51.100.87	HTTP (poort 8080)	■ Let op

Conclusie

Het aanvalsoppervlak van testbedrijf.nl is beperkt en overzichtelijk. Het subdomain old.testbedrijf.nl draait op een verouderde server (zie Hoofdstuk 2). Controleer of dit subdomain nog actief in gebruik is; indien niet, verwijder of deactiveer het.

HOOFDSTUK 5

Website Beveiliging & Standaarden

Inleiding

Dit hoofdstuk controleert de technische beveiligingsinstellingen van uw website op basis van de internet.nl standaarden. Beveiligingsheaders, cookie-instellingen, DNSSEC en RPKI-routeringsbeveiliging worden beoordeeld.

Scope

Website bereikbaarheid, HTTPS-configuratie, HTTP-beveiligingsheaders, cookiebeveiliging, DNSSEC en security.txt van testbedrijf.nl.

Resultaten

[HOOG] Website bereikbaar via onbeveiligd HTTP — geen automatische doorverwijzing

Kans: GEMIDDELD

Bezoekers die uw website bezoeken via een onbeveiligde verbinding lopen het risico dat hun gegevens worden onderschept. Wachtwoorden, formuliergegevens en persoonlijke informatie zijn zichtbaar voor derden op hetzelfde netwerk.

Wat kan er gebeuren?	Iemand op hetzelfde wifi-netwerk als uw bezoeker kan alle uitgewisselde informatie lezen en aanpassen — zonder dat uw bezoeker dit merkt.
Aanbeveling:	Stel een 301-redirect in van http:// naar https:// op uw webserver of hostingpanel.

[GEMIDDELD] Geen HSTS-header — browser kan verbinding downgraden naar HTTP

Kans: GEMIDDELD

Zonder HSTS kunnen aanvallers bezoekers tijdelijk omleiden naar een onbeveiligde versie van uw website om inloggegevens te onderscheppen.

Wat kan er gebeuren?	Aanvallers op hetzelfde netwerk kunnen de HTTPS-verbinding omzeilen.
Aanbeveling:	Voeg de Strict-Transport-Security header toe: max-age=31536000; includeSubDomains

[GEMIDDELD] Geen Content Security Policy — website kwetsbaar voor script-injectie

Kans: KLEIN

Als er een fout in uw website zit, kan een CSP-header kwaadaardige code automatisch blokkeren en schade voorkomen.

Wat kan er gebeuren?	Bij een succesvolle XSS-aanval kan kwaadaardige code worden uitgevoerd in de browser van uw bezoekers.
Aanbeveling:	Voeg een Content-Security-Policy header toe die bepaalt welke bronnen mogen laden.

[GEMIDDELD] Geen X-Frame-Options — website kan worden ingesloten (clickjacking)

Kans: KLEIN

Aanvallers kunnen uw website onzichtbaar inladen en bezoekers misleiden om knoppen te klikken die ze niet willen klikken.

Wat kan er gebeuren?	Bezoekers kunnen worden misleid om betalingen te bevestigen of gegevens in te vullen.
Aanbeveling:	Voeg de header toe: X-Frame-Options: SAMEORIGIN

[LAAG] Geen security.txt — beveiligingsonderzoekers weten niet hoe ze contact opnemen

Kans: KLEIN

Als een beveiligingsonderzoeker een lek in uw website vindt, weet hij niet hoe hij dit verantwoord aan u kan melden.

Wat kan er gebeuren?	Kwetsbaarheden worden mogelijk niet gemeld en blijven onopgemerkt.
Aanbeveling:	Maak een security.txt aan op /.well-known/security.txt met contactgegevens.

Conclusie

De website van testbedrijf.nl voldoet niet volledig aan moderne beveiligingsstandaarden. De ontbrekende HTTPS-redirect is de prioritaire maatregel. De beveiligingsheaders zijn eenvoudig toe te voegen via uw webserver. 5 maatregelen vereisen aandacht.

SAMENVATTING

Eindsamenvatting

47

GEMIDDELD

RISICOSCORE

Totaal bevindingen	10
Kritieke bevindingen	0
Hoge bevindingen	3
Gemiddelde bevindingen	4
Lage bevindingen	3

Deelconclusies per module

E-mailbeveiliging

DMARC ontbreekt volledig op testbedrijf.nl. E-mailadressen kunnen worden nagebootst. SPF staat op soft fail. 2 maatregelen vereisen aandacht.

74/100
HOOG RISICO

Infrastructuur

Verouderde Apache-versie met actief misbruikte CVE aangetroffen op old.testbedrijf.nl. Databasepoort publiek bereikbaar. Directe actie vereist.

52/100
HOOG RISICO

SSL / Certificaten

Primair certificaat geldig. mail.testbedrijf.nl certificaat verloopt binnen 14 dagen. 1 maatregel vereist aandacht.

30/100
GEMIDDELD RISICO

Aanvalsoppervlak

Beperkt aanvalsoppervlak. old.testbedrijf.nl subdomain aandacht aanbevolen. Geen kritieke bevindingen.

0/100
LAAG RISICO

Website Hygiene

HTTPS-redirect ontbreekt, meerdere beveiligingsheaders afwezig. 5 maatregelen vereisen aandacht.

96/100
HOOG RISICO

Prioriteitsoverzicht — direct aanpakken

De onderstaande bevindingen zijn kritiek of hoog van ernst en vereisen de meeste aandacht. Ze zijn gesorteerd op ernst en vervolgens op urgentie.

Ernst	Module	Bevinding	Kans

HOOG	E-mailbeveiliging	DMARC ontbreekt — e-mail spoofing mogelijk	GEMIDDELD
HOOG	Infrastructuur	Verouderde Apache 2.4.49 — CVE-2021-41773	GROOT
HOOG	Website Hygiene	HTTP zonder redirect naar HTTPS	GEMIDDELD

BIJLAGE

Actieplan

In dit actieplan staan concrete instructies voor elke bevinding uit het rapport. De acties zijn bedoeld voor de eigenaar of IT-beheerder van uw organisatie. U heeft geen uitgebreide technische kennis nodig om deze stappen uit te voeren. Bij twijfel geeft u dit document door aan uw hostingprovider of IT-partner.

DIRECT	Onmiddellijke actie vereist	1 MAAND	Actie binnen een maand	3 MAANDEN	Actie binnen drie maanden

DIRECT

DMARC-record instellen op primair domein

Module: E-mailbeveiliging ■ 1–2 uur ■ € Gratis

1 Log in op uw DNS-beheeromgeving (bijv. TransIP, Antagonist, SIDN).

2 Maak een nieuw TXT-record aan voor _dmarc.testbedrijf.nl.

3 Gebruik als startwaarde: v=DMARC1; p=none; rua=mailto:dmarc@testbedrijf.nl

4 Wacht 24-48 uur en controleer rapporten. Zet daarna p=quarantine.

5 Test via dmarcian.com of MXToolbox DMARC-checker.

DIRECT

Update Apache naar actuele versie (patch CVE-2021-41773)

Module: Infrastructuur ■ 1–2 uur ■ € Gratis

1 Voer een update uit via uw pakketbeheerder: sudo apt update && sudo apt upgrade apache2

2 Controleer de versie na update: apache2 -v (moet 2.4.62 of hoger zijn).

3 Test uw website na de update op correcte werking.

4 Overweeg poort 8080 te sluiten als het subdomain old.testbedrijf.nl niet meer in gebruik is.

DIRECT

HTTP-redirect naar HTTPS instellen

Module: Website Hygiene ■ 30 minuten ■ € Gratis

1 Log in op uw webhostingpaneel (bijv. DirectAdmin, Plesk, cPanel).

2 Zoek de instelling "HTTPS redirect" of "Forceer SSL" en schakel deze in.

3 Als u toegang heeft tot .htaccess: voeg toe: Redirect 301 / https://testbedrijf.nl/

4 Test via een browser: typ http://testbedrijf.nl en controleer de doorverwijzing.

1 MAAND

SSL-certificaat mail.testbedrijf.nl vernieuwen

Module: SSL / Certificaten ■ 30 minuten ■ € Gratis

1 Neem contact op met uw webhostingprovider over certificaatverlenging.

2 Vraag naar automatische verlenging via Let's Encrypt.

3 Test na verlenging via ssllabs.com/ssltest.

1 MAAND

SPF-record aanscherpen naar hard fail (-all)

Module: E-mailbeveiliging ■ 1 uur ■ € Gratis

1 Controleer eerst welke mailservers legitiem e-mail versturen namens uw domein.

2 Pas het SPF-record aan: v=spf1 include:_spf.provider.nl -all

3 Test met MXToolbox SPF-checker of alle legitieme mail nog aankomt.

4 Wacht 24 uur na wijziging voordat u problemen uitsluit.

1 MAAND

HSTS, CSP en X-Frame-Options headers toevoegen

Module: Website Hygiene ■ 1–2 uur ■ € Gratis

1 Voeg via .htaccess of hostingpanel de volgende headers toe:

2 Strict-Transport-Security: max-age=31536000; includeSubDomains

3 X-Frame-Options: SAMEORIGIN

4 Content-Security-Policy: default-src 'self'; script-src 'self'

5 Test het resultaat via securityheaders.com.

3 MAANDEN

Databasepoort 3306 afsluiten voor extern verkeer

Module: Infrastructuur ■ 1 uur ■ € Gratis

1 Voeg een firewallregel toe die poort 3306 blokkeert voor externe verbindingen.

2 Zorg dat database-toegang alleen intern of via VPN mogelijk is.

3 Test met een externe poortscanner (bijv. nmap of Shodan) dat de poort gesloten is.

3 MAANDEN

security.txt aanmaken

Module: Website Hygiene ■ 30 minuten ■ € Gratis

1 Maak een tekstbestand aan met de naam security.txt:

2 Contact: mailto:security@testbedrijf.nl

3 Expires: 2027-01-01T00:00:00.000Z

4 Canonical: https://testbedrijf.nl/.well-known/security.txt

5 Plaats dit bestand op uw webserver in de map .well-known/