

VOORBEELDRAPPORT. voorbeeld-bakkerij.nl bestaat niet: het is een verzonnen bakkerijsite die we zelf hebben nagebouwd als verouderde WordPress-site. Zo ziet een rapport eruit; de bevindingen zijn typisch voor een site die jaren niet is bijgewerkt.

VOORBEELD

voorbeeld-bakkerij.nl
19 oktober 2026, 14:30
Alleen publieke controles

Webcontroleur.

0

van 100

Samenvatting

1 blokker

5 hoog

4 middel

4 ok

0 overgeslagen

Begin hier

Als je maar tijd hebt voor drie dingen, doe dan deze:

1. **Back-ups en databasebestanden die iedereen kan downloaden** (blokker)
2. **Beveiligingsinstructies voor browsers (headers)** (hoog)
3. **Mailbeveiliging (SPF en DMARC)** (hoog)

Alle controles

P1 Beveiligde verbinding (https)

OK

PUBLIEK

Uitslag: **in orde**

In orde. Hier hoeft je niets aan te doen.

► Technisch bewijs

P2 Altijd https afdwingen (HSTS)

MIDDEL

PUBLIEK

Uitslag: **niet in orde**

Wat er mis is. Je site vertelt browsers niet dat ze altijd de beveiligde verbinding moeten gebruiken. Daardoor kan een eerste bezoek toch via een onbeveiligde verbinding lopen.

Wat je kunt doen. Laat de header Strict-Transport-Security toevoegen, met een looptijd van minstens een half jaar.

- Technische instructie voor je webbouwer (Engels)
- Technisch bewijs

P3 Beveiligingsinstructies voor browsers (headers) HOOG

PUBLIEK

Uitslag: **niet in orde**

Wat er mis is. Je site geeft browsers niet de standaard beveiligingsinstructies mee. Die maken het lastiger om je site te misbruiken, bijvoorbeeld door hem onzichtbaar in een andere site te laden of er een kwaadaardig script in te smokkelen.

Wat je kunt doen. Laat je webbouwer of hoster de ontbrekende headers toevoegen. De technische instructie staat hieronder.

- Technische instructie voor je webbouwer (Engels)
- Technisch bewijs

P4 Bestanden die niet openbaar horen (.env, .git) OK

PUBLIEK

Uitslag: **in orde**

In orde. Hier hoeft je niets aan te doen.

- Technisch bewijs

P5 Wachtwoorden of sleutels in openbare code OK

PUBLIEK

Uitslag: **in orde**

In orde. Hier hoeft je niets aan te doen.

- Technisch bewijs

P6 Mailbeveiliging (SPF en DMARC) HOOG

PUBLIEK

Uitslag: **niet in orde**

Wat er mis is. Je domein vertelt mailservers niet goed welke afzenders echt van jou zijn. Iemand anders kan dan makkelijker mail sturen die van jou lijkt te komen, en je eigen mail belandt sneller in de spam.

Wat je kunt doen. Zet een SPF-record en een DMARC-record in je DNS. Je hoster of mailprovider kan je de juiste waarden geven.

- Technische instructie voor je webbouwer (Engels)
- Technisch bewijs

P7 Gebruikte techniek OK

PUBLIEK

Uitslag: **in orde**

In orde. Hier hoeft je niets aan te doen.

► Technisch bewijs

L1 Verouderde serversoftware MIDDEL

PUBLIEK

Uitslag: **niet in orde**

De server laat in zijn headers een oude, end-of-life versie zien (PHP 5, Apache 2.2). Software die geen updates meer krijgt, heeft bekende, ongepatchte kwetsbaarheden. Werk de server/PHP-versie bij naar een ondersteunde versie en verberg de versie in de Server/X-Powered-By header.

► Technisch bewijs

L2 Verouderde WordPress, Joomla of Drupal HOOG

PUBLIEK

Uitslag: **niet in orde**

De site draait op een oude, publiek zichtbare versie van WordPress (4.7). Versies die zo ver achterlopen hebben publiek bekende kwetsbaarheden waarvoor kant-en-klare exploits bestaan. Werk WordPress en de plugins/thema's bij naar de actuele versie en haal de versievermelding (generator-tag, readme.html) weg.

► Technisch bewijs

L3 Back-ups en databasebestanden die iedereen kan downloaden BLOKKER

PUBLIEK

Uitslag: **niet in orde**

Deze back-up-/databasebestanden zijn publiek te downloaden: /backup.zip, /wp-config.php.bak. Daarin zit vaak je complete database (klantgegevens) en/of je configuratie met wachtwoorden. Verwijder ze onmiddellijk van de server en ga ervan uit dat de inhoud gelekt is: wijzig de betrokken wachtwoorden en sleutels.

► Technisch bewijs

L4 Mappen waar iedereen doorheen kan bladeren MIDDEL

PUBLIEK

Uitslag: **niet in orde**

Deze mappen tonen een openbare bestandslijst: /wp-content/uploads/. Bezoekers kunnen zo door je bestanden bladeren en dingen vinden die niet bedoeld zijn om te delen. Zet directory listing uit (Options -Indexes in Apache, autoindex off in nginx).

► Technisch bewijs

L5 Sporen van versiebeheer of editors (.svn, .git) HOOG

PUBLIEK

Uitslag: **niet in orde**

Versiebeheer- of editor-metadata is publiek bereikbaar: /.svn/entries. Daarmee kan iemand (delen van) je broncode of mappenstructuur reconstrueren, inclusief sleutels die ooit zijn vastgelegd. Blokkeer toegang tot .git, .svn, .hg en .DS_Store op de server.

► Technisch bewijs

L6 Beheerpagina vindbaar INFO

PUBLIEK

Uitslag: **niet in orde**

Je inlog-/beheerpagina is publiek bereikbaar: /wp-admin/, /wp-login.php. Dat is normaal, maar wel het doelwit voor geautomatiseerde inlogpogingen. Overweeg two-factor, een inloglimiet (rate limiting) en eventueel IP-beperking of een extra wachtwoord op de map.

► Technisch bewijs

L7 Pagina met al je serverinstellingen (phpinfo) HOOG

PUBLIEK

Uitslag: **niet in orde**

Er staat een publieke phpinfo()-pagina online (/phpinfo.php). Die toont je volledige serverconfiguratie: paden, modules, versies en soms omgevingsvariabelen met geheimen. Verwijder dit bestand van de server.

► Technisch bewijs

L8 WordPress geeft gebruikersnamen prijs MIDDEL

PUBLIEK

Uitslag: **niet in orde**

Op deze WordPress-site geldt: je WordPress-gebruikersnamen zijn publiek op te vragen (via de REST-API), waardoor aanvallers gericht wachtwoorden kunnen gaan raden; en xmlrpc.php staat open, wat misbruikt wordt voor massale inlogpogingen en als DDoS-versterker. Beperk de REST-API user-endpoint, zet xmlrpc.php uit als je het niet gebruikt, en gebruik two-factor plus een inloglimiet.

► Technisch bewijs

Dit is een automatische, technische momentopname. Het is geen garantie dat je site veilig is en geen juridisch advies. Er zijn alleen controles gedaan op wat iedereen publiek kan zien. Diepere controles doen we alleen na een eigendomscheck. Dit voorbeeld is gemaakt met onze echte scanner, tegen een site die we zelf hebben nagebouwd.