GUARDIAN 360°

QUICKSCAN BENCHMARK

Benchmarkrapport Webbeveiliging

Nederland · België · Duitsland · Frankrijk · overige landen

Editie augustus 2026

Gebaseerd op 12.914 gescande domeinen

Inhoudsopgave

1. Managementsamenvatting

Dit benchmarkrapport brengt het beveiligingsniveau van publieke websites in kaart op basis van de Guardian360 Quickscan. Voor deze editie zijn 12.914 domeinen succesvol gescand. De Quickscan beoordeelt onder meer de aanwezigheid van essentiële beveiligingsheaders, veelvoorkomende misconfiguraties, het Content Security Policy, de SPF-instelling in DNS en de kwaliteit van de SSL/TLS-configuratie. Elk domein krijgt een score van 0 tot 100.

De gemiddelde score over alle domeinen komt uit op 68,6 punten, op een schaal waarop maximaal 100 punten te behalen zijn. Dat wijst op een redelijk basisniveau, maar tegelijk op structurele achterstanden bij een aantal belangrijke beveiligingsmaatregelen. Vooral moderne, preventieve maatregelen zoals een Content Security Policy en strikte SSL/TLS-configuraties blijven massaal achter.

Tussen de vier kernmarkten van Guardian360 zijn duidelijke verschillen zichtbaar. **België** scoort met een gemiddelde van 72,7 het hoogst en kent op vrijwel alle thema's de minste kwetsbaarheden. **Nederland** en **Duitsland** liggen dicht bij het gemiddelde, met 68,9 respectievelijk 68,4. **Frankrijk** blijft met 64,3 achter en laat op de meeste headers de hoogste kwetsbaarheidspercentages zien.

De belangrijkste bevindingen op hoofdlijnen:

- Ontbrekende beveiligingsheaders zijn eerder regel dan uitzondering. Op circa 60% van alle domeinen ontbreekt een X-Frame-Options header en op ongeveer de helft ontbreekt een correcte HSTS-instelling.
- Een Content Security Policy ontbreekt op 73,2% van de domeinen. Dit is de meest voorkomende tekortkoming over alle landen heen.
- Driekwart van de domeinen (75,6%) heeft ten minste één kwetsbaarheid in de SSL/TLS-configuratie, zoals verouderde protocollen of zwakke cipers.
- Basismaatregelen zijn juist wél breed op orde. Ernstige misconfiguraties zoals een blootgestelde PHPinfo-pagina (1,6%) of een actieve HTTP TRACE-methode (0,9%) komen weinig voor.

De boodschap is helder. Het merendeel van de organisaties heeft de fundamenten op orde, maar laat eenvoudig te realiseren en hoogwaardige beveiligingswinst liggen op het gebied van headers, CSP en TLS-hardening. Juist daar biedt de Quickscan een concreet en meetbaar startpunt voor verbetering.

2. Over deze benchmark

2.1 Doel

Guardian360 voert met de Quickscan een geautomatiseerde, niet-intrusieve beveiligingsscan uit op de publiek benaderbare kant van een website. Deze benchmark aggregeert de resultaten van een groot aantal scans tot een marktbeeld. Het doel is om distributeurs, partners en klanten inzicht te geven in hoe het beveiligingsniveau van een individueel domein zich verhoudt tot de bredere markt en tot vergelijkbare organisaties in andere landen.

Wilt u weten hoe uw eigen domein scoort? U kunt kosteloos een Quickscan uitvoeren via guardian360.nl/quickscan.

2.2 Dataset

De benchmark is gebaseerd op 12.914 domeinen die in deze meetperiode succesvol zijn gescand. Alle domeinen tellen mee in de totale benchmark. Voor de landenvergelijking lichten wij de vier kernmarkten van Guardian360 uit. De indeling naar land gebeurt op basis van de landcode in het topleveldomein.

Segment	Aantal domeinen	Gem. score	Mediaan
Nederland (.nl)	4.278	68,9	65
België (.be)	609	72,7	75
Duitsland (.de)	2.887	68,4	65
Frankrijk (.fr)	215	64,3	65
Overige domein extensies	4.925	68,3	65
Alle landen (totaal)	**12.914**	**68,6**	**65**

Tabel 1. Omvang en gemiddelde score per segment.

De rij “Overige domein extensies” bevat de 4.925 domeinen met een andere of generieke extensie, zoals .com, .eu, .ch en .net. Deze domeinen tellen wel mee in de totale benchmark maar vormen geen apart uitgelicht land, omdat de extensie geen betrouwbare aanwijzing voor het land van herkomst geeft. Samen zorgen zij ervoor dat de totale benchmark een breed marktbeeld weergeeft.

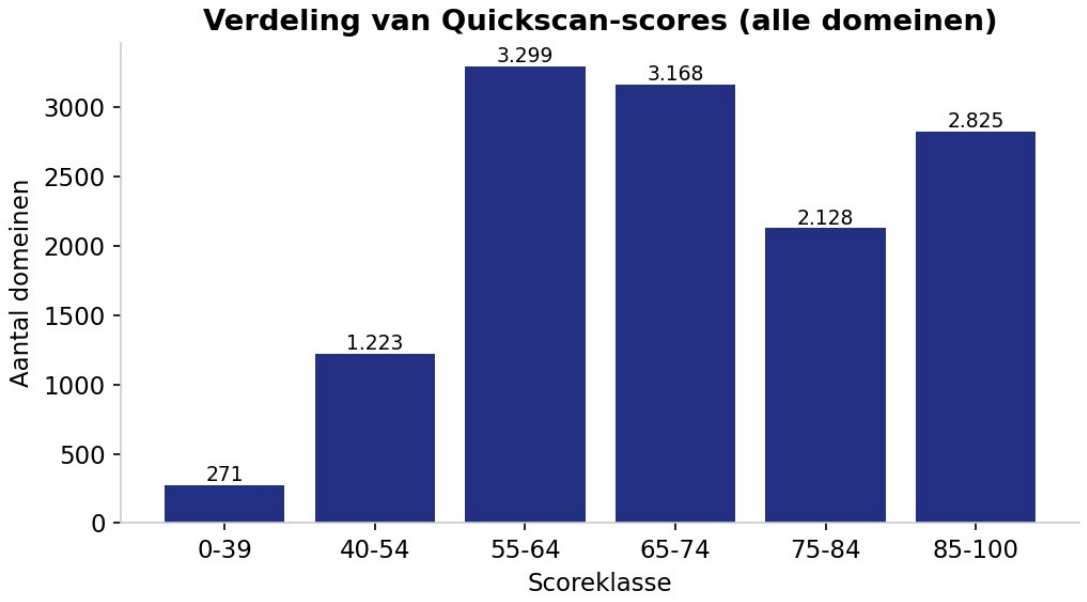
2.3 Wat de Quickscan meet

De Quickscan beoordeelt een aantal categorieën die samen een goed beeld geven van de beveiligingshygiëne van een website:

- Beveiligingsheaders: HTTP Strict Transport Security (HSTS), X-Content-Type-Options en X-Frame-Options.
- Content Security Policy (CSP): de aanwezigheid van een beleid dat het laden van ongewenste inhoud tegengaat.
- Misconfiguraties: onder meer het ontbreken van een HTTPS-redirect, het lekken van techniek via de X-Powered-By en Server headers, een blootgestelde PHPinfo-pagina en een actieve HTTP TRACE-methode.
- DNS: de aanwezigheid en juistheid van een SPF-record ter voorkoming van e-mailvervalsing.
- SSL/TLS: het gebruik van verouderde protocollen, zwakke cipers en bekende kwetsbaarheden in de versleutelde verbinding.

3. Algemeen beveiligingsniveau

De gemiddelde Quickscan-score over alle 12.914 domeinen bedraagt 68,6 punten, met een mediaan van 65. Dat betekent dat een typisch domein voldoet aan de belangrijkste basisvereisten, maar op meerdere onderdelen ruimte laat voor verbetering.

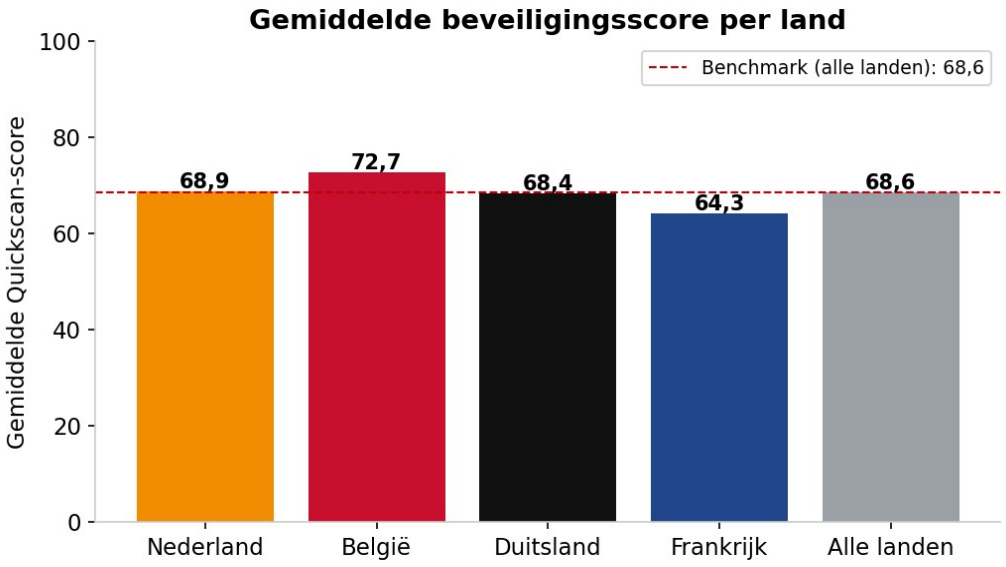


Figuur 1. Verdeling van de Quickscan-scores over alle domeinen.

De verdeling laat zien dat het zwaartepunt in de middenklasse ligt. De grootste groepen domeinen scoren tussen 55 en 74 punten. Aan de bovenkant haalt een substantiële groep van 2.825 domeinen een score van 85 of hoger, wat aantoont dat een hoog beveiligingsniveau goed haalbaar is. Aan de onderkant scoort een kleinere maar relevante groep van 271 domeinen onder de 40 punten. Deze domeinen kennen doorgaans een opeenstapeling van tekortkomingen en verdienen prioriteit.

4. Vergelijking tussen landen

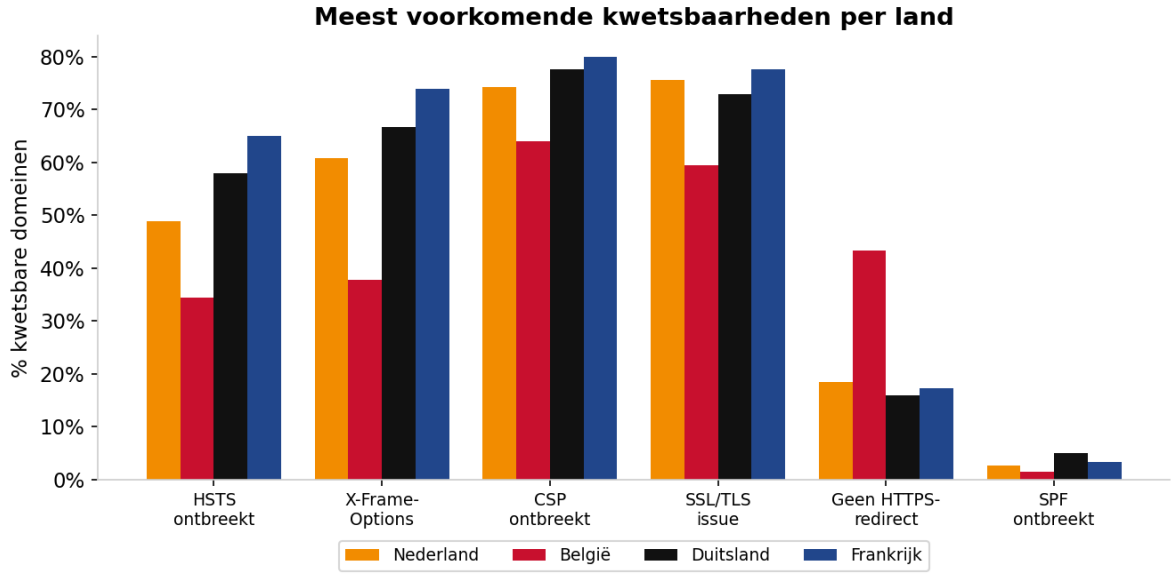
Hoewel de landen dicht bij elkaar liggen qua gemiddelde score, zijn er op onderdelen betekenisvolle verschillen. Onderstaande figuur toont de gemiddelde score per land, afgezet tegen de totale benchmark.



Figuur 2. Gemiddelde beveiligingsscore per land ten opzichte van de benchmark.

België springt er positief uit. Zowel de gemiddelde score van 72,7 als de mediaan van 75 liggen duidelijk boven de benchmark. Nederland en Duitsland volgen het gemiddelde vrijwel exact. Frankrijk blijft met 64,3 het verst achter, al is de steekproef voor Frankrijk met 215 domeinen kleiner en dus gevoeliger voor uitschieters.

De volgende figuur maakt de verschillen per thema concreet. Weergegeven is het percentage domeinen per land waarop de betreffende kwetsbaarheid is aangetroffen. Een lagere waarde is beter.



Figuur 3. Percentage kwetsbare domeinen per land voor de belangrijkste thema's.

Het beeld bevestigt de sterke positie van België op de beveiligingsheaders en op SSL/TLS. Opvallend is dat België juist zwakker scoort op de HTTPS-redirect, waar 43,3% van de Belgische domeinen bezoekers niet automatisch naar een versleutelde verbinding stuurt. Frankrijk kent de hoogste percentages ontbrekende

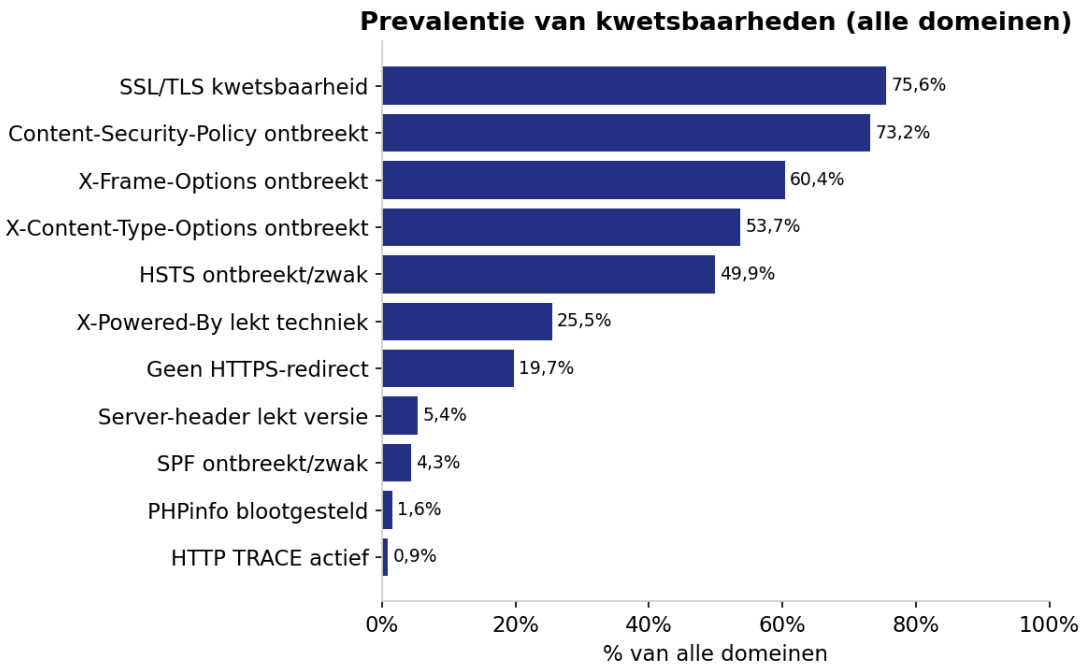
headers, terwijl Duitsland relatief vaak techniekinformatie lekt via de Server-header en het vaakst een ontbrekend of zwak SPF-record heeft.

5. Bevindingen per thema

Onderstaande tabel geeft de volledige uitsplitsing van de kwetsbaarheidspercentages per thema en per land. Alle percentages betreffen het aandeel domeinen waarop de tekortkoming is aangetroffen. Voor elk thema is een lagere waarde beter.

Thema	NL	BE	DE	FR	Totaal
HSTS ontbreekt of zwak	48,9%	34,5%	57,9%	65,1%	49,9%
X-Content-Type-Options ontbreekt	54,1%	33,5%	57,6%	67,9%	53,7%
X-Frame-Options ontbreekt	60,9%	37,8%	66,7%	74,0%	60,4%
Content-Security-Policy ontbreekt	74,3%	64,0%	77,7%	80,0%	73,2%
Geen HTTPS-redirect	18,4%	43,3%	16,0%	17,2%	19,7%
X-Powered-By lekt techniek	31,9%	9,7%	23,5%	35,3%	25,5%
Server-header lekt versie	3,2%	2,5%	9,4%	7,9%	5,4%
PHPinfo blootgesteld	1,3%	0,2%	2,6%	1,4%	1,6%
HTTP TRACE actief	0,9%	0,5%	1,2%	1,9%	0,9%
SPF ontbreekt of zwak	2,7%	1,5%	4,9%	3,3%	4,3%
SSL/TLS kwetsbaarheid	75,7%	59,4%	72,9%	77,7%	75,6%

Tabel 2. Percentage kwetsbare domeinen per thema en per land.



Figuur 4. Prevalentie van kwetsbaarheden over alle domeinen, oplopend gesorteerd.

5.1 Beveiligingsheaders

Beveiligingsheaders zijn een goedkope en effectieve manier om een groot deel van de veelvoorkomende aanvallen tegen te gaan. Toch blijven ze massaal achterwege. Op 60,4% van alle domeinen ontbreekt een X-Frame-Options header, waardoor de site kwetsbaar is voor clickjacking. Bij ongeveer de helft ontbreekt een

correcte HSTS-instelling en bij 53,7% de X-Content-Type-Options header. België doet het op alle drie de headers merkbaar beter dan de rest, terwijl Frankrijk consequent de hoogste percentages laat zien.

5.2 Content Security Policy

Het Content Security Policy is de meest voorkomende tekortkoming in deze benchmark. Op 73,2% van de domeinen ontbreekt een CSP volledig. Een goed ingericht CSP is een van de sterkste maatregelen tegen cross-site scripting en het ongewenst injecteren van inhoud. Dat de maatregel zo breed ontbreekt, komt doordat een CSP zorgvuldig moet worden afgestemd op de website en daarom vaak wordt uitgesteld. Ook hier presteert België het best met 64,0% en Frankrijk het zwakst met 80,0%.

5.3 Misconfiguraties

De ernstigste misconfiguraties komen gelukkig weinig voor. Een blootgestelde PHPinfo-pagina is op slechts 1,6% van de domeinen aangetroffen en een actieve HTTP TRACE-methode op 0,9%. Het lekken van techniekinformatie is hardnekkiger. Op 25,5% van de domeinen verraadt de X-Powered-By header welke technologie wordt gebruikt, wat aanvallers helpt bij het gericht zoeken naar kwetsbaarheden. De HTTPS-redirect verdient bijzondere aandacht in België, waar 43,3% van de domeinen deze basismaatregel mist.

5.4 SPF en e-mailbeveiliging

Het SPF-record voorkomt dat kwaadwillenden eenvoudig e-mail namens een domein kunnen versturen. Over alle domeinen ontbreekt een correct SPF-record bij 4,3%. Dat is relatief laag, wat aangeeft dat SPF inmiddels breed is ingeburgerd. Duitsland scoort hier met 4,9% iets minder dan de andere landen.

5.5 SSL/TLS-configuratie

De versleutelde verbinding is vrijwel overal aanwezig, maar de kwaliteit ervan laat te wensen over. Op 75,6% van alle domeinen is ten minste één SSL/TLS-kwetsbaarheid aangetroffen, zoals de ondersteuning van verouderde protocollen als TLS 1.0 of het aanbieden van zwakke cipers. Dit is samen met het ontbrekende CSP de meest voorkomende tekortkoming. België beperkt de schade tot 59,4%, terwijl Frankrijk met 77,7% het hoogste percentage kent.

6. Conclusies en aanbevelingen

De benchmark schetst een markt waarin de fundamenten grotendeels op orde zijn, maar waar hoogwaardige, preventieve beveiligingsmaatregelen structureel achterblijven. Vier conclusies staan centraal.

1. Het basisniveau is redelijk, maar niet meer dan dat. Met een gemiddelde score van 68,6 en een mediaan van 65 zit de markt in de middenmoot. De grote groep domeinen tussen 55 en 74 punten laat zien dat er met beperkte inspanning veel winst te behalen valt.

2. Headers, CSP en TLS zijn de grootste kansen. Deze drie thema's kennen de hoogste kwetsbaarheidspercentages en zijn tegelijk relatief eenvoudig te verbeteren. Ze vormen daarmee het logische startpunt van elk verbetertraject.

3. Er zijn duidelijke landverschillen. België loopt voorop, Frankrijk blijft achter en Nederland en Duitsland volgen de benchmark. Deze verschillen bieden aanknopingspunten voor gerichte marktbewerking per land.

4. De Quickscan maakt het meetbaar. Doordat elk domein een eenduidige score en een concrete lijst van bevindingen krijgt, is verbetering direct zichtbaar te maken. Dat maakt de Quickscan een sterk instrument voor zowel de eerste kennismaking als de periodieke voortgangsmeting.

6.1 Aanbevelingen voor MSPs, partners en distributeurs

- Positioneer de Quickscan als kosteloze nulmeting waarmee een (potentiële) klant direct ziet hoe zijn domein zich verhoudt tot deze benchmark.
- Gebruik de landverschillen uit dit rapport voor gerichte marktbewerking, bijvoorbeeld door in Frankrijk de nadruk te leggen op ontbrekende beveiligingsheaders.
- Bied de Quickscan aan als terugkerende dienst, zodat klanten hun voortgang periodiek kunnen meten en verbeteringen zichtbaar worden.

6.2 Aanbevelingen voor organisaties

- Bepaal met een Quickscan uw eigen uitgangspositie ten opzichte van deze benchmark.
- Richt de eerste verbeterslag op beveiligingsheaders en de HTTPS-redirect, omdat deze snel en zonder grote impact te realiseren zijn.
- Plan een tweede slag rond het Content Security Policy en de TLS-hardening, waar de grootste inhoudelijke winst ligt.
- Herhaal de scan periodiek zodat de voortgang zichtbaar blijft en het beveiligingsniveau op peil blijft.

Zelf een Quickscan uitvoeren?

Benieuwd hoe uw eigen domein scoort ten opzichte van deze benchmark? Voer kosteloos een Quickscan uit via

guardian360.nl/quickscan

Bijlage. Methodologische toelichting

De cijfers in dit rapport zijn afgeleid uit de ruwe resultaten van de Guardian360 Quickscan. Alleen scans met de status “completed” zijn meegenomen. Scans die zijn mislukt of niet volledig zijn afgerond, zijn buiten beschouwing gelaten. Voor deze editie ging het om 717 mislukte scans op een totaal van 13.631, wat neerkomt op 12.914 bruikbare resultaten.

De indeling naar land gebeurt op basis van de landcode in het topleveldomein. Een domein dat eindigt op .nl wordt toegerekend aan Nederland, .be aan België, .de aan Duitsland en .fr aan Frankrijk. Deze methode is eenvoudig en reproduceerbaar, maar kent een beperking. Een organisatie die actief is in een bepaald land maar een generiek domein zoals .com gebruikt, wordt niet aan dat land toegerekend. Deze domeinen tellen wel mee in de totale benchmark.

Een kwetsbaarheid wordt geteld wanneer de Quickscan het betreffende onderdeel als kwetsbaar markeert. Voor SSL/TLS geldt dat een domein als kwetsbaar wordt aangemerkt zodra ten minste één afzonderlijke bevinding, zoals een verouderd protocol of een zwakke cipher, is aangetroffen. De gerapporteerde percentages betreffen steeds het aandeel domeinen binnen het betreffende segment.