GUARDIAN 360°

QUICKSCAN BENCHMARK

Web Security Benchmark Report

Netherlands · Belgium · Germany · France · other countries

August 2026 edition

Based on 12,914 scanned domains

Table of contents

1. Executive summary

This benchmark report maps the security level of public websites based on the Guardian360 Quickscan. For this edition, 12,914 domains were successfully scanned. The Quickscan assesses, among other things, the presence of essential security headers, common misconfigurations, the Content Security Policy, the SPF setting in DNS and the quality of the SSL/TLS configuration. Each domain receives a score from 0 to 100.

The average score across all domains is 68.6 points, on a scale with a maximum of 100 points. This points to a reasonable baseline, but at the same time to structural shortcomings in a number of important security measures. Modern, preventive measures such as a Content Security Policy and strict SSL/TLS configurations lag behind on a massive scale.

There are clear differences between Guardian360's four core markets. **Belgium** scores highest with an average of 72.7 and shows the fewest vulnerabilities on almost every theme. **The Netherlands** and **Germany** sit close to the average, at 68.9 and 68.4 respectively. **France** lags behind at 64.3 and shows the highest vulnerability rates on most headers.

The main findings at a glance:

- Missing security headers are the rule rather than the exception. On around 60% of all domains an X-Frame-Options header is missing, and on about half a correct HSTS setting is missing.
- A Content Security Policy is missing on 73.2% of domains. This is the most common shortcoming across all countries.
- Three quarters of domains (75.6%) have at least one vulnerability in the SSL/TLS configuration, such as outdated protocols or weak ciphers.
- Basic measures, by contrast, are widely in order. Serious misconfigurations such as an exposed PHPinfo page (1.6%) or an active HTTP TRACE method (0.9%) are rare.

The message is clear. Most organisations have the fundamentals in place, but leave easy-to-achieve, high-value security gains on the table in the areas of headers, CSP and TLS hardening. That is precisely where the Quickscan offers a concrete and measurable starting point for improvement.

2. About this benchmark

2.1 Purpose

With the Quickscan, Guardian360 performs an automated, non-intrusive security scan of the publicly accessible side of a website. This benchmark aggregates the results of a large number of scans into a market picture. The aim is to give distributors, partners and clients insight into how the security level of an individual domain compares to the wider market and to comparable organisations in other countries.

Would you like to know how your own domain scores? You can run a free Quickscan at guardian360.net/quickscan.

2.2 Dataset

The benchmark is based on 12,914 domains that were successfully scanned during this measurement period. All domains are included in the overall benchmark. For the country comparison we highlight Guardian360's four core markets. Domains are assigned to a country based on the country code in the top-level domain.

Segment	Number of domains	Avg. score	Median
Netherlands (.nl)	4,278	68.9	65
Belgium (.be)	609	72.7	75
Germany (.de)	2,887	68.4	65
France (.fr)	215	64.3	65
Other domain extensions	4,925	68.3	65
All countries (total)	**12,914**	**68.6**	**65**

Table 1. Size and average score per segment.

The "Other domain extensions" row contains the 4,925 domains with a different or generic extension, such as .com, .eu, .ch and .net. These domains are included in the overall benchmark but do not form a separate highlighted country, because the extension is not a reliable indicator of the country of origin. Together they ensure that the overall benchmark reflects a broad market picture.

2.3 What the Quickscan measures

The Quickscan assesses a number of categories that together give a good picture of a website's security hygiene:

- Security headers: HTTP Strict Transport Security (HSTS), X-Content-Type-Options and X-Frame-Options.
- Content Security Policy (CSP): the presence of a policy that prevents loading unwanted content.
- Misconfigurations: among others, the absence of an HTTPS redirect, technology leakage via the X-Powered-By and Server headers, an exposed PHPinfo page and an active HTTP TRACE method.
- DNS: the presence and correctness of an SPF record to prevent email spoofing.
- SSL/TLS: the use of outdated protocols, weak ciphers and known vulnerabilities in the encrypted connection.

3. Overall security level

The average Quickscan score across all 12,914 domains is 68.6 points, with a median of 65. This means a typical domain meets the most important basic requirements but leaves room for improvement on several fronts.

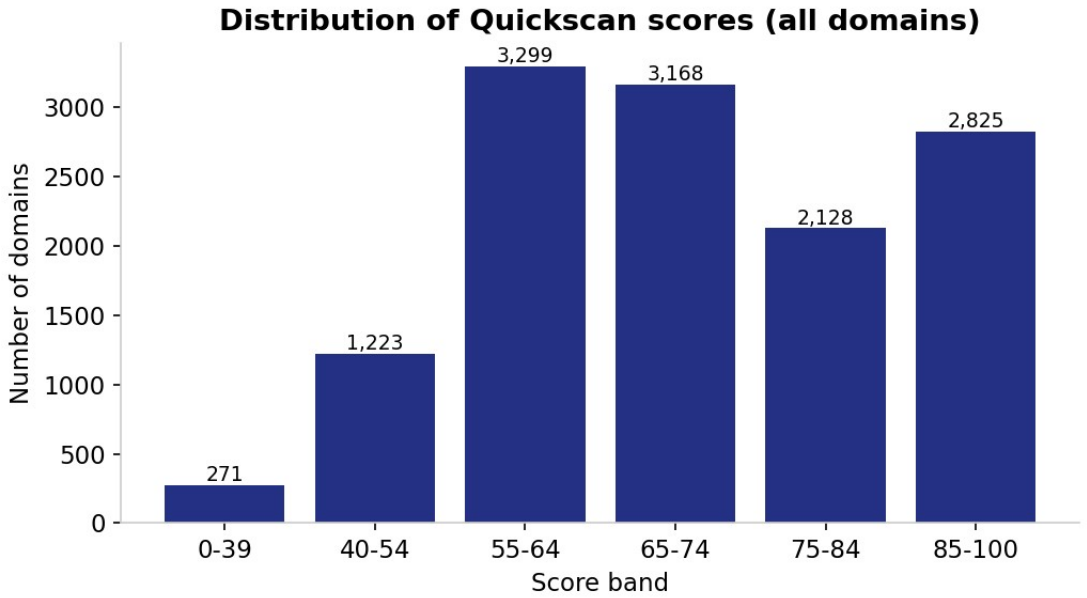

Figure 1. Distribution of Quickscan scores across all domains.

The distribution shows that the centre of gravity lies in the mid-range. The largest groups of domains score between 55 and 74 points. At the top end, a substantial group of 2,825 domains reaches a score of 85 or higher, showing that a high security level is well within reach. At the bottom end, a smaller but relevant group of 271 domains scores below 40 points. These domains usually show an accumulation of shortcomings and deserve priority.

4. Comparison between countries

Although the countries are close in terms of average score, there are meaningful differences on individual aspects. The figure below shows the average score per country, set against the overall benchmark.

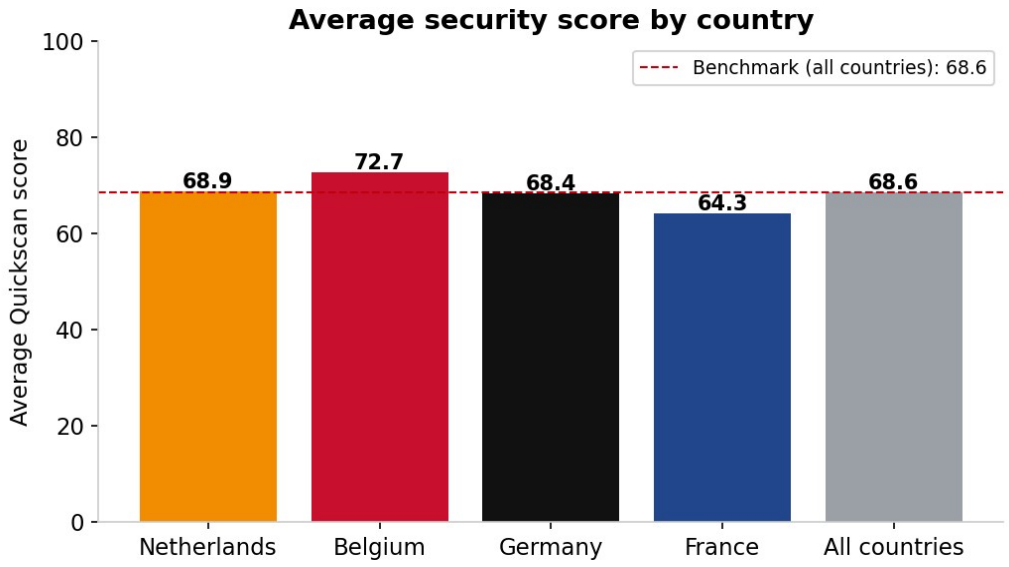

Figure 2. Average security score per country compared to the benchmark.

Belgium stands out positively. Both the average score of 72.7 and the median of 75 lie clearly above the benchmark. The Netherlands and Germany follow the average almost exactly. France lags furthest behind at 64.3, although the French sample, at 215 domains, is smaller and therefore more sensitive to outliers.

The next figure makes the differences per theme concrete. It shows the percentage of domains per country on which the relevant vulnerability was found. A lower value is better.

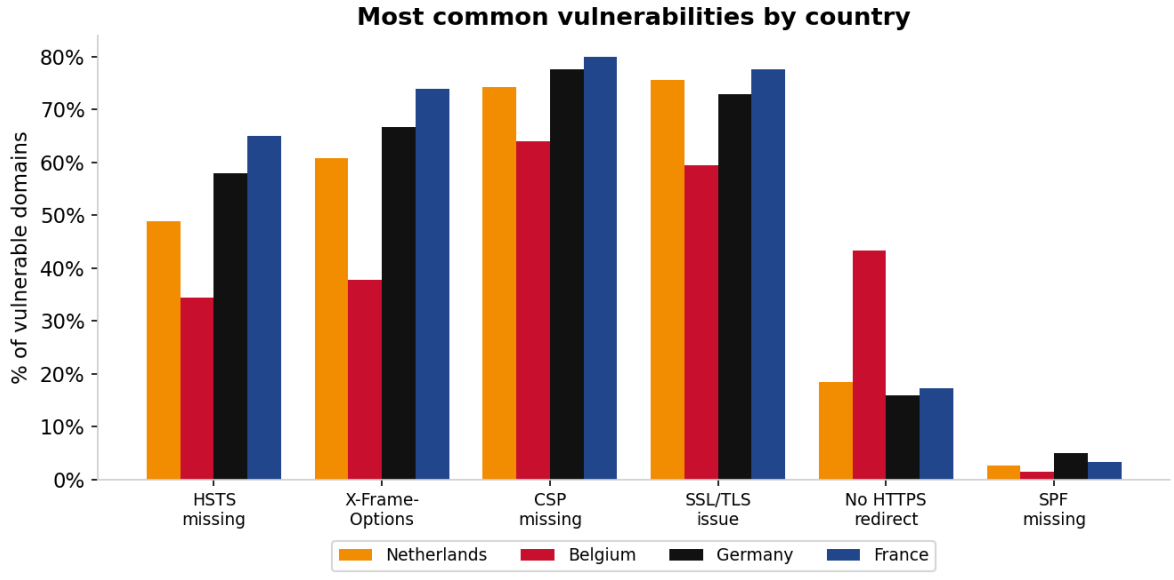

Figure 3. Percentage of vulnerable domains per country for the main themes.

The picture confirms Belgium's strong position on security headers and on SSL/TLS. Notably, Belgium performs worse on the HTTPS redirect, where 43.3% of Belgian domains do not automatically send visitors to an

encrypted connection. France has the highest percentages of missing headers, while Germany relatively often leaks technology information via the Server header and most often has a missing or weak SPF record.

5. Findings by theme

The table below gives the full breakdown of vulnerability percentages per theme and per country. All percentages represent the share of domains on which the shortcoming was found. For each theme, a lower value is better.

Theme	NL	BE	DE	FR	Total
HSTS missing or weak	48.9%	34.5%	57.9%	65.1%	49.9%
X-Content-Type-Options missing	54.1%	33.5%	57.6%	67.9%	53.7%
X-Frame-Options missing	60.9%	37.8%	66.7%	74.0%	60.4%
Content-Security-Policy missing	74.3%	64.0%	77.7%	80.0%	73.2%
No HTTPS redirect	18.4%	43.3%	16.0%	17.2%	19.7%
X-Powered-By leaks technology	31.9%	9.7%	23.5%	35.3%	25.5%
Server header leaks version	3.2%	2.5%	9.4%	7.9%	5.4%
PHPinfo exposed	1.3%	0.2%	2.6%	1.4%	1.6%
HTTP TRACE enabled	0.9%	0.5%	1.2%	1.9%	0.9%
SPF missing or weak	2.7%	1.5%	4.9%	3.3%	4.3%
SSL/TLS vulnerability	75.7%	59.4%	72.9%	77.7%	75.6%

Table 2. Percentage of vulnerable domains per theme and per country.

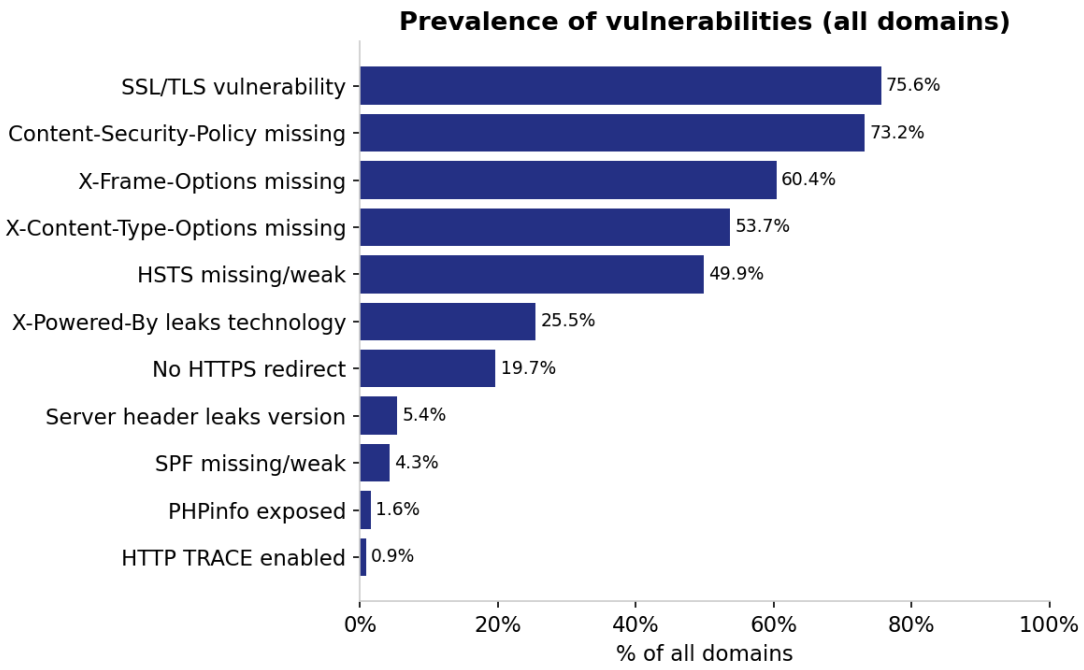

Figure 4. Prevalence of vulnerabilities across all domains, sorted ascending.

5.1 Security headers

Security headers are a cheap and effective way to counter a large share of common attacks. Yet they are widely absent. On 60.4% of all domains an X-Frame-Options header is missing, leaving the site vulnerable to

clickjacking. On about half a correct HSTS setting is missing, and on 53.7% the X-Content-Type-Options header. Belgium does noticeably better on all three headers, while France consistently shows the highest percentages.

5.2 Content Security Policy

The Content Security Policy is the most common shortcoming in this benchmark. On 73.2% of domains a CSP is entirely missing. A well-configured CSP is one of the strongest measures against cross-site scripting and unwanted content injection. The reason it is so widely absent is that a CSP must be carefully tailored to the website and is therefore often postponed. Here too, Belgium performs best at 64.0% and France worst at 80.0%.

5.3 Misconfigurations

The most serious misconfigurations are fortunately rare. An exposed PHPinfo page was found on just 1.6% of domains and an active HTTP TRACE method on 0.9%. Leaking technology information is more persistent. On 25.5% of domains the X-Powered-By header reveals which technology is used, helping attackers to search for vulnerabilities in a targeted way. The HTTPS redirect deserves particular attention in Belgium, where 43.3% of domains lack this basic measure.

5.4 SPF and email security

The SPF record prevents malicious parties from easily sending email on behalf of a domain. Across all domains, a correct SPF record is missing on 4.3%. That is relatively low, indicating that SPF is now widely adopted. Germany scores slightly worse here at 4.9%.

5.5 SSL/TLS configuration

The encrypted connection is present almost everywhere, but its quality leaves much to be desired. On 75.6% of all domains at least one SSL/TLS vulnerability was found, such as support for outdated protocols like TLS 1.0 or the offering of weak ciphers. Together with the missing CSP, this is the most common shortcoming. Belgium limits the damage to 59.4%, while France has the highest percentage at 77.7%.

6. Conclusions and recommendations

The benchmark paints a market in which the fundamentals are largely in place, but where high-value, preventive security measures structurally lag behind. Four conclusions stand out.

1. The baseline is reasonable, but no more than that. With an average score of 68.6 and a median of 65, the market sits in the middle. The large group of domains between 55 and 74 points shows that much can be gained with limited effort.

2. Headers, CSP and TLS are the biggest opportunities. These three themes have the highest vulnerability rates and are at the same time relatively easy to improve. They therefore form the logical starting point of any improvement programme.

3. There are clear country differences. Belgium leads, France lags and the Netherlands and Germany follow the benchmark. These differences offer angles for targeted, country-specific market development.

4. The Quickscan makes it measurable. Because each domain receives an unambiguous score and a concrete list of findings, improvement can be made visible immediately. That makes the Quickscan a strong instrument for both the first introduction and periodic progress measurement.

6.1 Recommendations for MSPs, partners and distributors

- Position the Quickscan as a free baseline measurement that lets a (prospective) client see immediately how their domain compares to this benchmark.
- Use the country differences from this report for targeted market development, for example by emphasising missing security headers in France.
- Offer the Quickscan as a recurring service, so that clients can measure their progress periodically and improvements become visible.

6.2 Recommendations for organisations

- Determine your own starting position relative to this benchmark with a Quickscan.
- Focus the first improvement round on security headers and the HTTPS redirect, as these can be implemented quickly and with little impact.
- Plan a second round around the Content Security Policy and TLS hardening, where the greatest substantive gains lie.
- Repeat the scan periodically so that progress remains visible and the security level is maintained.

Run your own Quickscan?

Curious how your own domain scores against this benchmark? Run a free Quickscan at **guardian360.net/quickscan**

Appendix. Methodological notes

The figures in this report are derived from the raw results of the Guardian360 Quickscan. Only scans with the status “completed” were included. Scans that failed or were not fully completed were excluded. For this edition this concerned 717 failed scans out of a total of 13,631, leaving 12,914 usable results.

Domains are assigned to a country based on the country code in the top-level domain. A domain ending in .nl is attributed to the Netherlands, .be to Belgium, .de to Germany and .fr to France. This method is simple and reproducible, but has a limitation. An organisation that is active in a particular country but uses a generic domain such as .com is not attributed to that country. These domains are included in the overall benchmark.

A vulnerability is counted when the Quickscan marks the relevant item as vulnerable. For SSL/TLS, a domain is flagged as vulnerable as soon as at least one individual finding, such as an outdated protocol or a weak cipher, is detected. The reported percentages always represent the share of domains within the relevant segment.