

RESEARCH REPORT

CSS Industry Security Report

The State of Web Security in the European Comparison Shopping Service Industry

143 CSS partners assessed | 13 countries | May 2026

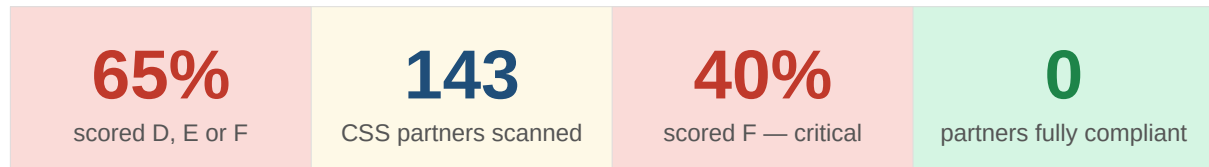
Published by ShoppingPartnerLab.com | Measured via Snyk Security Headers

CONTEXT

This report was initiated in the wake of a major data breach at Odido, one of the largest telecom providers in the Netherlands in 2026, in which the personal data of millions of customers was exposed. That incident raised a fundamental question: if a company of that scale fails to implement basic security measures, how does the CSS partner industry — a sector that manages daily access to Google Ads accounts and payment data for thousands of online retailers — fare?

Executive Summary

This report presents the findings of the first large-scale independent security assessment of the European CSS (Comparison Shopping Service) partner industry. In May 2026, **143 CSS partners across 13 countries** were evaluated on their implementation of critical HTTP security headers, measured via the Snyk Security Headers platform (securityheaders.com).



Key findings:

- 65% of all CSS partners score D, E or F — more than two thirds of the industry fails to meet minimum security requirements
- Only 4% achieve an A+ grade, and not a single CSS partner has all 9 security layers fully and correctly implemented
- The A-grade is misleading: partners scoring A still systematically lack critical headers such as COEP, COOP and CORP
- 40% score F — the lowest possible grade, where basic protection is entirely absent
- One partner is still running on unencrypted HTTP in 2026, exposing all traffic to interception
- Budget and company size do not correlate with security quality — well-funded scale-ups score as poorly as small players
- Germany and the Netherlands, home to the highest number of CSS partners, also show the most F-scores

Research Methodology

What are security headers?

Security headers are instructions sent by a web server alongside every page a visitor requests. They tell the browser how to safely render the page and protect users against a wide range of cyberattacks. Missing security headers are among the most common and most easily exploited vulnerabilities in modern web infrastructure.

The 9 measured headers and their function:

Header	Protects against
Strict-Transport-Security (HSTS)	Enforces HTTPS — prevents man-in-the-middle attacks and data interception
Content-Security-Policy (CSP)	Blocks XSS attacks — prevents injection of malicious scripts
X-Frame-Options	Prevents clickjacking — blocks the site from loading in an invisible frame
X-Content-Type-Options	Prevents MIME-sniffing — enforces correct file type interpretation
Referrer-Policy	Controls what data is shared when users navigate to external sites
Permissions-Policy	Blocks unwanted access to camera, microphone and location APIs
Cross-Origin-Embedder-Policy (COEP)	Prevents loading external resources without explicit permission
Cross-Origin-Opener-Policy (COOP)	Isolates browsing context — protects against cross-origin attacks
Cross-Origin-Resource-Policy (CORP)	Controls who is permitted to load external resources

Measurement tool and methodology

All measurements were conducted via Snyk Security Headers (securityheaders.com) — the world's most widely used independent security analysis platform, trusted by developers at Google, Microsoft and Amazon. Each URL was scanned in May 2026 with the 'Follow Redirects' option enabled to ensure accurate results.

Of the 143 CSS partners scanned, 138 could be assessed. Five partners (3%) could not be measured due to technical blocks or timeouts and have been excluded from statistical calculations.

Results

Overall distribution

The table below shows the complete grade distribution across all 143 scanned CSS partners.

Grade	Count	Percentage	Assessment
A+	6	4%	Excellent — all critical headers correctly implemented
A	14	10%	Good — nearly complete, minor gaps remain
B	15	10%	Adequate — several headers missing
C	13	9%	Moderate — multiple security risks present
D	32	22%	Poor — significant exposure to attacks
E	1	1%	Critical — no HTTPS encryption
F	57	40%	Dangerous — immediate action required
N/A	5	3%	Not measurable (blocked / timeout)

Alarming conclusion

Only 35 of the 138 measurable CSS partners (25%) achieve an adequate score (A+, A or B). The vast majority — 90 of 138 partners (65%) — score D, E or F, failing to meet the minimum security standards required to adequately protect the online retailers that depend on them.

Distribution by country

The table below shows the grade distribution by country of origin. Countries with a predominantly red background have more than 70% D/E/F scores.

Country	A+	A	B	C	D	E/F	Total
Germany (DE)	—	2	2	2	4	—	15
Netherlands (NL)	1	1	4	—	1	—	5
Czech Republic (CZ)	2	2	1	3	6	—	2
Poland (PL)	—	1	2	3	4	—	5
United Kingdom (UK)	—	2	—	1	3	—	4
EU (other)	—	4	2	1	6	—	13
France (FR)	—	1	—	—	2	—	4
Sweden (SE)	—	—	1	2	—	—	2
Denmark (DK)	—	—	—	—	2	1	2

USA (US)	2	—	—	—	—	—	2
Greece (GR)	1	—	1	—	1	—	0
Other	—	1	—	—	1	—	3

The A-Grade Paradox: Good Is Not Good Enough

One of the most surprising findings of this research is the gap between an official grade and actual security status. Several CSS partners score an A — apparently an excellent result — yet on closer analysis still lack critical security layers.

Core finding

Not a single one of the 143 CSS partners assessed has all 9 security headers fully and correctly implemented. Even the six A+ scorers systematically lack the Cross-Origin headers (COEP, COOP, CORP). The industry believes it is secure — but it is not.

Header presence by grade level

In the table below, ✓ means present and correctly configured, ~ means present but weakly configured, and ✗ means entirely absent.

Security Header	A+ avg.	A avg.	B avg.	C avg.	D avg.	F avg.
HSTS	✓	✓	✓	✓	✓	✓
X-Content-Type-Options	✓	✓	✓	✓	✓	✓
X-Frame-Options	✓	~	✓	✓	✓	✓
Referrer-Policy	~	~	✓	✓	✓	✓
Permissions-Policy	~	~	~	✓	✓	✓
Content-Security-Policy	~	~	~	~	✓	✓
COEP	✗	✗	✗	✗	✗	~
COOP	✗	✗	✗	✗	✗	✓
CORP	✗	✗	✗	✗	✗	✓

It is striking that the **Cross-Origin headers (COEP, COOP, CORP)** are absent across virtually the entire industry. These are increasingly important headers that protect against sophisticated cross-origin attacks — attacks that in the AI era are increasingly executed by automated exploit tooling.

The Threats: Concrete Attack Scenarios

Missing security headers are not merely technical oversights — they represent concrete, exploitable vulnerabilities. For CSS partners, who manage access to Google Merchant Center accounts and Google Ads budgets on behalf of their clients, the consequences are particularly severe.

1. XSS credential theft

Cross-Site Scripting (XSS) is the most common attack vector on the web. Without a correctly configured Content-Security-Policy, an attacker can inject malicious JavaScript onto a CSS partner's website. Every retailer who subsequently logs in to that partner's portal silently hands their Google Ads credentials directly to the attacker.

Impact: Full takeover of Google Ads accounts, fraudulent ad spend, loss of campaign and customer data.

2. Clickjacking via iframe injection

Without X-Frame-Options or a correctly configured CSP frame-ancestors directive, an attacker can load a CSS partner's login page invisibly inside their own fake website. Users click buttons they see on the fake site while actually interacting with the real CSS partner — allowing passwords and session tokens to be intercepted.

Impact: Account takeover, session hijacking, unauthorised changes to advertising campaigns.

3. Supply chain attack

CSS partners are a classic supply chain target: one successful attack on central infrastructure does not affect one retailer, but potentially hundreds or thousands of connected online stores simultaneously. Poor security at the CSS partner becomes poor security for all of their clients.

Impact: Mass data theft, compromised ad accounts across hundreds of retailers, reputational damage throughout the supply chain.

4. Man-in-the-middle attacks via missing HSTS

Partners that do not correctly enforce HTTPS via Strict-Transport-Security expose users to man-in-the-middle attacks, where network traffic is intercepted on public Wi-Fi networks or via compromised routers. In the CSS context, login credentials, session cookies and feed data can all be eavesdropped on.

Impact: Credential theft, session hijacking, unauthorised data access.

5. GDPR liability

The General Data Protection Regulation (GDPR) requires organisations to implement appropriate technical measures to protect personal data. Regulators treat missing security headers as a failure to meet this obligation. In the event of a data breach caused by missing headers, fines of up to 4% of global annual turnover are possible.

Impact: Financial penalties, mandatory breach notification, reputational damage, liability towards clients.

Security in the AI Era: SEO, Advertising and Google

The consequences of poor web security extend far beyond direct cyberattacks. In a digital ecosystem increasingly dominated by artificial intelligence, technical security has a direct impact on discoverability, advertising effectiveness and the relationship with Google as a platform.

Impact on Google rankings and SEO

Google has confirmed that HTTPS is a ranking factor. But the impact of technical security on SEO goes beyond HTTPS alone:

- Core Web Vitals and technical health: Google's ranking algorithm assesses the technical quality of websites. Missing security headers signal technical neglect, which can negatively affect the overall technical score.
- Trust signals: Google's algorithms work with trust signals. A site that fails to adequately protect visitors generates higher bounce rates when browsers display security warnings — a negative ranking signal.
- Indexation and crawl budget: Sites with security issues may be deprioritised in Google's crawl scheduling or experience slower indexation.

Google Ads penalties and account risks

CSS partners manage Google Ads campaigns and Google Merchant Center accounts on behalf of online retailers. Google's own policy and security requirements create direct risks:

Google's security requirements

Google requires that CSS partners advertising on behalf of retailers meet minimum security and reliability standards. A CSS partner whose infrastructure is compromised risks suspension from the Google Partner programme — directly affecting all connected retailer accounts.

- Account suspension: Google can suspend CSS partner accounts following confirmed security incidents or policy violations, causing all linked retailer accounts to be affected simultaneously.
- Loss of CSS status: CSS partners that lose their Google CSS partner status can no longer offer retailers discounts on Google Shopping costs.
- Fraud detection: Compromised accounts used for click fraud or unauthorised campaigns can result in permanent account exclusion.

Impact on AI discoverability and LLM search engines

The search landscape is shifting fundamentally. LLM-based search engines such as ChatGPT Search, Perplexity and Google's AI Overviews are becoming increasingly important as discovery channels for online retailers:

- Technical authority as a ranking factor: LLM-based search engines evaluate not only content but also the technical trustworthiness of sources. Sites with strong security implementations are regarded as more reliable.

- Crawlability for AI: AI search engines actively crawl the web for training data and real-time information. Sites with security issues or technical errors may be crawled less frequently.
- E-E-A-T signals: Google's Experience, Expertise, Authoritativeness and Trustworthiness framework — which also influences AI-generated answers — is negatively affected by security shortcomings.
- Reputation in AI-generated answers: A CSS partner involved in a data breach risks that information appearing in AI-generated responses about the company, causing permanent reputational damage.

Recommendations

For online retailers selecting a CSS partner

Online retailers entrust their Google Ads budgets and customer data to CSS partners. Security must be an explicit selection criterion, alongside price and service quality:

- Check the security score: Scan your CSS partner's website via securityheaders.com and use this as one of your selection criteria.
- Ask about GDPR compliance policy: What technical measures does the CSS partner take? What is their data breach policy?
- Assess technical professionalism: A CSS partner that fails to secure their own website is unlikely to adequately secure their clients' data either.
- Check your own webshop: Use the same tool to scan your own website at shoppingpartnerlab.com.

For CSS partners

Implementing all 9 security headers is a matter of hours for a professional web developer, not weeks. The key steps:

- Implement immediately: HSTS, X-Content-Type-Options and X-Frame-Options — the basic hygiene that no professional platform should be without.
- Configure CSP correctly: A Content-Security-Policy containing only 'unsafe-inline' or 'upgrade-insecure-requests' is insufficient. A strict whitelist is required.
- Add Cross-Origin headers: COEP, COOP and CORP are absent across virtually the entire industry, yet are relatively straightforward to implement.
- Set up automated monitoring: Configure alerts via securityheaders.com so that regressions are detected immediately.
- Conduct regular penetration tests: Security headers are one layer of a broader security programme.

Conclusion

The European CSS partner industry has a structural security problem. 65% of all partners fail to meet minimum security requirements, and not a single partner has all 9 critical headers fully and correctly implemented. In an era of increasing data breaches, growing AI search engine scrutiny of technical trustworthiness, and ever-stricter Google requirements for partners, this represents a serious risk — not only for the CSS partners themselves, but for all the online retailers they represent.

The good news: the solution is technically straightforward and can be implemented by any professional development team. The question is not whether it can be done — but whether the industry will make it a priority.

Research conducted by **ShoppingPartnerLab.com** — Europe's only independent CSS partner comparison platform. Measured via Snyk Security Headers (securityheaders.com).
May 2026.

For enquiries, the full dataset or a free security scan of your webshop:
shoppingpartnerlab.com