WebAuditPlus is a service provided by Belitum BV

Cybersecurity audit report for your website

Company name: Conson

Website: https://www.conson.com/en

WebAuditPlus ID: WAPL-3119-3481-5554-7910

WebAuditPlus version: 1.0.1

Created at: 2026-07-21

Table of Contents

Introduction

This report provides an independent analysis of your website, focusing on visible risks, improvement opportunities, and overall quality.

It is designed to be understandable for both technical and non-technical readers.

What this report helps you understand

- Whether your website shows visible cybersecurity or privacy risks

- Whether it may impact your visibility, trust, or business results

- What can be improved in terms of performance, SEO, and technical quality

- How your website may be perceived by users and AI systems

- Which actions and recommendations can help reduce or mitigate these risks

How to use this report

You do not need to read everything in detail.

We recommend starting with the Summary section, which highlights the most important findings and priorities.

Each section of the report includes:

- a clear description of the issue

- practical recommendations and suggested actions

You can focus on the most relevant areas depending on your needs.

Important note

This report does not require any technical access to your website.

It is based on publicly accessible information and visible indicators.

Need help understanding or acting on this report?

We can assist you with this report and its recommendations by contacting us via info@webauditplus.com.

Summary

This section provides a summary of key risks and priorities. It helps you to understand the current cybersecurity posture of the website and where remediation should start first.

Metric	Value
Overall risk level	High
Overall score (0-100)	65
Grade	D
Total penalty	180.46
Findings distribution	Critical 0 | High 1 | Medium 19 | Low 11 | Info 16

Score (0-100) reflects overall website risk and quality. Penalty is the total score reduction caused by findings. Grade is the score band (A best).

Top 10 Priorities

Note: The Top 10 priorities are based exclusively on verified findings (validated evidence), not on assumptions.

Severity	Module	Description
High	Tracking Indicators	Tracking technologies were detected but no consent/CMP signal was found on the homepage (heuristic). Ensure consent management and disclosures are implemented where required.
Medium	HTTP Security Headers	Content-Security-Policy is missing. (A CSP helps reduce XSS and data injection risks.)
Medium	Image Assets	4 images exceed 500 KB, which can slow down page load times.
Medium	Sitemaps & robots.txt	No reachable sitemap was found (robots.txt sitemap lines or /sitemap.xml).
Medium	AI Perception Analysis	Technical jargon may confuse non-technical customers
Medium	AI Perception Analysis	Unclear target customer segments
Medium	AI Perception Analysis	Incomplete product information
Medium	AI Perception Analysis	Potential confusion about product compatibility.
Medium	AI Perception Analysis	Unclear target audience for installers.
Medium	AI Perception Analysis	Ambiguity in product availability.

Top score impact (modules)

Module	Category	Penalty	Findings
AI Perception Analysis	AI	94.5	14
HTTP Security Headers	Security	25.02	6
Tracking Indicators	Privacy	17.32	2
Image Assets	Performance	11.88	4
Sitemaps & robots.txt	SEO	9.5	2
Link Health	SEO	9.0	2
Accessibility Basics	Accessibility	5.74	1
Forms	Privacy	2.75	2
Advanced SEO Analysis	SEO	2.5	2
JavaScript Indicators	Performance	2.25	3
GDPR & Privacy Compliance	Compliance	0.0	0

ISO 27001 Indicators	Compliance	0.0	1

AI Perception Analysis

This section analyses how the website may be perceived by modern AI systems and large language models based on publicly accessible information.

AI systems increasingly act as a first information source. If your content is vague or inconsistent, AI answers may misrepresent your business or miss key offerings.

Per-model results (what AI understands from your website)

Model	What they think you do	For who	Services mentioned	Clarity (0-100)
openai/gpt-4o-mini	Conson provides home and building automation products to enhance comfort and control.	Homeowners and building professionals such as installers and engineering offices.	Products for controlling and monitoring home systems like lighting, screens, and thermostats, along with software for configuration	85
google/gemini-3-flash-preview	Conson develops and manufactures hardware and software for home and building automation, specializing in decentralized intelligent modules for controlling lighting, heating, and shutters.	Homeowners, building managers, professional electrical installers, and engineering offices involved in new construction or renovation projects.	Manufacturing of automation modules (relays, dimmers, gateways), providing free configuration software (Contool), remote management systems (Consonbox/CONLINX), and technical documentation for legacy systems	88
x-AI/grok-4.3	Manufacturer of modular home and building automation hardware and software for lighting, relays, dimming, gateways and remote management	Homeowners and building owners via professional installers and engineering offices, with emphasis on renovation and circular construction projects	Hardware modules (XP series), free configuration software (Contool), internet management system (Consonbox with CONLINX), technical documentation and retro-compatibility support	88
anthropic/claude-sonnet-4	Manufactures and sells home and building automation products including dimmers, relay modules, power supplies, gateways, and management systems for controlling lights, screens, thermostats and other building systems	Homeowners, building owners, electrical installers, engineering offices, and dealers seeking automation solutions for residential and commercial buildings	Home and building automation products with remote control capabilities, free configuration software (Contool), internet-based management system (Consonbox with CONLINX software), technical documentation, and dealer network support	85

Cross-model consistency

Most common core activity	Manufactures and sells home and building automation products including dimmers, relay modules, power supplies, gateways, and management systems for controlling lights, screens, thermostats and other building systems
Most common audience	Homeowners, building owners, electrical installers, engineering offices, and dealers seeking automation solutions for residential and commercial buildings

Most common offerings	Home and building automation products with remote control capabilities, free configuration software (Contool), internet-based management system (Consonbox with CONLINX software), technical documentation, and dealer network support
Consistency level	low

AI misinterpretation risks & fixes (from model outputs)

Model	Risk	Suggested fix
anthropic/claude-sonnet-4	Technical jargon may confuse non-technical customers	Add plain language descriptions alongside technical specifications
anthropic/claude-sonnet-4	Unclear target customer segments	Create separate sections or pages for homeowners versus professional installers
anthropic/claude-sonnet-4	Incomplete product information	Ensure all product pages have complete technical details and clear pricing information
openai/gpt-4o-mini	Potential confusion about product compatibility.	Provide clearer guidelines or examples of compatible products.
openai/gpt-4o-mini	Unclear target audience for installers.	Add a dedicated section explaining the benefits for installers.
openai/gpt-4o-mini	Ambiguity in product availability.	Clearly list available products and their features.
openai/gpt-4o-mini	Technical jargon may alienate non-expert users.	Simplify language or provide definitions for technical terms.
google/gemini-3-flash-preview	End-users might try to install the hardware themselves.	Clearly state that hardware installation should be performed by a certified Conson installer.
google/gemini-3-flash-preview	Confusion between legacy CP modules and current XP modules.	Use a clearer 'Legacy vs. Current' comparison table to guide users toward the correct XP replacement.
google/gemini-3-flash-preview	Language mixing in localized versions.	Perform a full audit of translated pages to ensure 100% language consistency.

Findings

✓ Verified finding

Severity	Description	Recommendation
Medium ✓	Technical jargon may confuse non-technical customers	Add plain language descriptions alongside technical specifications
Medium ✓	Unclear target customer segments	Create separate sections or pages for homeowners versus professional installers
Medium ✓	Incomplete product information	Ensure all product pages have complete technical details and clear pricing information
Medium ✓	Potential confusion about product compatibility.	Provide clearer guidelines or examples of compatible products.
Medium ✓	Unclear target audience for installers.	Add a dedicated section explaining the benefits for installers.
Medium ✓	Ambiguity in product availability.	Clearly list available products and their features.
Medium ✓	Technical jargon may alienate non-expert users.	Simplify language or provide definitions for technical terms.
Medium ✓	Assumption of internet access for product functionality.	Clarify which features require internet access and which do not.
Medium ✓	Lack of information on customer support.	Include information on customer support and troubleshooting resources.

Medium ✓	End-users might try to install the hardware themselves.	Clearly state that hardware installation should be performed by a certified Conson installer.
Medium ✓	Confusion between legacy CP modules and current XP modules.	Use a clearer 'Legacy vs. Current' comparison table to guide users toward the correct XP replacement.
Medium ✓	Language mixing in localized versions.	Perform a full audit of translated pages to ensure 100% language consistency.
Medium ✓	End-users may assume direct consumer purchase and DIY installation	Add prominent 'For professionals' or ' Installer network' section on homepage
Medium ✓	Perception that full turnkey installation service is offered	Clarify on Products and About pages that Conson supplies components only

Crawl & Website Overview

This table shows how the scanned pages responded during the crawl. Pages with 200 codes loaded successfully, 300 codes redirected to another URL, 400 codes indicate client-side errors such as broken or inaccessible pages, and 500 codes indicate server-side errors that may require technical investigation.

Metric	Value
Pages crawled	8
2xx (Success)	8
3xx (Redirect)	0
4xx (Client Error)	0
5xx (Server Error)	0
Broken pages	0
Avg response time (ms)	1752

Technology & CMS

This section provides best-effort platform hints based on public signals and may contain false positives.

Detected / possible platform: WordPress (Confidence: Medium)

Signals observed:

Evidence is derived from public page markup (meta tags, scripts/links, and discovered paths).

- Path: /wp-content/

- Path: /wp-includes/

- Path: /wp-json/

- Path: https://www.conson.com/wp-json/

- File: https://www.conson.com/wp-content/plugins/cookie-law-info/public/css/cookie-law-info-public.css?ver=1.8.9

- File: https://www.conson.com/wp-content/plugins/sitepress-multilingual-CMS/res/js/jquery.cookie.js?ver=4.3.16

- File: https://www.conson.com/wp-includes/css/dist/block-library/style.min.css

- File: https://www.conson.com/wp-includes/js/jquery/jquery.js?ver=1.12.4-wp

AI-Generated Contextual Insights

The following insights are generated using AI based exclusively on verified technical findings from this module. They provide contextual interpretation and do not replace a formal security assessment or legal advice.

Model: anthropic/claude-sonnet-4

Area	Interpretation	Impact
Platform Detection	WordPress identified with medium confidence level	Platform-specific security considerations may apply

Model: x-ai/grok-4.3

Area	Interpretation	Impact
CMS Identification	Primary platform identified as WordPress with medium confidence.	No validated security exposures detected.

Model: google/gemini-3-flash-preview

Area	Interpretation	Impact
Platform Identification	WordPress has been identified as the primary content management system with medium confidence.	The ecosystem allows for extensive plugin integration but requires consistent maintenance.
Vulnerability Assessment	No validated exposures or security vulnerabilities were detected during the scan.	The current configuration does not present immediate known risks based on the available data.

Findings

✓ Verified finding

Severity	Description	Recommendation

Info	Detected via fingerprinting signals (confidence: medium).	Keep the platform and plugins up to date, minimize publicly exposed version information, and review hardening guides for this stack.

Server & Hosting Indicators

This section summarizes observable server/hosting signals from HTTP response headers, such as CDN/WAF hints, caching strategy, compression and HTTP/3 advertisement. It is based on heuristics and may not reflect the full infrastructure.

Metric	Value
Final URL	https://www.conson.com/
Server header	Apache
CDN/WAF candidates	None detected
Cache-Control	no-cache, no-store, must-revalidate
Content-Encoding	gzip
HTTP/3 advertised (Alt-Svc)	✗

Recommended actions

Enable compression (gzip/brotli) for text assets, define a caching strategy (Cache-Control) and consider a CDN/WAF where appropriate. Keep infrastructure transparent in documentation and align technical controls with security requirements.

Findings

✓ Verified finding

Severity	Description	Recommendation
Info	No clear CDN/WAF signal was detected from response headers (heuristic).	Review this finding and apply the appropriate remediation based on the issue described.

HTTP Security Headers

HTTP response headers can improve security and privacy by reducing common browser-based attack vectors (e.g., XSS, clickjacking). This section checks the homepage response for widely used security headers.

Metric	Value / status
Strict-Transport-Security	max-age=31536000; includeSubdomains;
Content-Security-Policy	Missing
X-Frame-Options	DENY
X-Content-Type-Options	nosniff
Referrer-Policy	no-referrer
Permissions-Policy	Missing
Cross-Origin-Opener-Policy	Missing
Cross-Origin-Embedder-Policy	Missing
Cross-Origin-Resource-Policy	Missing

Final URL	https://www.conson.com/
Server	Apache
X-Powered-By	N/A
Cache-Control	no-cache, no-store, must-revalidate

Recommended actions

Add missing security headers where appropriate. Start with HTTPS + HSTS, then implement a Content-Security-Policy, and verify clickjacking and MIME-sniffing protections. Always test changes in staging, as strict policies can impact functionality.

Findings

✓ Verified finding

Severity	Description	Recommendation
Medium ✓	Content-Security-Policy is missing. (A CSP helps reduce XSS and data injection risks.)	Create a Content-Security-Policy to reduce XSS and data injection risk. Start in report-only mode, review violations, then enforce after testing.
Low ✓	Permissions-Policy is missing. (Browser features may not be restricted to the minimum required set.)	Configure a Permissions-Policy header so sensitive browser features such as camera, microphone, geolocation and payment are limited to what the website really needs.
Low ✓	Cross-Origin-Opener-Policy is missing. (Cross-origin window interactions may not be restricted as strictly, increasing certain isolation risks.)	Consider setting Cross-Origin-Opener-Policy where appropriate to improve cross-origin isolation and reduce risks from untrusted browsing contexts.
Low ✓	Cross-Origin-Embedder-Policy is missing. (External resources may not be isolated as strictly, reducing protection against certain cross-origin data leaks.)	Consider setting Cross-Origin-Embedder-Policy where the site requires strong cross-origin isolation. Test carefully because it can block third-party resources.
Low ✓	Cross-Origin-Resource-Policy is missing. (External websites may be able to load certain resources more freely than intended.)	Consider setting Cross-Origin-Resource-Policy for sensitive resources to control which origins may load them.

Info	The Server header is present.	Minimize or remove detailed Server header information where possible to reduce technology fingerprinting.

TLS & Transport Security

HTTPS (TLS) encrypts traffic between visitors and the website. This section checks basic HTTPS reachability, HTTP->HTTPS redirection and certificate properties (expiry, issuer, protocol).

Metric	Value
Final URL	https://www.conson.com/
HTTPS status	200
HTTP -> HTTPS redirect	✓
TLS protocol	TLSv1.3
Cipher	TLS_AES_256_GCM_SHA384 (TLSv1.3)
Certificate valid from	2026-07-05T22:58:10Z
Certificate valid until	2026-10-03T22:58:09Z
Issuer	countryName=US, organizationName=Let's Encrypt, commonName=YR1

Recommendation

Ensure the site is always served over HTTPS with a valid certificate. Redirect HTTP to HTTPS, keep certificates renewed, and prefer TLS 1.2/1.3 only. For high-security sites, consider hardening cipher suites and enabling HSTS after testing.

Cookies & Session Security

This module reviews cookies observed during the crawl and highlights security attributes (Secure, HttpOnly, SameSite), lifetime, third-party usage, and potential tracking indicators.

Metric	Value
Cookies observed (unique)	0
First-party cookies	0
Third-party cookies (by Domain)	0
Session cookies	0
Persistent cookies	0
Long-lived (>= 365 days)	0
With Secure	0
With HttpOnly	0
With SameSite	0
Missing Secure	0
Missing HttpOnly	0
Missing SameSite	0
SameSite=None without Secure	0
Tracking cookie indicators	0
Max observed lifetime (days)	0
Cookie security score (0-100)	100

How to interpret these results

- Secure cookies are protected in transit when HTTPS is enforced.

- HttpOnly reduces exposure to client-side script access during XSS.

- SameSite can reduce CSRF risk; use Lax by default and None+Secure only when needed.

- Tracking cookies and third-party domains typically require careful consent and documentation.

AI-Generated Contextual Insights

The following insights are generated using AI based exclusively on verified technical findings from this module. They provide contextual interpretation and do not replace a formal security assessment or legal advice.

Model: anthropic/claude-sonnet-4

Observation	Interpretation	Business risk
No cookies detected during website analysis	The website operates without setting any cookies, indicating minimal client-side data storage	Low risk - no cookie-related security vulnerabilities present

Model: google/gemini-3-flash-preview

Observation	Interpretation	Business risk
No cookies were detected during the scan.	The website does not currently utilize first-party or third-party cookies for session management or tracking.	None identified. The absence of cookies eliminates risks related to cookie-based vulnerabilities or tracking non-compliance.

Findings

✓ Verified finding

Severity	Description	Recommendation
Info	No Set-Cookie headers were found in the crawled HTTP responses. This may be normal for static sites or sites that set cookies only after consent, login, or JavaScript execution.	If the site uses analytics, login sessions, or consent banners, verify cookie behavior in a real browser session (before and after consent) and ensure cookie flags are configured correctly.

Sitemaps & robots.txt

robots.txt gives crawl guidance to search engines and other crawlers. A sitemap helps search engines discover important pages. This section checks whether robots.txt and one or more sitemap URLs are reachable.

Metric	Value
Base URL	https://www.conson.com
robots.txt URL	https://www.conson.com/robots.txt
robots.txt status	200 (OK)
Sitemaps checked	1

robots.txt overview

- User-agents: *
- Sitemaps: None
- Disallow rules: 0

Sitemap fetch results

URL	Status
https://www.conson.com/sitemap.xml	500 (Internal Server Error)

Recommendation

Provide a robots.txt with clear crawl guidance, and publish a sitemap.xml that lists important canonical pages. Ensure sitemap URLs are reachable and updated when site structure changes.

Findings

✓ Verified finding

Severity	Description	Recommendation
Medium ✓	No reachable sitemap was found (robots.txt sitemap lines or /sitemap.xml).	Add sitemap references to robots.txt and ensure /sitemap.xml (or your sitemap URL) returns 200 and is kept up-to-date.
Low ✓	Some sitemap URLs were unreachable.	Review this finding and apply the appropriate remediation based on the issue described.

Link Health

This section analyzes the health of links found on 8 crawled pages of the website, based on the crawl limit configured for this report. It helps identify broken links, redirects and pages that do not return a valid HTTP response.

Internal links

Metric	Value
Total internal links	72
OK / reachable	64
Redirects	6
Errors / unreachable	1

Internal links with issues

URL	Status	Recommendation
https://www.conson.com/wp-json/oembed/1.0/embed	400 (Bad Request)	Update the internal URL or add a correct redirect to a working page.

External links

Metric	Value
Total external links	5
OK / reachable	3
Errors / unreachable	2

External links with issues

URL	Status	Recommendation
https://fonts.googleapis.com/css	400 (Bad Request)	Review the third-party URL and replace, remove or update the reference.
https://fonts.googleapis.com	404 (Not Found)	Review the third-party URL and replace, remove or update the reference.

Findings

✓ Verified finding

Severity	Description	Recommendation
Medium ✓	One or more internal links returned an error or could not be reached.	Fix broken internal links by correcting the target URL, restoring the target page or adding an appropriate redirect.
Low ✓	One or more external links returned an error or could not be reached.	Review affected third-party links and replace, remove or update references that no longer work.

Performance Indicators

This section provides lightweight performance indicators based on a single homepage request.

Metric	Value
Final URL	https://www.conson.com/
HTTP status	200 (OK)
Response time (ms)	1261
HTML size (bytes)	77988
Cache-Control	no-cache, no-store, must-revalidate

Findings

✓ Verified finding

Severity	Description	Recommendation
Info	Cache-Control suggests caching is disabled (no-store/no-cache).	Ensure this is intentional. If not, enable caching for non-sensitive content and static resources.

Accessibility Basics

WCAG quick checks based on crawled pages. WCAG check is an accessibility check of a website or web page against the Web Content Accessibility Guidelines.

Meta description missing on 0/8 pages.

Title missing on 0/8 pages.

HTML lang missing on 0/8 pages.

152/168 crawled images are missing alt text.

URL	Title	Meta	Lang	ALT missing
https://www.conson.com	✓	✓	✓	19/21
https://www.conson.com/pt-pt	✓	✓	✓	19/21
https://www.conson.com/nl	✓	✓	✓	19/21
https://www.conson.com/it	✓	✓	✓	19/21
https://www.conson.com/fr	✓	✓	✓	19/21
https://www.conson.com/es	✓	✓	✓	19/21
https://www.conson.com/de	✓	✓	✓	19/21
https://www.conson.com/da	✓	✓	✓	19/21

Findings

✓ Verified finding

Severity	Description	Recommendation
Medium ✓	Alt text missing for 152/168 crawled images.	Add meaningful alt text for informative images; use empty alt for decorative images. Keep it concise and descriptive.

Basic SEO Analysis

Search engines use page titles, meta descriptions, canonical URLs and headings to understand content. This section checks basic SEO signals on the homepage and provides quick improvements.

Metric	Value
Final URL	https://www.conson.com/
Title	Conson - Home and building automation products
Meta description	Increase your comfort with our home and building automation products. Control, monitor and manage your home by using your PC, smartphone or tablet.
Canonical	https://www.conson.com
Robots meta	index, follow, noarchive
H1 count	5
H2 count	6

H1 overview

- Increase your comfort with our home and building automation products
- Control and monitor your home from anywhere using your PC, phone or tablet
- Control your lights, screens or thermostat easily and much more.
- Only one push button in this building? How will the rest be served? See further...

H2 overview

- FEATURES
- Products
- Downloads
- DEALERS
- About
- CONTACT

Recommendation

Create unique titles per page, write a compelling meta description, set canonical URLs for key pages, and structure content with one clear H1. Add OpenGraph/Twitter tags to improve link previews on social media.

Findings

✓ Verified finding

Severity	Description	Recommendation
Info	Multiple H1 headings detected. Prefer a single main H1 for clarity and structure.	Review this finding and apply the appropriate remediation based on the issue described.
Info	OpenGraph og:title is missing.	Review this finding and apply the appropriate remediation based on the issue described.
Info	Open Graph image is missing on the homepage	Add an og:image meta tag with a representative image URL (absolute URL recommended). This improves link previews when your pages are shared on social platforms.

Advanced SEO Analysis

This section provides a consolidated overview of key site-wide SEO signals identified across the analyzed pages, focusing on structural, technical and content-related factors that may influence search visibility and organic performance.

Category	Metric	Value / pages
Coverage	Pages crawled	8
Coverage	Pages analyzed	8
Metadata	Long page titles	2
Metadata	Missing meta descriptions	0
Metadata	Long meta descriptions	5
Headings	Pages missing H1	0
Headings	Pages missing H2	0
Indexing & canonical URL	Pages with valid canonical URL	8
Indexing & canonical URL	Pages missing canonical URL	0
Indexing & canonical URL	Pages with invalid canonical URL	0
Indexing & canonical URL	Pages with canonical URL mismatch	0
Indexing & canonical URL	Pages marked noindex	0
Duplicates	Duplicate title groups	0
Duplicates	Duplicate meta description groups	0

Findings

✓ Verified finding

Severity	Description	Recommendation
Low ✓	Overly long <title> tags detected.	Shorten titles to ~50-60 characters to avoid truncation in search results while keeping the main keyword near the start.
Info	Overly long meta descriptions detected.	Trim meta descriptions to ~120-160 characters (focus on the first sentence) so search engines don't truncate the snippet.

Image Assets

We checked 280 images discovered during the crawl across 8 of 8 crawled pages. 37 image URLs were technically checked.

4 large image assets were detected while reviewing 280 image occurrences.

Images ≥ 500 KB

Source	Image URL	Alt	WxH	Loading	Size	Type
https://www.conson.com/	https://www.conson.com/wp-content/uploads/2020/07/BackgroundB.png		1183 x1136	Not set	1.8 MB	png
https://www.conson.com/	https://www.conson.com/wp-content/uploads/2020/08/BackgroundVillaGsm-2.png		1183 x1136	Not set	1.9 MB	png
https://www.conson.com/	https://www.conson.com/wp-content/uploads/2020/08/KitchenTabletGrijs.png		1183 x1136	Not set	1.1 MB	png
https://www.conson.com/	https://www.conson.com/wp-content/uploads/2020/08/BuildingWitXp.png		1183 x1135	Not set	1.2 MB	png

Findings

✓ Verified finding

Severity	Description	Recommendation
Medium ✓	4 images exceed 500 KB, which can slow down page load times.	Compress/resize images, use modern formats (WebP/AVIF), and enable caching/CDN where appropriate.
Low ✓	152 image occurrences are missing ALT text.	Add meaningful alt text for content images; use empty alt (alt="") for decorative images.
Low ✓	32 image occurrences are missing explicit width/height attributes.	Add width and height attributes (or CSS aspect-ratio) for images to reduce layout shift.
Info	168 image occurrences are missing a loading attribute.	Use loading="lazy" for below-the-fold images and keep critical images eager.

JavaScript Indicators

This section analyzes JavaScript resources detected on the website. It provides visibility into scripts, third-party dependencies and client-side technologies that may affect security, privacy, performance and maintainability.

Metric	Value
Pages crawled	8
Pages with scripts	8
Pages with inline scripts	8
Cap	100
Unique script URLs detected	21
Script URL occurrences	168
Metric Total Script Tag Occurrences	256
Average script occurrences per page	32.0
Maximum script occurrences on one page	32
Pages with inline scripts	8
Metric Inline Script Occurrences	88
Average inline script occurrences per page	11.0
Maximum inline script occurrences on one page	11

Scripts (all)

URL	Async/Defer	Pages
https://www.google-analytics.com/analytics.js	async	8
https://www.conson.com/wp-includes/js/jquery/jquery.js	-	8
https://www.conson.com/wp-includes/js/jquery/jquery-migrate.min.js	-	8
https://www.conson.com/wp-content/plugins/sitepress-multilingual-CMS/res/js/jquery.cookie.js	-	8
https://www.conson.com/wp-content/plugins/sitepress-multilingual-CMS/res/js/cookies/language-cookie.js	-	8
https://www.conson.com/wp-content/plugins/cookie-law-info/public/js/cookie-law-info-public.js	-	8
https://www.conson.com/wp-content/plugins/sitepress-multilingual-CMS/templates/language-switchers/legacy-dr...	-	8
https://www.conson.com/wp-content/plugins/sitepress-multilingual-CMS/dist/js/browser-redirect/app.js	-	8
https://www.conson.com/wp-content/themes/onepress/assets/js/plugins.js	-	8
https://www.conson.com/wp-content/themes/onepress/assets/js/bootstrap.min.js	-	8
https://www.conson.com/wp-content/themes/onepress/assets/js/owl.carousel.min.js	-	8
https://www.conson.com/wp-content/themes/onepress/assets/js/theme.js	-	8
https://www.conson.com/wp-content/plugins/onepress-plus/assets/js/slider.js	-	8
https://www.conson.com/wp-content/plugins/onepress-plus/assets/js/onepress-plus.js	-	8
https://www.conson.com/wp-includes/js/wp-embed.min.js	-	8
https://www.conson.com/wp-content/plugins/wpforms/assets/js/wpforms.js	-	8
https://www.conson.com/wp-content/plugins/wpforms-captcha/assets/js/wpforms-captcha.min.js	-	8

https://www.conson.com/wp-content/plugins/wpforms/assets/js/choices.min.js	-	8
https://www.conson.com/wp-content/plugins/wpforms/assets/js/jquery.validate.min.js	-	8
https://www.conson.com/wp-content/plugins/wpforms/assets/js/mailcheck.min.js	-	8
https://www.google.com/recaptcha/API.js	-	8

Script URL details (HEAD requests)

URL	Size (KB)	Type
https://www.google-analytics.com/analytics.js	20	text/javascript
https://www.conson.com/wp-includes/js/jquery/jquery.js	32	application/javascript
https://www.conson.com/wp-includes/js/jquery/jquery-migrate.min.js	3	application/javascript
https://www.conson.com/wp-content/plugins/sitepress-multilingual-CMS/res/js/jquery.cookie.js	1	application/javascript
https://www.conson.com/wp-content/plugins/sitepress-multilingual-CMS/res/js/cookies/language-cookie.js	0	application/javascript
https://www.conson.com/wp-content/plugins/cookie-law-info/public/js/cookie-law-info-public.js	7	application/javascript
https://www.conson.com/wp-content/plugins/sitepress-multilingual-CMS/templates/language-switchers/legacy-dr...	0	application/javascript
https://www.conson.com/wp-content/plugins/sitepress-multilingual-CMS/dist/js/browser-redirect/app.js	27	application/javascript
https://www.conson.com/wp-content/themes/onepress/assets/js/plugins.js	26	application/javascript
https://www.conson.com/wp-content/themes/onepress/assets/js/bootstrap.min.js	11	application/javascript
https://www.conson.com/wp-content/themes/onepress/assets/js/owl.carousel.min.js	11	application/javascript
https://www.conson.com/wp-content/themes/onepress/assets/js/theme.js	6	application/javascript
https://www.conson.com/wp-content/plugins/onepress-plus/assets/js/slider.js	0	application/javascript
https://www.conson.com/wp-content/plugins/onepress-plus/assets/js/onepress-plus.js	4	application/javascript
https://www.conson.com/wp-includes/js/wp-embed.min.js	0	application/javascript
https://www.conson.com/wp-content/plugins/wpforms/assets/js/wpforms.js	15	application/javascript
https://www.conson.com/wp-content/plugins/wpforms-captcha/assets/js/wpforms-captcha.min.js	0	application/javascript
https://www.conson.com/wp-content/plugins/wpforms/assets/js/choices.min.js	18	application/javascript
https://www.conson.com/wp-content/plugins/wpforms/assets/js/jquery.validate.min.js	7	application/javascript
https://www.conson.com/wp-content/plugins/wpforms/assets/js/mailcheck.min.js	1	application/javascript
https://www.google.com/recaptcha/API.js	1	text/javascript; charset=utf-8

Findings

✓ Verified finding

Severity	Description	Recommendation
Info	Many script tags detected	Reduce the number of scripts by removing unused libraries, bundling files, and loading only what is needed for the page.
Info	Many inline scripts detected	Move repeated inline scripts to reusable files and enable caching; keep inline scripts only for critical bootstrapping.
Low ✓	Some scripts are missing async/defer	Add async/defer to non-critical scripts to avoid blocking rendering. Keep blocking scripts only when required for above-the-fold content.

Forms

This section reviews forms detected on the website and highlights observable form-related indicators.

Form	Method	Inputs	Details
https://www.conson.com/da https://www.conson.com/de https://www.conson.com/es https://www.conson.com/fr https://www.conson.com/it https://www.conson.com/nl https://www.conson.com/pt-pt https://www.conson.com/	POST	18	- wpforms[fields][4] (text, required) - wpforms[fields][5] (text, required) - wpforms[fields][9] (email, required) - wpforms[fields][7] (text, not required) - wpforms[fields][8] (text, not required) - wpforms[fields][26][] (checkbox, required) - wpforms[fields][29][] (checkbox, not required) - wpforms[fields][31][a] (text, required) - wpforms[fields][31][cal] (hidden, not required) - wpforms[fields][31][n2] (hidden, not required) - wpforms[fields][31][n1] (hidden, not required) - wpforms[hp] (text, not required) - g-recaptcha-hidden (text, required) - wpforms[id] (hidden, not required) - wpforms[author] (hidden, not required) - wpforms[post_id] (hidden, not required) - wpforms[fields][2] (textarea, required) - wpforms[fields][3] (select, required) • ... (+3 more items)

Findings

✓ Verified finding

Severity	Description	Recommendation
Info	Forms that appear to collect personal data, such as an email address, were detected without a clear consent or privacy notice checkbox.	Add a clear privacy notice near the submit button and, where appropriate, a consent checkbox with a link to the privacy policy.
Low ✓	POST forms were detected without a CSRF-like token based on hidden input fields.	Implement server-side CSRF protection and include a per-session token field in POST form submissions.

Tracking Indicators

This section identifies tracking technologies and indicators detected on the website, such as analytics, advertising, tag management and consent mechanisms. It helps understand how visitor activity may be measured or shared with third parties.

Metric	Value
Final URL	https://www.conson.com/
Tracker technologies detected	1
CMP/consent signals detected	0
Cookie banner hint	✗
Third-party domains (scripts/iframes)	5

Detected tracker families

Name	Example URLs
Google Analytics	https://www.google-analytics.com/analytics.js

Third-party domains

Complete list (all observed third-party domains during the audit).

Domain
gmpg.org
www.google-analytics.com
fonts.googleapis.com
s.w.org
www.google.com

Findings

✓ Verified finding

Severity	Description	Recommendation
High ✓	Tracking technologies were detected but no consent/CMP signal was found on the homepage (heuristic).	If you use non-essential trackers (analytics/marketing), ensure consent is collected before loading them and document vendors/purposes in your cookie/privacy policy.
Info	Several third-party resources were detected. Third-party scripts do not automatically mean tracking, but they should be reviewed for privacy and consent impact.	Review this finding and apply the appropriate remediation based on the issue described.

GDPR & Privacy Compliance

This section evaluates whether the website meets essential GDPR transparency and consent requirements.

Metric	Value
GDPR compliance score (0-100)	100
Legal risk level (heuristic)	Low

Key policies & consent signals

Item	Status
Privacy policy	✓
Cookie policy	✓
Terms & conditions	✓
Cookie consent banner	✓

Detected policy pages or links

Item	Detected page or link
Privacy policy	https://www.conson.com/wp-content/uploads/2020/08/Privacy-declaration_EN.pdf
Cookie policy	https://www.conson.com/wp-content/uploads/2020/08/CookiePolicy_EN.pdf
Terms & conditions	https://www.conson.com/wp-content/uploads/2020/08/Terms_and_conditions_www.conson.com_EN.pdf

Cookie consent banner details

Item	Value
Cookie banner detection method	Technical/CMP indicator in HTML
Cookie banner indicator	cookie-law-info

Exposure Checks

This module identifies potential cybersecurity exposures. This section reviews publicly visible exposure indicators such as exposed paths, contact data, tokens, and developer references.

Exposed path findings

Path	URL	HTTP	Content type / note
-	-	-	No exposed path findings were detected.

Communication exposure indicators

No exposed email addresses or phone numbers were detected in the crawled pages.

Potential secrets or credentials

No exposed secrets, tokens, or credential-like patterns were detected in the crawled pages.

Internal network and credential-in-URL indicators

No internal IP addresses or credential-in-URL patterns were detected.

Developer and debug exposure indicators

No developer/debug exposure signals were detected (e.g., source maps, stack traces, debug flags, admin/dev references).

Cloud storage and service references

No cloud storage/service references were detected in the crawled pages.

OWASP Basics

This section maps observed website signals to the OWASP Top 10 risk areas. The checks are automated and heuristic, and they do not replace a full penetration test.

Metric	Value
Baseline security score (0-100)	100
Indicators found (themes with signals)	9

Overview of the OWASP top 10 themes

Theme	Description	Status
A01 - Broken Access Control	Restrictions and authorization flaws that allow users to access data or functions beyond intended permissions.	Public indicators found: Accessible admin/login paths: https://www.conson.com/login, https://www.conson.com/wp-login.php; Publicly accessible sensitive/restricted files: https://www.conson.com/readme.html, https://www.conson.com/CHANGELOG.txt
A02 - Cryptographic Failures	Weaknesses in encryption or transport security that can expose sensitive data.	Public indicators found: HTTPS observed for audited site
A03 - Injection	Untrusted input reaching interpreters (SQL/NoSQL/OS/LDAP), including XSS in some contexts.	Public indicators found: HTML forms on public pages: 1; Inline script tags detected: 11
A04 - Insecure Design	Missing or ineffective security controls by design (requires architecture review).	Public indicators found: POST forms without visible CSRF-like token: 1
A05 - Security Misconfiguration	Insecure default settings, missing headers, exposed files, or misconfigured services.	Public indicators found: Missing security headers: Content-Security-Policy, Permissions-Policy; Technology disclosure headers present: Server; Exposed configuration/sensitive files: https://www.conson.com/readme.html, https://www.conson.com/CHANGELOG.txt; Debug information publicly visible on: https://www.conson.com
A06 - Vulnerable and Outdated Components	Using libraries, frameworks, or platforms with known vulnerabilities or exposed version info.	Public indicators found: Version/package metadata exposed: https://www.conson.com/readme.html, https://www.conson.com/CHANGELOG.txt; Scripts without integrity attribute: 2; Generator metadata detected on: https://www.conson.com
A07 - Identification and Authentication Failures	Weaknesses in login, session management, or credential handling.	Public indicators found: Login/authentication paths exposed: https://www.conson.com/login, https://www.conson.com/wp-login.php; POST forms without visible CSRF-like token: 1
A08 - Software and Data Integrity Failures	Missing integrity checks (e.g., SRI) or insecure update/CI pipelines.	Public indicators found: Version/package metadata exposed: https://www.conson.com/readme.html, https://www.conson.com/CHANGELOG.txt; Third-party domains referenced: www.google-analytics.com, www.google.com

A09 - Security Logging and Monitoring Failures	Insufficient logging/monitoring for detecting and responding to attacks.	Public indicators found: Stack trace information visible on: https://www.conson.com; Debug/runtime information visible on: https://www.conson.com; Technology disclosure headers present: Server
A10 - Server-Side Request Forgery (SSRF)	Server fetches attacker-controlled URLs (often via URL inputs); typically needs deeper testing.	No public indicator found

Disclaimer

These findings are based on automated checks and heuristics. For higher assurance, perform manual review and/or a penetration test, especially for authentication, authorization, and application logic vulnerabilities.

Findings

✓ Verified finding

Severity	Description	Recommendation
Info	OWASP indicators are based on public signals only; this is not a penetration test.	Review this finding and apply the appropriate remediation based on the issue described.

ISO 27001 Indicators

This analysis reflects cybersecurity controls aligned with ISO 27001. This section discusses ISO 27001 indicators based on publicly observable information. For each theme, the report states whether a public indication was found, no public indication was found, or the theme was not scanned for indication.

Metric	Value
Framework	ISO 27001 indicators
Indicators	7
Themes with public indicators	6

Indicator overview by theme

Control theme	Objective	Status
A.9 Access control	Access-related entry points show signs of controlled authentication and request protection	Public indicators found. Evidence: Accessible admin/login paths detected: https://www.conson.com/login, https://www.conson.com/wp-login.php; Publicly accessible sensitive paths detected: https://www.conson.com/readme.html, https://www.conson.com/CHANGELOG.txt; POST forms without visible CSRF-like token: 1
A.10 Cryptography	Transport encryption and cookie protection are configured securely	Public indicators found. Evidence: HTTPS observed for audited site
A.12 Operations security	Operational configuration reduces information leakage and insecure defaults	Public indicators found. Evidence: Exposed sensitive files/paths: https://www.conson.com/readme.html, https://www.conson.com/CHANGELOG.txt; Debug information publicly visible on: https://www.conson.com; Stack trace indicators visible on: https://www.conson.com
A.13 Communications security	External communications and third-party data exchanges are controlled and transparent	Public indicators found. Evidence: HTTPS used for website communications; Missing security headers: Content-Security-Policy, Permissions-Policy; Third-party communication domains observed: www.google-analytics.com, www.google.com
A.14 System acquisition, development and main...	Technology choices and development signals support secure maintenance practices	Public indicators found. Evidence: Version/package metadata exposed: https://www.conson.com/readme.html, https://www.conson.com/CHANGELOG.txt; External JavaScript files detected: 21; Generator metadata detected on: https://www.conson.com
A.16 Information security incident management	Public incident and security contact channels are visible and usable	No public indicator found
A.18 Compliance	Public transparency and privacy/compliance signals support legal and regulatory obligations	Public indicators found. Evidence: Privacy policy page detected: https://www.conson.com/wp-content/uploads/2020/08/Privacy-declaration_EN.pdf; Cookie policy page detected: https://www.conson.com/wp-content/uploads/2020/08/CookiePolicy_EN.pdf; Terms and conditions page detected: https://www.conson.com/wp-content/uploads/2020/08/Terms_and_conditions_www.conson.com_EN.pdf; Cookie consent mechanism detected; Tracking scripts detected on pages: 1

Notes

- ISO/IEC 27001 certification cannot be confirmed by automated website scanning alone.
- These indicators map technical signals to high-level ISO 27001/Annex A themes to support discussion and prioritization.

Disclaimer

These are indicative signals only. ISO/IEC 27001 certification requires a full ISMS scope assessment, evidence review and audits. Use this section as a readiness / best-practice lens, not as a compliance statement.

Findings

✓ Verified finding

Severity	Description	Recommendation
Info	ISO 27001 indicators are based on publicly observable website information and are not a certification assessment.	Review this finding and apply the appropriate remediation based on the issue described.

Risk & Action Plan

This section identifies cybersecurity risks and translates the most important findings into a prioritized action plan.

Top 10 Priorities

Severity	Module	Description
High	Tracking Indicators	Tracking technologies were detected but no consent/CMP signal was found on the homepage (heuristic). Ensure consent management and disclosures are implemented where required.
Medium	HTTP Security Headers	Content-Security-Policy is missing. (A CSP helps reduce XSS and data injection risks.)
Medium	Image Assets	4 images exceed 500 KB, which can slow down page load times.
Medium	Sitemaps & robots.txt	No reachable sitemap was found (robots.txt sitemap lines or /sitemap.xml).
Medium	AI Perception Analysis	Technical jargon may confuse non-technical customers
Medium	AI Perception Analysis	Unclear target customer segments
Medium	AI Perception Analysis	Incomplete product information
Medium	AI Perception Analysis	Potential confusion about product compatibility.
Medium	AI Perception Analysis	Unclear target audience for installers.
Medium	AI Perception Analysis	Ambiguity in product availability.

Suggested timeline overview

Suggested timeline	Severity	Item description	Module
0-30 days	High	Tracking technologies were detected but no consent/CMP signal was found on the homepage (heuristic). Ensure consent management and disclosures are implemented where required.	Tracking Indicators
0-30 days	Medium	Content-Security-Policy is missing. (A CSP helps reduce XSS and data injection risks.)	HTTP Security Headers
0-30 days	Medium	No reachable sitemap was found (robots.txt sitemap lines or /sitemap.xml).	Sitemaps & robots.txt
30-60 days	Medium	Technical jargon may confuse non-technical customers	AI Perception Analysis
30-60 days	Medium	Unclear target customer segments	AI Perception Analysis
30-60 days	Medium	Incomplete product information	AI Perception Analysis
30-60 days	Medium	Potential confusion about product compatibility	AI Perception Analysis
30-60 days	Medium	Unclear target audience for installers	AI Perception Analysis
30-60 days	Medium	Ambiguity in product availability	AI Perception Analysis
30-60 days	Medium	Technical jargon may alienate non-expert users	AI Perception Analysis
30-60 days	Medium	Assumption of internet access for product functionality	AI Perception Analysis
30-60 days	Medium	Lack of information on customer support	AI Perception Analysis

30-60 days	Medium	End-users might try to install the hardware themselves	AI Perception Analysis
30-60 days	Medium	Confusion between legacy cp modules and current xp modules	AI Perception Analysis
30-60 days	Medium	Language mixing in localized versions	AI Perception Analysis
30-60 days	Medium	End-users may assume direct consumer purchase and DIY installation	AI Perception Analysis
30-60 days	Medium	Perception that full turnkey installation service is offered	AI Perception Analysis
30-60 days	Medium	4 images exceed 500 KB, which can slow down page load times.	Image Assets
30-60 days	Medium	One or more internal links returned an error or could not be reached.	Link Health
30-60 days	Medium	Alt text missing for 152/168 crawled images.	Accessibility Basics
30-60 days	Low	Permissions-Policy is missing. (Browser features may not be restricted to the minimum required set.)	HTTP Security Headers
30-60 days	Low	Cross-Origin-Opener-Policy is missing. (Cross-origin window interactions may not be restricted as strictly, increasing certain isolation risks.)	HTTP Security Headers
30-60 days	Low	Cross-Origin-Embedder-Policy is missing. (External resources may not be isolated as strictly, reducing protection against certain cross-origin data leaks.)	HTTP Security Headers
30-60 days	Low	Cross-Origin-Resource-Policy is missing. (External websites may be able to load certain resources more freely than intended.)	HTTP Security Headers
30-60 days	Low	POST forms were detected without a CSRF-like token based on hidden input fields.	Forms
30-60 days	Low	Overly long <title> tags detected.	Advanced SEO Analysis
60+ days	Low	152 image occurrences are missing ALT text.	Image Assets
60+ days	Low	32 image occurrences are missing explicit width/height attributes.	Image Assets
60+ days	Low	Some sitemap URLs were unreachable. Fix or remove broken sitemap references.	Sitemaps & robots.txt
60+ days	Low	One or more external links returned an error or could not be reached.	Link Health
60+ days	Low	Some scripts are missing async/defer	JavaScript Indicators
60+ days	Info	The Server header is present. Consider minimizing server or version exposure where possible.	HTTP Security Headers
60+ days	Info	Several third-party resources were detected. Third-party scripts do not automatically mean tracking, but they should be reviewed for privacy and consent impact.	Tracking Indicators
60+ days	Info	168 image occurrences are missing a loading attribute.	Image Assets
60+ days	Info	Forms that appear to collect personal data, such as an email address, were detected without a clear consent or privacy notice checkbox.	Forms
60+ days	Info	Overly long meta descriptions detected.	Advanced SEO Analysis
60+ days	Info	Many script tags detected	JavaScript Indicators
60+ days	Info	Many inline scripts detected	JavaScript Indicators

60+ days	Info	No Set-Cookie headers were found in the crawled HTTP responses. This may be normal for static sites or sites that set cookies only after consent, login, or JavaScript execution.	Cookies & Session Security
60+ days	Info	OWASP indicators are based on public signals only; this is not a penetration test.	OWASP Basics
60+ days	Info	Cache-Control suggests caching is disabled (no-store/no-cache).	Performance Indicators
60+ days	Info	Multiple H1 headings detected. Prefer a single main H1 for clarity and structure.	Basic SEO Analysis
60+ days	Info	OpenGraph og:title is missing. Add it to improve link previews on social platforms.	Basic SEO Analysis
60+ days	Info	Open Graph image is missing on the homepage	Basic SEO Analysis
60+ days	Info	No clear CDN/WAF signal was detected from response headers (heuristic). Consider a CDN/WAF for performance and security where appropriate.	Server & Hosting Indicators
60+ days	Info	Detected via fingerprinting signals (confidence: medium).	Technology & CMS

Next actions / service pack

Service	Recommendation
AI Visibility Pack	Improve AI discoverability: structured data, entity signals, topical authority, and citation readiness.
Security Headers Pack	Implement CSP, HSTS, X-Content-Type-Options, Referrer-Policy and harden headers configuration.

Disclaimer

This report is created based on publicly accessible information. It does not constitute legal advice and is intended as a cybersecurity assessment and does not replace a full penetration test.

Verify critical findings and consult qualified professionals for security, legal and compliance decisions.

No warranty

This report is provided "as is" without any express or implied warranty, including (without limitation) warranties of completeness, accuracy, fitness for a particular purpose, or non-infringement. The absence of findings does not mean the absence of vulnerabilities, risks, or compliance gaps.

Limitation of liability

To the maximum extent permitted by applicable law, Belitum BV shall not be liable for any indirect, incidental, consequential, special, punitive, reputational, or business interruption damages (including loss of profits, revenue, goodwill, or data) arising out of or related to this report, even if Belitum BV has been advised of the possibility of such damages. In all cases, the total liability of Belitum BV is limited to the amount paid for the generation of this report.

No certification, no attestation

References to GDPR, ISO/IEC 27001, OWASP, NIST, or other standards and frameworks are purely indicative mappings based on automated signals. They do not constitute certification, regulatory approval, a formal audit, or a legal conformity assessment. Formal compliance requires an appropriately scoped review by qualified professionals.

Client responsibility & validation

The recipient remains solely responsible for evaluating and validating findings, implementing measures, and complying with applicable laws and regulations. Critical findings should be independently validated before action is taken. Consult qualified professionals for security, legal, and compliance decisions.

Security is ongoing

Security and compliance are ongoing processes. This report does not guarantee immunity from cyber attacks, future vulnerabilities, or continued compliance. Results may change due to updates, configuration changes, third-party services, or newly disclosed vulnerabilities.

Confidentiality & use

This report is intended for the addressed recipient. It may not be copied, distributed, published, or used by third parties without the prior written consent of Belitum BV.

Applicable law & competent court

This report is governed by Belgian law. Disputes fall under the exclusive jurisdiction of the competent courts of the registered office of Belitum BV.