SAMPLE REPORT

Website Security Check

Pre-launch review and findings summary

PREPARED FOR	WEBSITE	REPORT DATE	REFERENCE
Northline Cabinetry	northlinecabinetry.com	August 14, 2026	CSV-SC-2026-0148

SCOPE OF THIS CHECK

This review covers the public website at the address above: its transport security and certificate, HTTP security headers, contact and quote form abuse protection, request rate limiting, exposed files and directories, software and dependency currency, and the configuration of the hosting and DNS records we manage for this site.

RESULT

Site cleared for launch

8 checks run · 5 passed as configured · 3 items fixed before launch · 0 items left open

This is a point-in-time review, not a certification, compliance audit, or penetration test. It reduces risk; no website can be guaranteed secure. Findings reflect the site as configured on the report date and may change as content, plugins, or third-party services change.

SECTION ONE

Summary at a glance

Plain English first: the site is in good shape. Five of the eight checks passed exactly as we configure them by default. Three needed work — all three were fixed before launch and re-tested. Nothing is left open for you to action.

CHECK	STATUS
HTTPS and SSL certificate Valid, auto-renewing, HTTP redirected to HTTPS	PASS
Security headers HSTS, CSP, X-Frame-Options, referrer and MIME policies applied	FIXED
Form abuse protection Spam, profanity and payload-size filtering on both forms	PASS
Request rate limiting Per-source limits on forms and the chat endpoint	PASS
Exposed files and directories No source maps, backups, config or index listings reachable	FIXED
Software and dependencies All packages current, no known advisories at build	PASS
DNS and email records SPF and DMARC present; registrar lock enabled	FIXED
Admin surface No login, database or admin panel exposed on this site	PASS

WHAT THE STATUSES MEAN

Pass — configured correctly at the time of testing. Fixed — an issue was found and corrected by us before launch, then re-tested. Note — no action needed now, but worth knowing about.

SECTION TWO

Findings and what we did

01 Strict-Transport-Security header was missing

FIXED

Why it matters
Without it, a visitor's very first request can be made over plain HTTP before the redirect happens, which is the moment an attacker on shared Wi-Fi would target.

What we did
Added HSTS with a one-year duration covering subdomains, and confirmed every HTTP request now redirects to HTTPS before any content is served.

02 Content Security Policy allowed any external script source

FIXED

Why it matters
A permissive policy means that if a third-party embed were ever compromised, the browser would happily run whatever it was told to run.

What we did
Narrowed the policy to the specific analytics and font providers this site actually uses, removed wildcard sources, and verified the site still renders and tracks correctly.

03 Build source maps were reachable in production

FIXED

Why it matters
Source maps expose your unminified code and internal file structure — useful to an attacker mapping the site, and of no benefit to visitors.

What we did
Disabled source map output for production builds and confirmed the previous files return a 404 rather than content.

HOW WE TEST

Every item above is checked against the live site with industry-standard scanning tools and by hand, then re-tested after any fix. We only ever scan sites we build and operate, or sites the owner has authorised us in writing to test. Nothing destructive is run, no passwords are guessed, and no customer data is touched.

SECTION TWO, CONTINUED

Findings and what we did

04 Contact and quote forms accepted unbounded submissions

PASS

Why it matters
Unlimited submissions invite spam floods and can run up sending costs.

What we did
Already covered by our standard build: per-source rate limiting, a payload size cap, and spam and profanity filtering. Verified by submitting test traffic against both forms.

05 Vulnerability scanners were able to enumerate pages freely

PASS

Why it matters
Automated tools sweep the internet constantly looking for known weak points; letting them crawl unchecked gives them a free map.

What we did
Automated abuse blocking is active: scanner signatures and abnormal crawl patterns are refused, while search engines such as Google and Bing remain allowed.

06 Domain email records were incomplete

FIXED

Why it matters
Missing SPF and DMARC records make it easier for someone to send email that appears to come from your domain.

What we did
Published SPF and DMARC records at the registrar and enabled the registrar's transfer lock. Deliverability re-tested after propagation.

WORDING WE AVOID

You will not see the words hack-proof, certified or compliant anywhere in this report, because no honest review can promise them. What you get instead is a plain record of what was checked, what was changed, and what is still your responsibility — written so you can hand it to an insurer, a client or a new developer and have it make sense.

SECTION THREE

What this does not cover

Being straight with you matters more than sounding impressive, so here is the honest edge.

- It is a review of the public site and the configuration we control — not a penetration test, a code audit of third-party software, or a compliance certification.
- It does not cover your email inbox, your social accounts, your devices, or any system we did not build or configure for you.
- It cannot protect against a password you reuse or share. Account security on your registrar, email and payment tools stays with you.
- It reflects the site on the report date. New pages, plugins, embeds or integrations added later are outside the scope of this report.

NEXT STEPS

Keeping it this way

Keep the certificate on auto-renew

Already enabled. Nothing to do unless you move hosting.

Tell us before adding embeds

Booking widgets, chat tools and tracking pixels change the security policy — we adjust it in minutes.

Quarterly re-check

On any care plan we re-run this check every three months and send you an updated one-page summary.

Attack alerts

Care plan sites email us automatically if a scanner or attack pattern is detected, so we see it before you do.

QUESTIONS ABOUT THIS REPORT

Reply to the email it came with, or reach us directly.

contact@casvori.com · (551) 226-9834 · casvori.com