Website *Security Check*

Prepared for Northline Cabinetry

Site reviewed: https://northlinecabinetry.example

Scan date: August 22, 2026 · Report issued: August 25, 2026

RESULT AT A GLANCE

10 findings · 1 high · 3 medium · 4 low · 2 informational

No evidence of an active compromise. The high-risk finding is a publicly reachable database backup file, which should be removed today. Everything else is configuration work.

SCOPE

Automated security scanning of the public website at the address above (44 pages crawled), followed by a manual review of every alert to remove false positives. Anything behind a login, third-party embeds, and infrastructure not serving this website were out of scope.

AUTHORIZATION

Testing was carried out during the window agreed with Northline Cabinetry on August 21, 2026, after written confirmation that the requester owns the website or is authorized by its owner to approve testing of it.

PLEASE READ

This is a point-in-time review of a public website. It is not a certification, a compliance audit (SOC 2, PCI, HIPAA, GDPR), or a penetration test, and no website can be guaranteed secure. It reflects the site as configured on the scan date above.

Summary of findings

Findings are grouped by risk. Confidence describes how certain we are the issue is real after the manual pass; instances is how many pages or responses it appeared on.

RISK	FINDING	CONFIDENCE	SEEN ON
High	Database backup file publicly downloadable	High	1
Medium	No Content Security Policy header	High	44
Medium	Session cookie missing Secure and HttpOnly flags	High	3
Medium	Outdated JavaScript library with known advisories	Medium	2
Low	Strict-Transport-Security header not set	High	44
Low	Clickjacking protection header absent	High	44
Low	MIME-type sniffing not disabled	High	44
Low	Directory listing enabled on /uploads/	Medium	1
Info	No DMARC record published for the domain	High	1
Info	Source maps published alongside site scripts	Medium	4

TESTED, NOTHING FOUND

SQL injection and command injection on every form field found · reflected and stored cross-site scripting · path traversal and local file inclusion · open redirects · exposed .git and .env files · mixed content on HTTPS pages · default admin paths and installer files · weak or expired TLS certificate · SPF record (present and correctly scoped).

HOW WE GRADE RISK

High	Exploitable now, with real consequences for you or your customers. Fix today.
Medium	Removes a protection an attacker would otherwise have to defeat. Fix this month.
Low	Hardening. Individually minor, collectively the difference between a maintained and an abandoned site.
Info	Not a vulnerability. Worth knowing, worth tidying when convenient.

HOW WE TEST

Industry-standard automated security scanning across the whole public site, then a manual pass over every alert. Raw scans over-report; anything we could not reproduce by hand was removed before this report was written.

Findings in detail

One entry per finding: where we saw it, why it matters in plain English, and the specific change to make.

HIGH — Fix: Today

Database backup file publicly downloadable

Where https://northlinecabinetry.example/backups/site-2026-02-14.sql.gz (2.4 MB, returned 200 OK)

Why Anyone who guesses or stumbles on this address can download a copy of your database — customer enquiries, order records, and any password hashes it contains — without logging in to anything.

Do this Delete the file from the web root today and move backups to storage that is not served by the website. Then check your access logs for prior downloads of that path.

MEDIUM — Fix: This month

No Content Security Policy header

Where All 44 pages crawled

Why Without this header, a script injected through a compromised plugin or advert can run freely on your pages and read what visitors type into your forms.

Do this Add a Content-Security-Policy header that names the sources your site actually uses, starting in report-only mode for a week so nothing legitimate breaks.

MEDIUM — Fix: This month

Session cookie missing Secure and HttpOnly flags

Where Login and cart cookies on 3 responses

Why A cookie without these flags can travel over an unencrypted connection and can be read by JavaScript, which makes session hijacking considerably easier.

Do this Set Secure, HttpOnly and SameSite=Lax on all session cookies in your platform's session configuration.

MEDIUM — Fix: This month

Outdated JavaScript library with known advisories

Where jQuery 1.12.4 loaded on 2 templates

Why The version in use has publicly documented vulnerabilities. Automated attack tools scan for exactly this and it also signals that other components may be behind.

Do this Update to a currently supported release and re-test the pages that use it. If a theme pins the old version, raise it with the theme vendor.

LOW — Fix: This quarter

Strict-Transport-Security header not set

Where All 44 pages crawled

Why Visitors typing your address without https:// make one unencrypted request before being redirected, which is the moment an attacker on shared Wi-Fi can intercept.

Do this Add Strict-Transport-Security with a one-year max-age once you are confident every subdomain serves HTTPS.

Findings in detail (continued)

Lower-risk items. None of these are urgent on their own; together they are the difference between a site that looks maintained and one that looks abandoned.

LOW **Fix: This quarter**

Clickjacking protection header absent

Where All 44 pages crawled

Why Your pages can be loaded invisibly inside someone else's site and used to trick visitors into clicking things they cannot see.

Do this Add frame-ancestors to the Content Security Policy, and X-Frame-Options: SAMEORIGIN for older browsers.

LOW **Fix: This quarter**

MIME-type sniffing not disabled

Where All 44 pages crawled

Why Browsers left to guess a file's type can be tricked into running an uploaded image or document as code.

Do this Send X-Content-Type-Options: nosniff on every response.

LOW **Fix: This quarter**

Directory listing enabled on /uploads/

Where https://northlinecabinetry.example/uploads/ returns a browsable file index

Why It lets anyone read the full contents of the folder, including files you uploaded but never linked from a page.

Do this Turn off directory indexing for that path at the server or host level.

INFO **Fix: This quarter**

No DMARC record published for the domain

Where DNS lookup: _dmarc.northlinecabinetry.example — no record

Why Without DMARC it is easier for someone to send invoices or quotes that appear to come from your domain.

Do this Publish a DMARC record starting at p=none, review the reports for a fortnight, then move to quarantine.

INFO **Fix: This quarter**

Source maps published alongside site scripts

Where 4 .map files reachable under /assets/

Why Source maps rebuild your original code in a browser's developer tools. Not a vulnerability by itself, but it hands anyone poking at the site a much clearer map of it.

Do this Stop publishing .map files in production builds, or block them at the host.

Limits, and what happens next

WHAT THIS COVERS

The public website at the address on the cover, as configured on the scan date. Automated scanning across every page we could reach by following links, plus a manual review of each alert.

WHAT IT DOES NOT COVER

— Anything behind a login, unless credentials were supplied and testing them was agreed in writing.

— Password or credential guessing, denial-of-service or load testing, social engineering, and phishing.

— Third-party services embedded in the site (payment widgets, booking tools, chat), which belong to their vendors.

— Your email accounts, staff devices, internal networks, and anything not serving this website.

— Compliance certification of any kind. This report is not evidence of SOC 2, PCI DSS, HIPAA, or GDPR compliance.

— Any guarantee. A site can be secure on the scan date and vulnerable a week later after a plugin update.

WHAT HAPPENS NEXT

Work through the high finding today and the medium findings this month. If you would like us to carry out the fixes, we quote that separately once we have seen the hosting setup. A re-check after remediation confirms the changes landed. Care plan clients get a re-check each quarter at no extra cost.

RE-CHECKING

A re-check after remediation is $79 within 60 days of this report and confirms each finding above is closed. Sites on a Casvori care plan are re-checked every quarter as part of the plan, with a short written summary each time.

Questions about anything in this report?

Email contact@casvori.com or call (551) 226-9834. We are happy to walk through it with whoever maintains the site, at no charge.

Casvori Website Design LLC · Morristown, New Jersey · Report reference SC-2026-0184

WORDING WE AVOID, ON PURPOSE

We will never describe this work as a penetration test, an audit, a certification, or proof of compliance, and we ask that you do not either. It is a security check: a scan of a public website plus a human review, on one date. Anyone offering more than that for this price is describing something they are not doing.