Security Report

Automated, authorized security assessment

ASSESSED TARGET

https://www.muster-schreinerei.example

Created
1 Oct 2026, 10:30 CEST

Scan performed
1 Oct 2026, 10:30 CEST

Assessment depth
In-depth assessment (after proof of ownership)

C

Overall rating

Medium vulnerabilities — remediation recommended.

Most severe issue: Medium

4	4	1	0	9
Vulnerabilities	Defended	Not applicable	Errors	Total checks

SAMPLE REPORT: Fictional website under the reserved .example domain. All findings are examples and do not concern any real company.

1. Introduction

This report documents an automated security assessment of the website named above, performed by Sondar. It checks whether the site is protected against the most common and most consequential vulnerabilities — from the configuration of encryption and protective headers, through the handling of input, to openly accessible files and services.

Because ownership of the domain was proven, the assessment includes active tests in addition to the passive inspection: Sondar sends clearly harmless test inputs and observes the response to demonstrate whether a vulnerability is actually exploitable — without exploiting it.

Important: a scan is a snapshot at the time of testing. It shows the vulnerabilities found and how to remediate them, but does not prove complete security.

2. System analysis

Target URL	**https://www.muster-schreinerei.example**
Scan ID	**00000000-0000-4000-8000-000000000000**
Assessment time	**1 Oct 2026, 10:30 CEST**
Proof of ownership	**provided — active in-depth assessment unlocked**
Scope	**9 individual checks**
Rating	**Grade C · most severe Medium**

3. Attack surface

Before testing, Sondar determines which addresses your site actually exposes — from robots.txt, the sitemap, and the links and forms on the homepage. Only what appears here can then be tested in a targeted way.

Discovered endpoints	**4**
Requests for discovery	**12**
Sitemap	**6 entries**
robots.txt	**present, 1 disallow rule**

GET https://www.muster-schreinerei.example/
Homepage · no parameters

GET https://www.muster-schreinerei.example/suche
Form · Parameters: q

GET https://www.muster-schreinerei.example/kontakt
Link · no parameters

GET https://www.muster-schreinerei.example/referenzen
Sitemap · Parameters: seite

4. Checks performed

The following check areas were covered. The coloured dot shows the result per area: red/orange = vulnerability requiring action, green = protection confirmed, grey = nothing notable.

- **Security Misconfiguration**
  Medium — action required · 4 checks
- **Software and Data Integrity Failures**
  Medium — action required · 1 check
- **Email Security**
  Low — action required · 2 checks
- **Cryptographic Failures**
  Protection confirmed · 1 check

- **Injection**
  Protection confirmed · 1 check

5. What was attempted where

The active checks send only clearly marked, harmless test inputs and demonstrate solely the EXISTENCE of a vulnerability — no data is read out. Most of them test via GET; endpoints whose address suggests a state change (e.g. log out, delete, order) are deliberately left out. The form checks (CSV/formula injection (Sheets), Email header injection (CRLF)), however, send at most one marked test submission per form endpoint via POST, including to typical form addresses such as /api/kontakt; it may reach the operator as an email or a spreadsheet row. The list below shows which endpoint was tested with which input and what came back.

- **GET https://www.muster-schreinerei.example/suche · q** — clean
  Input: XSS marker — Response: not reflected
- **GET https://www.muster-schreinerei.example/referenzen · seite** — clean
  Input: XSS marker — Response: not reflected
- **GET https://www.muster-schreinerei.example/uploads/** — clean
  Input: Directory request — Response: HTTP 403, no file listing

6. Findings in detail

Strict-Transport-Security missing/weak

Vulnerability · Medium · Security Misconfiguration

EVIDENCE

The homepage is served over HTTPS but sends no Strict-Transport-Security header. A browser may fall back to HTTP on the first visit.

RECOMMENDATION

Set the header "Strict-Transport-Security: max-age=31536000; includeSubDomains" in the web server or hosting panel once all subdomains support HTTPS.

Third-party scripts without Subresource Integrity (SRI)

Vulnerability · Medium · Software and Data Integrity Failures

EVIDENCE

Two scripts are loaded from a third-party CDN without an integrity attribute. If the CDN is compromised, foreign code runs on the website.

RECOMMENDATION

Add an integrity attribute with the SHA-384 hash and crossorigin="anonymous" to each third-party script, or serve the file yourself.

DMARC in monitoring mode only (p=none)

Vulnerability · Low · Email Security

EVIDENCE

The DMARC record is "v=DMARC1; p=none". Forged mail in the domain's name is reported but not rejected.

RECOMMENDATION

Review the reports for a few weeks, then raise the policy step by step to "p=quarantine" and later "p=reject".

Cookie "kontakt_sitzung": missing flags (SameSite)

Vulnerability · Low · Security Misconfiguration

EVIDENCE

The contact form's session cookie is set without the SameSite attribute.

RECOMMENDATION

Set the cookie with "SameSite=Lax" (or "Strict"), "Secure" and "HttpOnly".

Current TLS version

Defended · Info · Cryptographic Failures

EVIDENCE

The server offers only TLS 1.2 and 1.3.

RECOMMENDATION

No action needed.

No reflection of input found in HTML

Defended · Info · Injection

EVIDENCE

The marked test inputs in the search field did not appear unfiltered in the response.

RECOMMENDATION

No action needed.

No open directory listings

Defended · Info · Security Misconfiguration

EVIDENCE

Typical directories such as /uploads/ return no file listing.

RECOMMENDATION

No action needed.

SPF record present

Defended · Info · Email Security

EVIDENCE

The domain publishes an SPF record ending in "-all".

RECOMMENDATION

No action needed.

No CORS headers configured

Not applicable · Info · Security Misconfiguration

EVIDENCE

The website sends no CORS headers; for a website without an API this is harmless.

RECOMMENDATION

No action needed.