Sicherheitsbericht

Automatisierte, autorisierte Sicherheitsprüfung

GEPRÜFTES ZIEL

https://www.muster-schreinerei.example

Erstellt
01.10.2026, 10:30 MESZ

Scan durchgeführt
01.10.2026, 10:30 MESZ

Prüftiefe
Tiefenprüfung (nach Besitznachweis)

C

Gesamtbewertung

Mittlere Lücken — beheben empfohlen.

Schwerste Lücke: Mittel

4	4	1	0	9
Lücken	Abgewehrt	Nicht zutreffend	Fehler	Prüfungen gesamt

MUSTERBERICHT: Fiktive Website unter der reservierten Endung .example. Alle Befunde sind Beispiele und betreffen keine reale Firma.

1. Einleitung

Dieser Bericht dokumentiert eine automatisierte Sicherheitsprüfung der oben genannten Website durch Sondar. Geprüft wird, ob die Seite gegen die häufigsten und folgenreichsten Schwachstellen abgesichert ist — von der Konfiguration der Verschlüsselung und der Schutz-Header über die Behandlung von Eingaben bis hin zu offen zugänglichen Dateien und Diensten.

Da der Besitz der Domain nachgewiesen wurde, umfasst die Prüfung neben der passiven Sichtprüfung auch aktive Tests: Sondar sendet dabei gezielt harmlose Testeingaben und beobachtet die Reaktion, um zu belegen, ob eine Lücke tatsächlich ausnutzbar ist — ohne sie auszunutzen.

Wichtig: Ein Scan ist eine Momentaufnahme zum Prüfzeitpunkt. Er zeigt gefundene Schwachstellen und wie sie zu beheben sind, beweist aber keine vollständige Sicherheit.

2. Systemanalyse

Ziel-URL	**https://www.muster-schreinerei.example**
Scan-Kennung	**00000000-0000-4000-8000-000000000000**
Zeitpunkt der Prüfung	**01.10.2026, 10:30 MESZ**
Besitznachweis	**erbracht — aktive Tiefenprüfung freigeschaltet**
Umfang	**9 Einzelprüfungen**
Bewertung	**Note C · schwerste Lücke Mittel**

3. Angriffsfläche

Bevor geprüft wird, ermittelt Sondar, welche Adressen Ihre Seite überhaupt anbietet — aus robots.txt, der Sitemap sowie den Links und Formularen der Startseite. Nur was hier steht, kann anschliessend gezielt geprüft werden.

Erkannte Endpunkte	**4**
Abrufe für die Erkennung	**12**
Sitemap	**6 Eintrag/Einträge**
robots.txt	**vorhanden, 1 Disallow-Regel(n)**

GET https://www.muster-schreinerei.example/
Startseite · keine Parameter

GET https://www.muster-schreinerei.example/suche
Formular · Parameter: q

GET https://www.muster-schreinerei.example/kontakt
Link · keine Parameter

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

4. Durchgeführte Prüfungen

Die folgenden Prüfbereiche wurden abgedeckt. Der farbige Punkt zeigt je Bereich das Ergebnis: rot/orange = Lücke mit Handlungsbedarf, grün = Schutz bestätigt, grau = nichts Auffälliges.

- **Security Misconfiguration**
  Mittel — Handlungsbedarf · 4 Prüfung(en)
- **Software and Data Integrity Failures**
  Mittel — Handlungsbedarf · 1 Prüfung(en)
- **Email Security**
  Tief — Handlungsbedarf · 2 Prüfung(en)
- **Cryptographic Failures**
  Schutz bestätigt · 1 Prüfung(en)

- **Injection**
  Schutz bestätigt · 1 Prüfung(en)

5. Was wurde wo versucht

Die aktiven Prüfungen senden ausschliesslich klar markierte, schadfreie Testeingaben und weisen allein die EXISTENZ einer Lücke nach — es werden keine Daten ausgelesen. Die meisten prüfen per GET; Endpunkte, deren Adresse eine Zustandsänderung nahelegt (z. B. abmelden, löschen, bestellen), lassen sie bewusst aus. Die Formular-Prüfungen (CSV/Formel-Injection (Sheets), E-Mail-Header-Injection (CRLF)) senden dagegen je Formular-Endpunkt höchstens eine markierte Testeinsendung per POST, auch an typische Formular-Adressen wie /api/kontakt; sie kann beim Betrieb als E-Mail oder Tabellenzeile ankommen. Die folgende Liste zeigt, welcher Endpunkt mit welcher Eingabe geprüft wurde und was zurückkam.

- **GET https://www.muster-schreinerei.example/suche · q** — **unauffällig**
  Eingabe: XSS-Marker — Antwort: nicht reflektiert
- **GET https://www.muster-schreinerei.example/referenzen · seite** — **unauffällig**
  Eingabe: XSS-Marker — Antwort: nicht reflektiert
- **GET https://www.muster-schreinerei.example/uploads/** — **unauffällig**
  Eingabe: Verzeichnisaufruf — Antwort: HTTP 403, keine Dateiliste

6. Befunde im Detail

Strict-Transport-Security fehlt/schwach

Lücke · Mittel · Security Misconfiguration

BELEG

Die Startseite antwortet über HTTPS, sendet aber keinen Strict-Transport-Security-Header. Ein Browser kann beim ersten Aufruf auf HTTP zurückfallen.

EMPFEHLUNG

Im Webserver oder Hosting-Panel den Header «Strict-Transport-Security: max-age=31536000; includeSubDomains» setzen, nachdem alle Subdomains HTTPS können.

Fremd-Skripte ohne Subresource Integrity (SRI)

Lücke · Mittel · Software and Data Integrity Failures

BELEG

Zwei Skripte werden von einem fremden CDN geladen, ohne integrity-Attribut. Wird das CDN kompromittiert, läuft fremder Code auf der Website.

EMPFEHLUNG

Für jedes fremde Skript ein integrity-Attribut mit dem SHA-384-Hash und crossorigin="anonymous" ergänzen oder die Datei selbst ausliefern.

DMARC nur im Beobachtungsmodus (p=none)

Lücke · Tief · Email Security

BELEG

Der DMARC-Eintrag lautet «v=DMARC1; p=none». Gefälschte Mails im Namen der Domain werden gemeldet, aber nicht abgewiesen.

EMPFEHLUNG

Berichte einige Wochen auswerten, dann die Richtlinie schrittweise auf «p=quarantine» und später «p=reject» anheben.

Cookie "kontakt_sitzung": fehlende Flags (SameSite)

Lücke · Tief · Security Misconfiguration

BELEG

Das Sitzungs-Cookie des Kontaktformulars wird ohne das Attribut SameSite gesetzt.

EMPFEHLUNG

Das Cookie mit «SameSite=Lax» (oder «Strict»), «Secure» und «HttpOnly» setzen.

Aktuelle TLS-Version

Abgewehrt · Info · Cryptographic Failures

BELEG

Der Server bietet nur TLS 1.2 und 1.3 an.

EMPFEHLUNG

Keine Massnahme nötig.

Keine Reflexion der Eingabe im HTML gefunden

Abgewehrt · Info · Injection

BELEG

Die markierten Testeingaben im Suchfeld erschienen nicht ungefiltert in der Antwort.

EMPFEHLUNG

Keine Massnahme nötig.

Keine offenen Verzeichnislisten

Abgewehrt · Info · Security Misconfiguration

BELEG

Typische Verzeichnisse wie /uploads/ liefern keine Dateiliste.

EMPFEHLUNG

Keine Massnahme nötig.

SPF-Record vorhanden

Abgewehrt · Info · Email Security

BELEG

Die Domain veröffentlicht einen SPF-Eintrag mit «-all».

EMPFEHLUNG

Keine Massnahme nötig.

Keine CORS-Header konfiguriert

Nicht zutreffend · Info · Security Misconfiguration

BELEG

Die Website liefert keine CORS-Header; für eine Website ohne API ist das unbedenklich.

EMPFEHLUNG

Keine Massnahme nötig.