MUSTERBERICHT · vollständig fiktiv · keine Website geprüft

AO Conversions

Webriegel · Website-Sicherheitscheck

Musterbericht

Alle Angaben und **Beleg**e sind erfunden. Keine Kundenreferenz und kein Nachweis einer tatsächlichen Prüfung.

Firma : Musterbetrieb Beispielwerk (fiktiv)

Domain : musterbetrieb.example

Beispielkennung : MUSTER-001

Beispielstand : 03.11.2026

Beispieldatum : 03.11.2026, 10:00 Uhr CET

Datengrundlage : Ausschließlich erfundene Musterdaten; kein Kundenauftrag

Alle Angaben und **Beleg**e sind erfunden. Keine Kundenreferenz und kein Nachweis einer tatsächlichen Prüfung.

Kurzfassung

Der Bericht ordnet die dokumentierten **Befund**e nach ihrer Dringlichkeit. Manuelle Punkte bleiben offen und sind keine Entwarnung.

Kritisch : 0

Hoch : 1

Mittel : 2

Niedrig : 0

OK : 3

Manuell : 2

Befunde nach Dringlichkeit

Hoch M-03

Software und Versionen

Befund Eine fiktive Erweiterung verwendet im Beispiel einen nicht mehr gepflegten Versionsstand. Dafür sind keine weiteren Sicherheitsupdates vorgesehen.

Empfehlung Zuerst Sicherung erstellen. Erweiterung in einer Testumgebung aktualisieren oder ersetzen und anschließend die Funktionen prüfen. Keine konkrete ausnutzbare Lücke nachgewiesen.

Beleg Synthetischer **Beleg**: Beispiel-Erweiterung Formularbaustein; Wartungsstatus im Szenario: eingestellt. Keine reale Versions- oder CVE-Aussage. 03.11.2026, 10:00 Uhr CET

Mittel M-02

Schutz-Header und Cookies

Befund Die Content-Security-Policy fehlt im Beispiel. Eine solche Regel kann unerwünschte Skripte und fremde Einbettungen begrenzen.

Empfehlung Passende Regeln zunächst im Report-Only-Modus testen. Danach aktivieren und Formulare sowie eingebundene Inhalte prüfen. Fehlender Header allein beweist keinen Angriff.

Beleg Synthetischer **Beleg**: Content-Security-Policy fehlt; Sitzungscookie mit Secure und HttpOnly. 03.11.2026, 10:00 Uhr CET

Mittel M-08

Schutz vor gefälschten E-Mails

Befund SPF erlaubt im Beispiel zu viele Absender; DMARC überwacht nur. Gefälschte Absender werden dadurch nicht zuverlässig zurückgewiesen.

Empfehlung SPF auf berechtigte Versender begrenzen. DKIM-Signaturen anhand einer autorisierten Testmail prüfen. DMARC nach Auswertung schrittweise verschärfen, um legitime Mails nicht zu blockieren.

Beleg Synthetischer **Beleg**: SPF v=spf1 +all; DMARC v=DMARC1; p=none; DKIM-Signierung nicht verifiziert. 03.11.2026, 10:00 Uhr CET

OK M-01

HTTPS und Verschlüsselung

Befund Im Beispiel sind HTTPS und ein gültiges Zertifikat vorhanden. Das schützt die Übertragung, nicht die gesamte Website.

Empfehlung Zertifikatserneuerung überwachen und Weiterleitungen regelmäßig prüfen.

Beleg Synthetischer **Beleg**: HTTPS aktiv; TLS 1.3; Zertifikatsprüfung erfolgreich. 03.11.2026, 10:00 Uhr CET

OK M-04

Offene Dateien und Zugänge

Befund Im Beispiel liefern die vorgesehenen Dateipfade keine öffentlich lesbaren Konfigurations- oder Sicherungsdateien.

Empfehlung Sicherungen außerhalb des öffentlichen Webverzeichnisses speichern. Einzelne erfolglose Abrufe schließen andere offene Dateien nicht aus.

Beleg Synthetischer **Beleg**: feste Testpfade mit 404; Gegenprobe ebenfalls 404; keine Dateiinhalte. 03.11.2026, 10:00 Uhr CET

OK M-06

Geheime Schlüssel im Code

Befund Im betrachteten Beispielcode wurde kein geheimer Schlüssel erkannt. Das ist keine vollständige Prüfung aller Dateien.

Empfehlung Geheimnisse ausschließlich serverseitig verwalten. Bei einem echten Fund betroffene Schlüssel nach Prüfung sperren und ersetzen.

Beleg Synthetischer **Beleg**: Startseiten-Code und eigene Skripte ohne Schlüsseltreffer; keine echten Schlüssel verwendet. 03.11.2026, 10:00 Uhr CET

Manuell M-05

Formulare

MUSTER · vollständig fiktiv · keine Website geprüft

Befund Das Beispielformular ist sichtbar. Eingabefilter, Versand und Missbrauchsschutz sind von außen nicht ausreichend beurteilbar.

Empfehlung Mit schriftlicher Freigabe serverseitige Eingabeprüfung und Missbrauchsschutz kontrollieren. In dieser Außenprüfung wird kein Formular versendet.

Beleg Synthetischer **Beleg**: Kontaktformular vorhanden; kein Absenden; interne Verarbeitung unbekannt. 03.11.2026, 10:00 Uhr CET

Manuell M-07

Schutz deiner Datenbank

Befund Datenbankregeln sind im Beispiel von außen nicht sichtbar. Ob fremde Zugriffe verhindert werden, bleibt offen.

Empfehlung Berechtigungen mit einem begrenzten Lesezugang prüfen lassen. Insbesondere anonyme Zugriffe und die Trennung verschiedener Benutzer kontrollieren.

Beleg Synthetischer **Beleg**: kein Datenbankzugriff; keine Anmeldedaten; Zugriffsregeln nicht geprüft. 03.11.2026, 10:00 Uhr CET

Alle Prüfpunkte

HTTPS und Verschlüsselung : M-01 (OK)

Schutz-Header und Cookies : M-02 (Mittel)

Software und Versionen : M-03 (Hoch)

Offene Dateien und Zugänge : M-04 (OK)

Formulare : M-05 (Manuell)

Geheime Schlüssel im Code : M-06 (OK)

Schutz deiner Datenbank : M-07 (Manuell)

Schutz vor gefälschten E-Mails : M-08 (Mittel)

Nicht geprüft

Was wir nicht geprüft haben

Keine Angriffe, keine Lasttests, keine Logins und kein Formularversand waren Teil dieser Prüfung.

Interne Serverlogik blieb ungeprüft.

M-05 : Formulare

M-07 : Schutz deiner Datenbank

Nächste Schritte im Beispiel

Priorität 1: Die nicht mehr gepflegte Beispiel-Erweiterung ersetzen oder aktualisieren.

Priorität 2: Schutz-Header sowie SPF und DMARC fachgerecht konfigurieren und auf Nebenwirkungen testen.

Priorität 3: Formularverarbeitung und Datenbankrechte manuell prüfen. Danach offene **Befund**e erneut kontrollieren.

Die Stufen zeigen die Dringlichkeit im erfundenen Szenario. Keine Sicherheitsgarantie und kein vollständiger Penetrationstest.

MUSTER · vollständig fiktiv · keine Website geprüft

Laufende Prüfung: 19 € im Monat

Der Website-Sicherheitscheck kostet 200 € einmalig, jeweils zuzüglich Umsatzsteuer. Nur für Unternehmen.

Neue Lücken werden laufend bekannt, etwa in PHP, WordPress oder Plugins. Deshalb prüfen wir deine Website nach dem Check jeden Monat erneut von außen. Du bekommst einen kurzen Bericht über neue und noch offene Punkte. Bei kritischen **Befund**en melden wir uns direkt bei dir. Du kannst die laufende Prüfung gleich mit dem Check oder später buchen und jederzeit per E-Mail zum Monatsende kündigen.

AO Conversions · Webriegel · Fiktives Beispiel · Stand: 03.11.2026, 10:00 Uhr CET