RAPPORT D'AUDIT DE SÉCURITÉ WEB

Client : **Boulangerie Moreau SARL**

Cible : **boulangerie-moreau.fr**

Réalisé par : Aegis

Date : 2026-07-24T20:44:18+00:00

Résumé exécutif

Cet audit a identifié **5** point(s) d'attention sur **boulangerie-moreau.fr**, dont **1** critique(s) et **1** élevé(s). La posture de sécurité est notée **E**. Une action corrective rapide est recommandée. Points prioritaires : EXPOSED PATH, SQLI ERROR BASED, CORS MISCONFIG.

Note de risque : **E** (score 78).

Évolution depuis le dernier scan : **4** nouveau(x), **1** persistant(s), **0** corrigé(s).
Audit réalisé sur une cible autorisée (mandat signé, autorisation scellée dans la chaîne de possession).

1. Synthèse par criticité

Sévérité	Nombre
CRITICAL	1
HIGH	1
MEDIUM	2
LOW	1
INFO	0

2. Détail des vulnérabilités

Sévérité	Type	Description	Remédiation
CRITICAL	EXPOSED PATH	Fichier de configuration /.env accessible publiquement (identifiants de base de donnees exposes). A05:2021 · CWE-538 · CVSS 7.5 · Confiance : confirmé	Restreindre ou retirer l'accès au chemin sensible exposé (authentification, règle serveur, retrait du fichier).
HIGH	SQLI ERROR BASED	Injection SQL possible sur le parametre id de la fiche produit. A03:2021 · CWE-89 · CVSS 9.8 · Confiance : confirmé	Corriger l'injection SQL : requêtes paramétrées, et masquer les messages d'erreur SQL en production.
MEDIUM	CORS MISCONFIG	Politique CORS permissive refletant une origine arbitraire. A05:2021 · CWE-942 · CVSS 7.5 · Confiance : confirmé	Restreindre Access-Control-Allow-Origin à une liste blanche d'origines de confiance ; ne jamais combiner « * » et allow-credentials.
MEDIUM	MISSING SECURITY HEADER	En-tete Content-Security-Policy absent (protection anti-injection affaiblie). A05:2021 · CWE-693 · CVSS 3.7 · Confiance : confirmé	Ajouter l'en-tête de sécurité manquant (HSTS, CSP, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy).
LOW	TECH STACK DISCOVERED	Version du serveur web exposee dans les en-tetes de reponse. A05:2021 · CWE-200 · CVSS 0.0 · Confiance : confirmé	Masquer les bannières de version (réduit la surface de reconnaissance de l'attaquant).

3. Conformité (indicatif)

RGPD — 1 contrôle(s) en défaut : Art.32 — Sécurité du traitement (2)
ISO 27001 — 2 contrôle(s) en défaut : A.8.9 — Gestion de configuration (4), A.8.28 — Codage sécurisé (1)
PCI-DSS — 2 contrôle(s) en défaut : Req.2 — Configuration sécurisée (4), Req.6 — Développement sécurisé (1)
NIS2 — 2 contrôle(s) en défaut : Art.21 — Hygiène de configuration (3), Art.21 — Gestion des vulnérabilités (1)
Mapping indicatif d'aide à la priorisation ; ne remplace pas un audit de conformité formel.