LISTE DE CONTRÔLE DE CONFORMITÉ TOP 10 DE L'OWASP

APPLICATION AUDITÉE : OWASP Juice Shop

URL : http://localhost:3000

TYPE DE TEST : Test de sécurité applicative (Black Box)

MÉTHODOLOGIE : OWASP Top 10

OUTILS UTILISÉS : OWASP ZAP, Burp Suite

SYSTÈME : Kali Linux (Docker)

AUTEUR : *BARIKI Wilson*

Sommaire

I- A01 - Broken Access Control

Élément vérifié	Statut	Commentaire
Contrôle d'accès sur les fonctions sensibles	Non conforme	Non évalué en profondeur dans ce projet
Restriction d'accès par rôle	Non conforme	Tests non réalisés
Protection contre l'accès direct aux objets	Non conforme	Hors périmètre

II- A02 – Cryptographic Failures

Élément vérifié	Statut	Commentaire
Exposition d'informations sensibles	Partiellement conforme	Présence de commentaires suspects
Gestion sécurisée des données	Non conforme	Informations internes révélées
Suppression des informations inutiles	Non conforme	Commentaires détectés

III- A03 – Injection

Élément vérifié	Statut	Commentaire
Protection contre l'injection SQL	Non conforme	Injection SQL confirmée

Validation des entrées utilisateur	Non conforme	Entrées non filtrées
Utilisation de requêtes préparées	Non conforme	Non implémenté

IV- A04 – Insecure Design

Élément vérifié	Statut	Commentaire
Conception sécurisée de l'application	Non conforme	Application volontairement vulnérable
Analyse des menaces	Non conforme	Non observée
Défense en profondeur	Non conforme	Manque de contrôles

V- A05 – Security Misconfiguration

Élément vérifié	Statut	Commentaire
Headers de sécurité HTTP	Non conforme	CSP manquant
Configuration CORS sécurisée	Non conforme	Configuration inter-domaines faible
Paramètres par défaut sécurisés	Non conforme	Mauvaises configurations détectées

VI- A06 – Vulnerable and Outdated Components

Élément vérifié	Statut	Commentaire

Utilisation de composants à jour	Inconnu	Non vérifié
Gestion des dépendances	Inconnu	Hors périmètre
Surveillance des vulnérabilités	Non conforme	Non observée

VII- A07 – Identification and Authentication Failures

Élément vérifié	Statut	Commentaire
Gestion sécurisée de l'authentification	Non évalué	Non testé
Protection contre le bruteforce	Non évalué	Hors périmètre
Gestion des sessions	Non évalué	Non testé

VIII- A08 – Software and Data Integrity Failures

Élément vérifié	Statut	Commentaire
Intégrité des scripts externes	Non conforme	Inclusion JS cross-domain
Utilisation de SRI	Non conforme	Absence de contrôle
Chaîne de confiance	Non conforme	Scripts non vérifiés

IX- A09 – Security Logging and Monitoring Failures

Élément vérifié	Statut	Commentaire
Journalisation des événements	Non conforme	Non observée

Détection d'activités suspectes	Non conforme	Non visible
Alertes de sécurité	Non conforme	Absentes

X- A10 – Server-Side Request Forgery (SSRF)

Élément vérifié	Statut	Commentaire
Protection contre SSRF	Non évalué	Aucun test réalisé
Validation des URLs	Non évalué	Hors périmètre
Restrictions réseau	Non évalué	Non analysé

XI- Synthèse de conformité

Statut	Nombre
Non conforme	Majorité
Partiellement / Non évalué	Plusieurs
Conforme	Aucun

Conclusion

L'application **ne respecte pas** les exigences de sécurité définies par l'OWASP Top 10. Plusieurs vulnérabilités critiques et de mauvaises configurations ont été identifiées, justifiant un **niveau de risque global élevé**.