Déploiement d'OWASP Juice Shop avec Docker

1. Contexte et objectif

OWASP Juice Shop est une application web volontairement vulnérable, développée par la fondation OWASP à des fins pédagogiques. Elle reproduit une boutique en ligne de jus de fruits contenant de nombreuses failles de sécurité classiques (injections, contrôle d'accès défaillant, XSS, mauvaise configuration, etc.), à retrouver sous forme de défis notés selon leur difficulté.

L'objectif de cette documentation est de présenter le déploiement de Juice Shop via Docker, ainsi qu'une découverte rapide de l'interface et du système de suivi des défis.

2. Installation et lancement via Docker

Le code source du projet est disponible sur le dépôt officiel GitHub :

https://github.com/juice-shop/juice-shop

Plutôt que d'installer l'application manuellement, il est recommandé d'utiliser l'image Docker officielle, ce qui garantit un environnement isolé et reproductible.

2.1 Installation de Docker

Docker est installé et son service démarré au boot, puis l'utilisateur courant est ajouté au groupe docker afin d'exécuter les commandes sans sudo :

```
sudo apt install -y docker.io
sudo systemctl enable --now docker
sudo usermod -aG docker $USER
newgrp docker
```

2.2 Lancement du conteneur Juice Shop

L'image officielle bkimminich/juice-shop est ensuite récupérée et exécutée. Le conteneur est lancé en mode éphémère (--rm) et le port 3000 du conteneur est mappé sur le port 3000 de la machine hôte :

```
docker run --rm -p 3000:3000 bkimminich/juice-shop
```

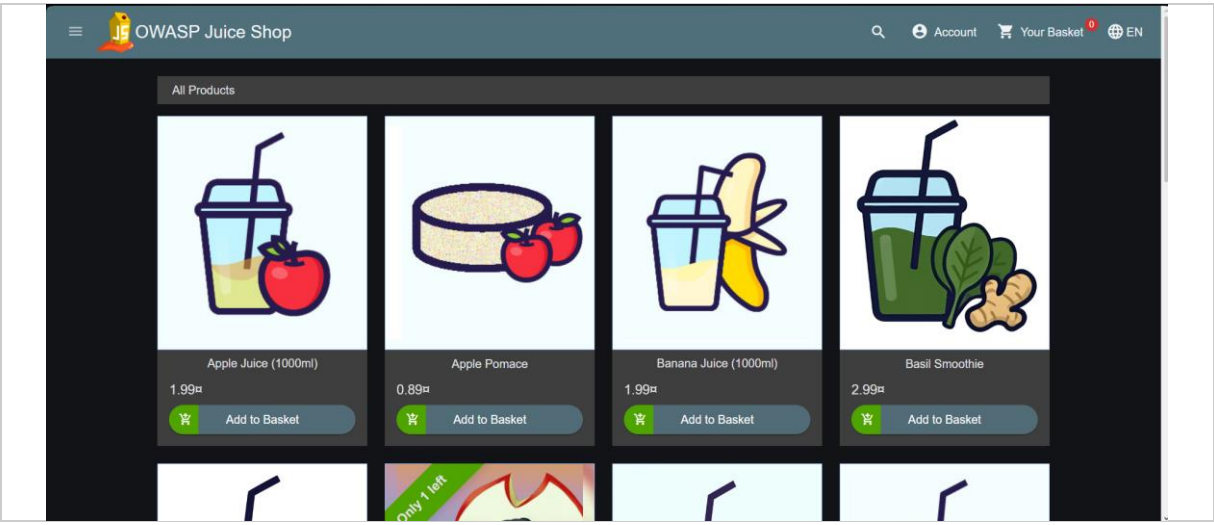
Une fois le conteneur démarré, l'application est accessible depuis un navigateur à l'adresse :

```
http://localhost:3000
```

3. Découverte de l'application

3.1 Page d'accueil

La page d'accueil affiche le catalogue des produits (jus, smoothies, etc.), chacun avec son prix et un bouton "Add to Basket" permettant de l'ajouter au panier. La barre de navigation supérieure donne accès au compte utilisateur, au panier et à la recherche.



3.2 Menu latéral

Le menu latéral donne accès aux fonctionnalités annexes de l'application : formulaire de contact, chat IA, informations sur l'entreprise (About Us), mur de photos, ainsi qu'au **Score Board** et au dépôt GitHub du projet.

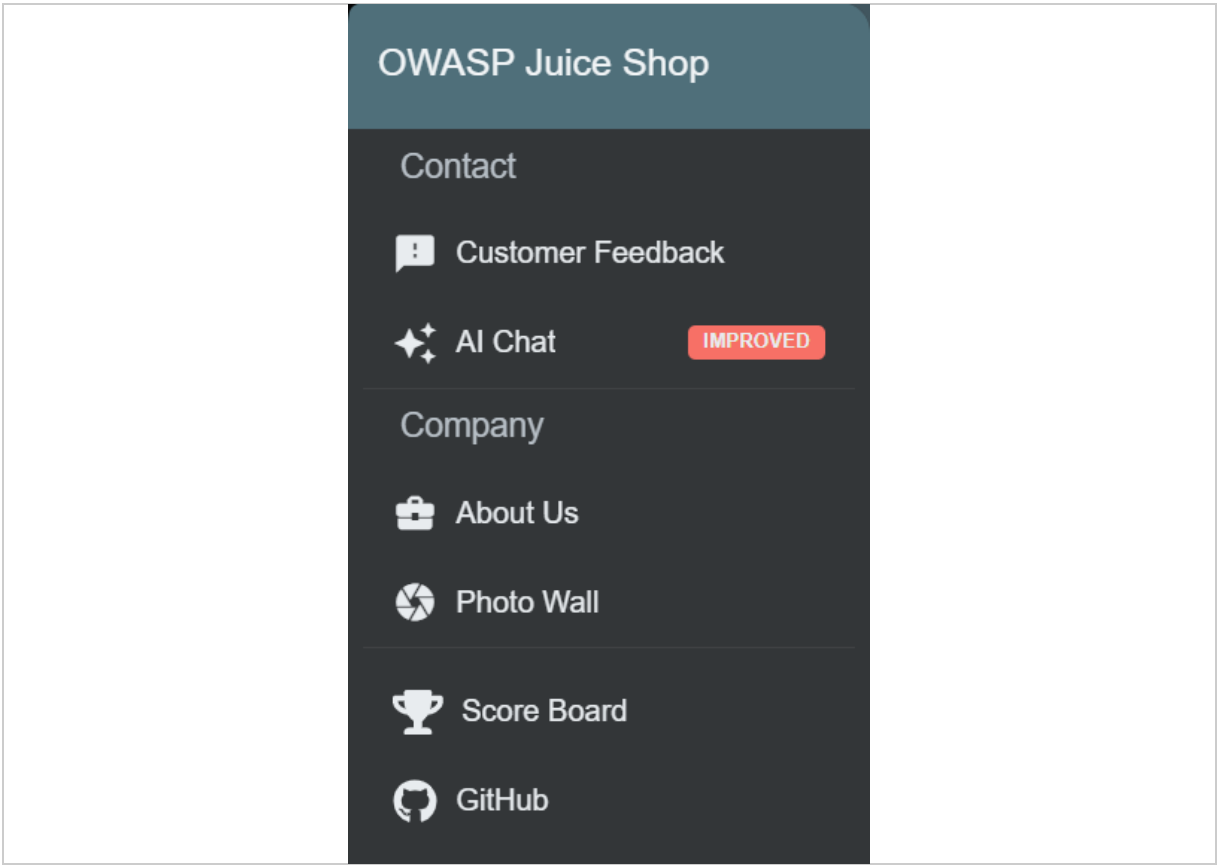
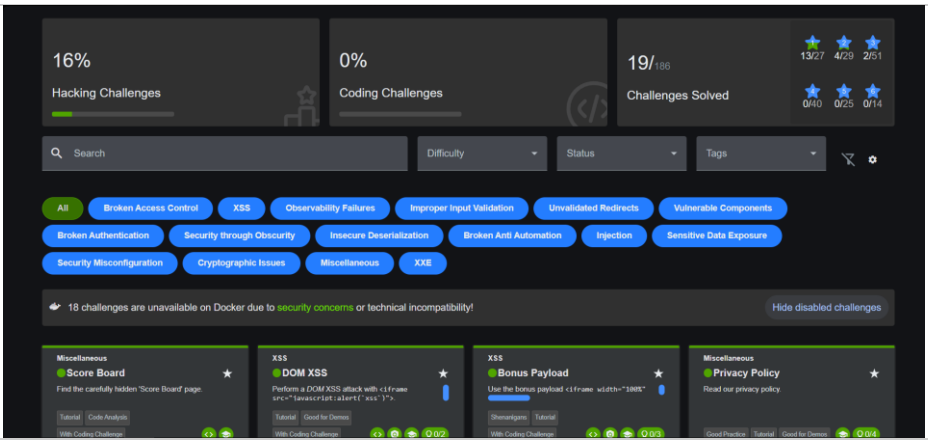


Figure 2 — Menu latéral de navigation

3.3 Score Board

Le Score Board recense l'ensemble des défis de l'application et permet de suivre sa progression, ici 19 défis sur 186 résolus (16% des défis "Hacking").



4. Types d'attaques disponibles dans les challenges

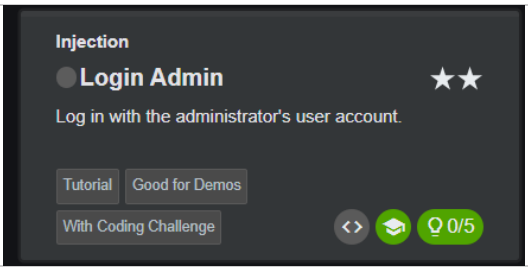
Chaque défi du Score Board est rattaché à une catégorie de vulnérabilité, correspondant globalement à l'OWASP Top 10 et à d'autres grandes familles de failles web. Les principales catégories proposées par Juice Shop sont :

- Injection : failles SQL, NoSQL ou commande, exploitées pour contourner une authentification ou extraire des données.
- Broken Access Control : contrôle d'accès défaillant permettant d'accéder à des ressources ou fonctions non autorisées.
- XSS (Cross-Site Scripting) : injection de scripts malveillants exécutés dans le navigateur d'une victime.
- Broken Authentication : mécanismes de connexion ou de gestion de session mal protégés.
- Sensitive Data Exposure : exposition de données confidentielles (mots de passe, informations personnelles).
- Security Misconfiguration : erreurs de configuration du serveur, de l'application ou de ses dépendances.
- Vulnerable Components : utilisation de bibliothèques ou dépendances obsolètes et vulnérables.
- Autres catégories : Improper Input Validation, Unvalidated Redirects, Insecure Deserialization, Broken Anti Automation, Cryptographic Issues, Observability Failures, XXE, Security through Obscurity et Miscellaneous.

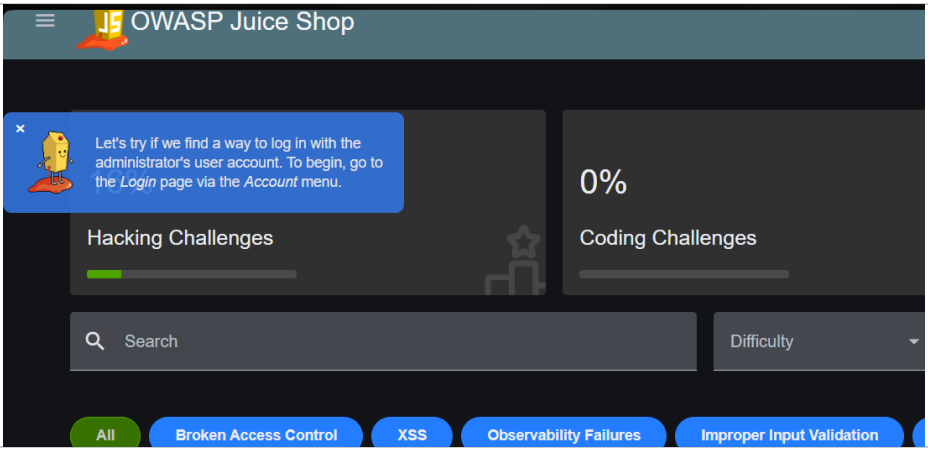
L'exercice ci-après illustre la résolution d'un défi de la catégorie Injection.

5. Exemple pratique : résolution du défi "Login Admin"

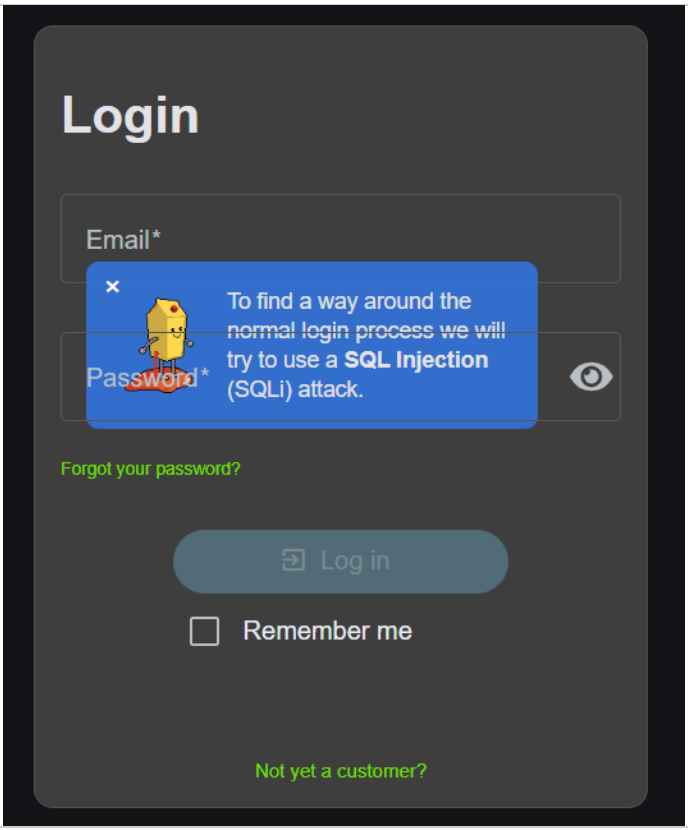
Le défi "Login Admin" (catégorie Injection, difficulté 2 étoiles) consiste à se connecter avec le compte administrateur du site sans en connaître le mot de passe.



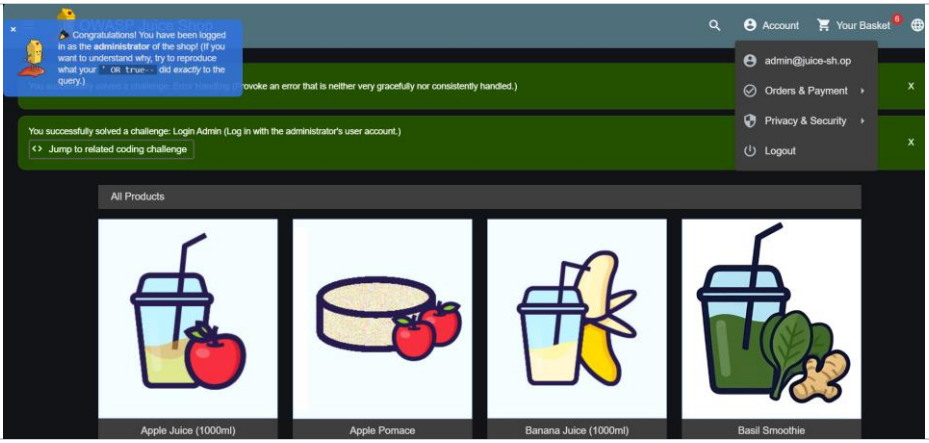
Un indice contextuel (pop-up bleue) s'affiche automatiquement sur la page d'accueil pour guider l'utilisateur : il invite à se rendre sur la page de connexion via le menu "Account".



Sur la page de connexion, un second indice précise la technique attendue : une injection SQL (SQL Injection) dans le formulaire d'authentification. En saisissant par exemple ' OR true-- dans le champ e-mail, la requête SQL exécutée côté serveur est détournée : la condition devient toujours vraie, ce qui permet de contourner la vérification du mot de passe et de se connecter avec le premier compte de la base, généralement celui de l'administrateur.



Une fois la requête piégée envoyée, l'application confirme la réussite du défi : un message de félicitations indique que la connexion a été effectuée en tant qu'administrateur, et une bannière verte confirme que le défi "Login Admin" est résolu. Le menu "Account" affiche alors l'adresse admin@juice-sh.op.



6. Conclusion

Le déploiement de Juice Shop via Docker permet d'obtenir en quelques commandes un environnement d'entraînement complet et isolé, sans installation de dépendances sur la machine hôte. Le Score Board constitue un outil pratique pour progresser méthodiquement à travers les différentes familles de vulnérabilités web (OWASP Top 10 et au-delà).