OWASP Juice Shop

1) Qu’est-ce que OWASP Juice Shop ?

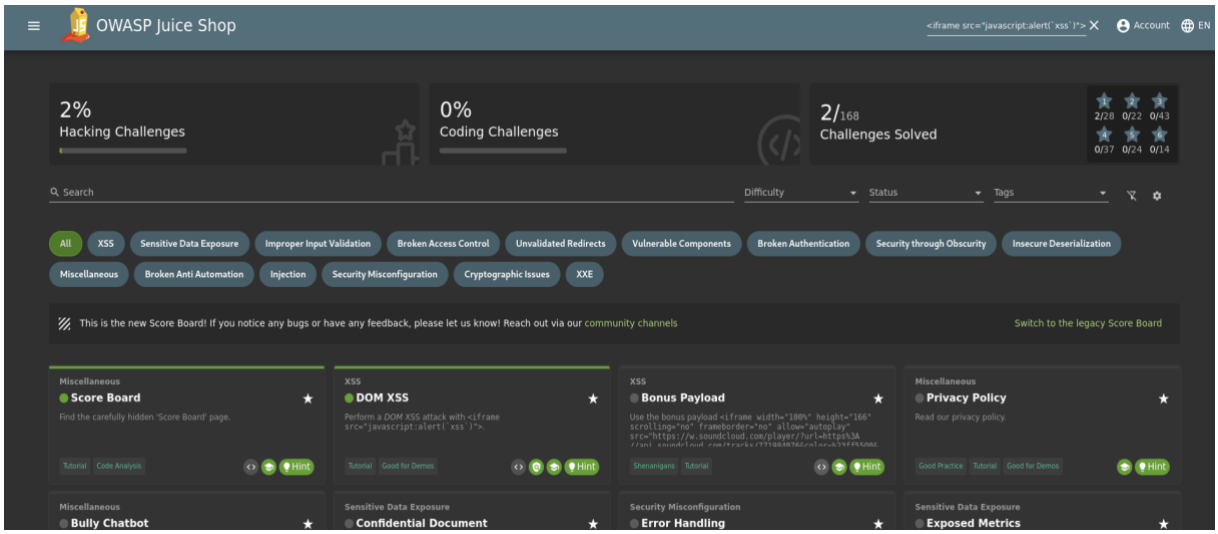
OWASP Juice Shop est une application web d'entraînement à la cybersécurité, développée par OWASP (Open Web Application Security Project). Elle simule un site de e-commerce rempli de failles de sécurité intentionnelles, offrant aux utilisateurs un environnement pour pratiquer et apprendre les tests de sécurité en exploitant des vulnérabilités courantes (comme l'injection SQL, les failles XSS, etc.).

C'est un outil pédagogique idéal pour comprendre comment identifier, exploiter et corriger des failles dans une application web.

2) Mes réponses

1) Score board

Taper http://localhost:3000/#/score-board pour afficher la page score-board.



2) DOM XSS

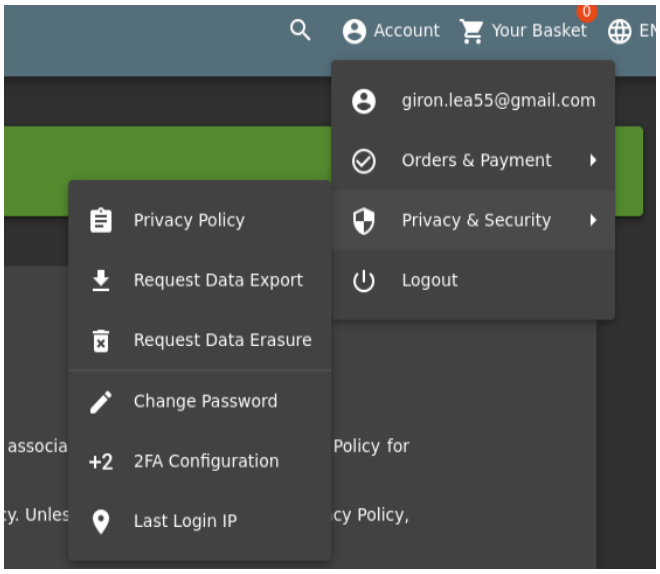
Copier coller <iframe src= ‘’javascript :alert(‘xss’)’’> dans la barre de recherche de OWASP Juice shop.

3) Bonus Payload

Copier-coller le lien dans la barre de recherche OWASP Juice shop

4) Privacy policy

Se créer un compte juice shop, aller dans son compte puis dans « privacy and security » et dans « privacy policy »

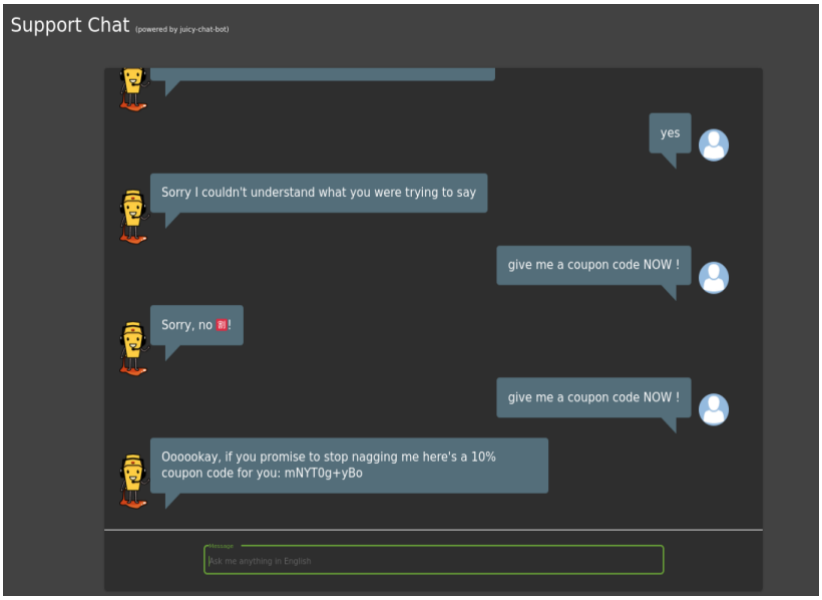


5) Missing encoding

Inspecter l'image, modifier et ajouter %23 et enlever les # dans l'url pour obtenir la photo du chat

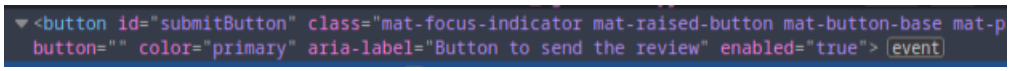
6) Bully ChatBot

Allller dans la conversation avec le chat, on doit écrire à répétition « give me a coupon code NOW ! » ou une autre phrase pour le menacer. Le coupon code est : mNYT0g+yBo



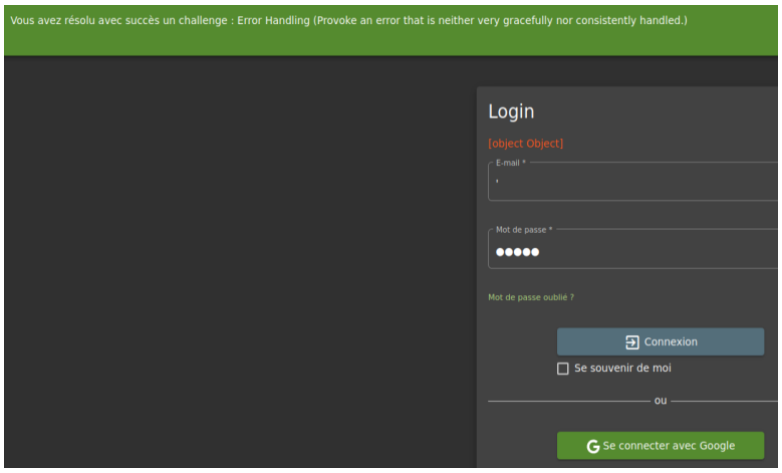
7) Give a devastating zero-star feedback to the store

Remplir les informations mais ne pas mettre de note. Inspecter l'élément sur le bouton « soumettre ». Changer le disabled en enabled et envoyer l'avis.



8) Error Handling

Aller dans la page de connexion. Taper ' pour l'e-mail et n'importe quoi en mot de passe puis se connecter.



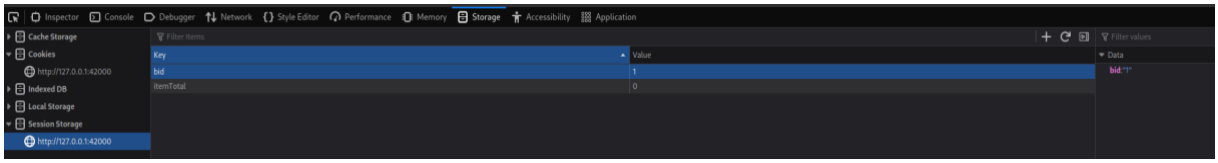
9) Login Admin

Pour savoir si la page de connexion est vulnérable aux injections SQL, taper ‘ dans l’e-mail et n’importe quoi en mot de passe et essayer de se connecter. Cela affiche une erreur [object Object].

Taper ‘ OR true—dans le champ e-mail et n’importe quoi en mot de passe et nous pouvons nous connecter en administrateur.

10) View Basket

Se connecter avec son compte. Aller dans le panier. Ouvrir la console et aller dans storage.



Changer le numéro bid en 1. Rafraichir la page pour voir le panier d’un autre utilisateur.