Mettre en pratique le top 10 OWASP

|  |  |
| --- | --- |
| Elément | Description |
| **Compétences** | **Pouvoir reconnaître les lacunes de sécurité ainsi que leurs causes dans une application. Pouvoir proposer et implémenter des contre-mesures.** |
| **Objectifs** | A la fin de cette séquence, les apprentis seront capables d’expliquer des lacunes de sécurité et les conséquences possibles lors d’attaques |
| **Durée estimée** | 45 min |
| **Répertoire de travail** |  |
| **Fichiers sources** |  |
| **A produire** | Répondre aux questions directement dans ce document |
| **Moyens d’aide** |  |
| **Changelog** | Auteur original et version |

# Mise en place du JuiceShop

Dans Powershell, exécutez la commande suivante :

docker pull bkimminich/juice-shop

Puis, pour démarrer le conteneur et l’application web :

run -d -p 3000:3000 bkimminich/juice-shop

Le site web est maintenant disponible sur :

<http://localhost:3000>

# Découvrir la page cachée du tableau des scores

La première étape consiste à découvrir la page cachée du tableau des scores, en anglais « score board ». Vous pouvez essayer de deviner l’url ou chercher une référence dans ce qui n’est pas normalement visible sur le site.

Quelle est le type de faille du top 10 ?

1…………………………………………………………………………………………………

# DOM XSS

Dans la page du tableau des scores, filtrer les challenges d’une étoile avec le mot clé « tutorial »

Résolvez le challenge DOM XSS

Quelle est le type de faille du top 10 ?

3…………………………………………………………………………………………………

Essayer le challenge Bonus Payload ?

Qu’en pensez-vous ?

C’est plutôt incroyable

# Confidential document

Dans la page du tableau des scores, filtrer les challenges d’une étoile avec le mot clé « tutorial »

Résolvez le challenge Confidential document

Quelle est le type de faille du top 10 ?

1…………………………………………………………………………………………………

# Error handling

Dans la page du tableau des scores, filtrer les challenges d’une étoile avec le mot clé « tutorial »

Résolvez le challenge Error Handling

Quelle est le type de faille du top 10 ?

5…………………………………………………………………………………………………

Quelles sont les informations que vous pouvez déduire de l’erreur ?

On peut savoir quel module vous utiliser…………………………………………….

# Login Admin

Dans la page du tableau des scores, filtrer les challenges de deux étoiles avec le mot clé « tutorial »

Résolvez le défi Login admin

Quelle est le type de faille du top 10 ?

3…………………………………………………………………………………………………

# Challenges bonus

**3 étoiles**

* View Basket
* Login Jim
* Login Bender