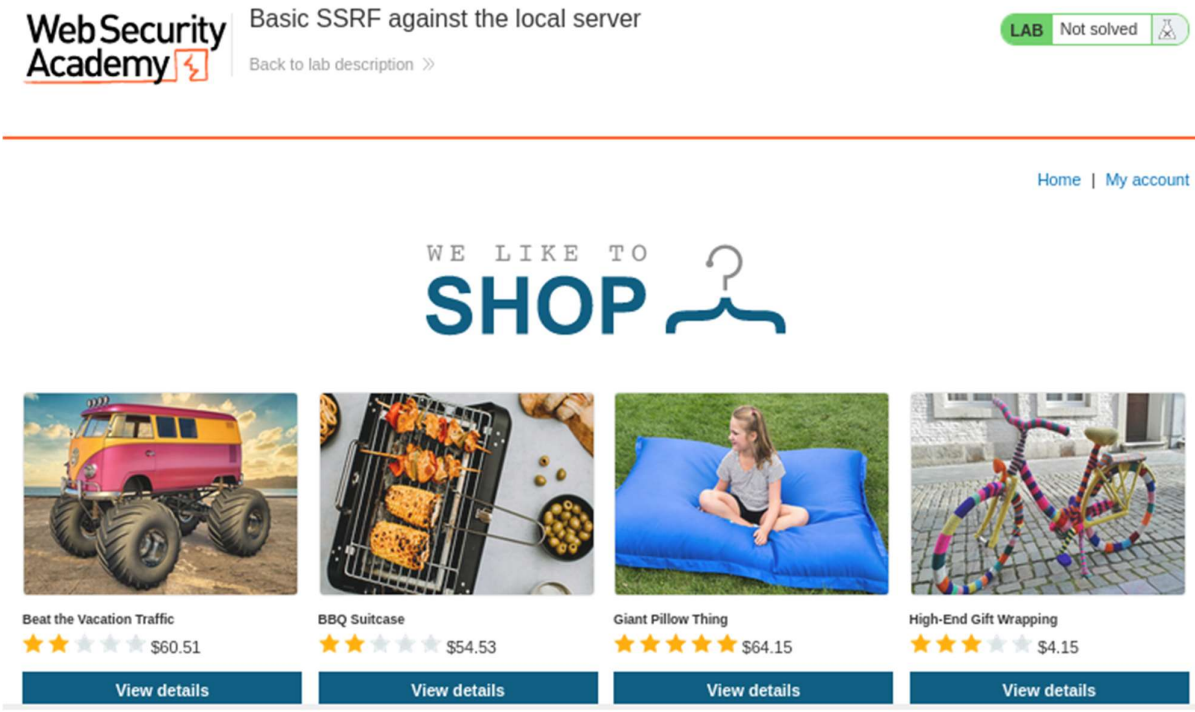
Défi n°1 : exploitation basique d'une vulnérabilité SSRF

Le lien permettant d'accéder au labo est le suivant :

https://portswigger.net/web-security/ssrf/lab-basic-ssrf-against-localhost

Ce défi permet d'accéder à une page qui affiche la quantité en stock de chaque produit.



Travail à faire :

Travaux préparatoires

Q1. Accéder à la page d'accueil du défi puis sélectionner un produit et afficher la quantité en stock d'un produit en cliquant sur le lien *check stock*.

Q2. Recommencer la manipulation précédente en activant le proxy BurpSuite (intercept ON), cliquer sur Forward plusieurs fois jusqu'à l'affichage du paramètre stockApi. Ensuite, envoyer la page obtenue vers le répéteur de BurpSuite. Revenir ensuite à l'onglet proxy.

Q3. Sélectionner avec la souris l'URL contenant le paramètre stockApi puis le décoder à l'aide de l'outil d'inspection de BurpSuite afin d'afficher cet URL en clair.

Q4. Conclure sur le procédé utilisé pour afficher la quantité en stock.

Q5. Récupérer l'URL décodé et tenter d'accéder au contenu associé en le copiant/collant dans le navigateur. Que remarquez-vous, pourquoi ? Vous pouvez mettre le proxy à OFF pour faire cette tentative d'accès.

Découverte de la vulnérabilité SSRF

Q6. Remettre le proxy à ON puis se rendre dans l'onglet répéteur contenant la requête envoyée précédemment sur le stock. Remplacer l'URL associé à la variable stockApi par les contenus suivants puis envoyer l'URL modifié (send) :

http://localhost
http://localhost/admin

Réalisation du défi

L'objectif du défi est de supprimer l'utilisateur Carlos ce qui nécessite normalement des droits d'administration.

Q7. Envoyer au serveur l'URL *localhost/admin* puis chercher dans le code de réponse du serveur le mot clé « Carlos ». En déduire l'URL complet permettant de supprimer l'utilisateur Carlos.

Q8. Vérifier que l'utilisateur Carlos est bien supprimé en testant à nouveau l'URL suivant dans le répéteur :

http://localhost/admin

Une fois la réponse obtenue, cliquer sur l'onglet Render afin de vérifier que l'utilisateur Carlos n'est plus présent.