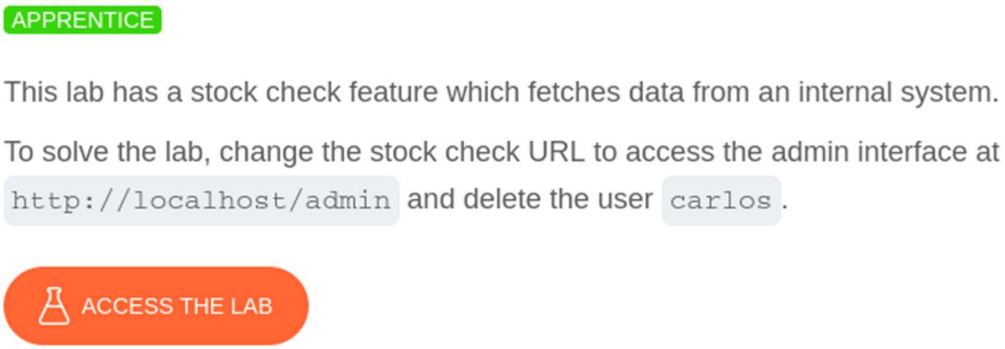
Défi n°1 : Exploitation basique d'une vulnérabilité SSRF

Ouvrir le lien suivant :

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

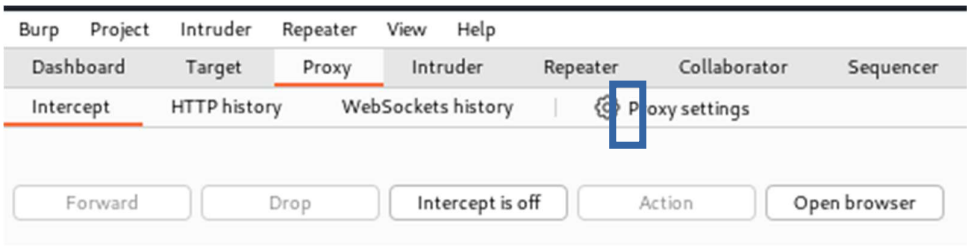


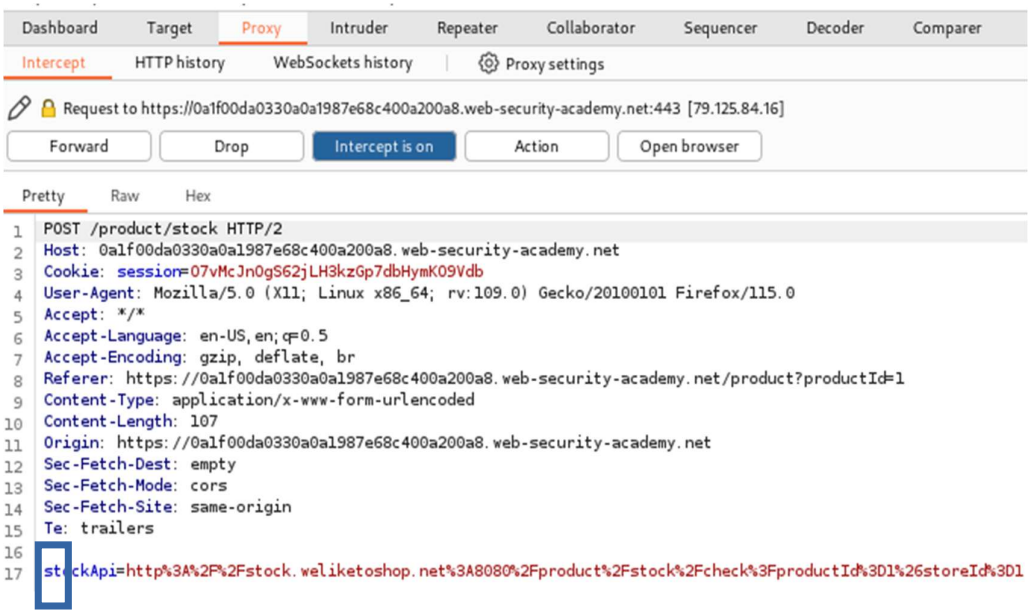
Cliquer sur le bouton ACCESS THE LAB

Travaux préparatoires :

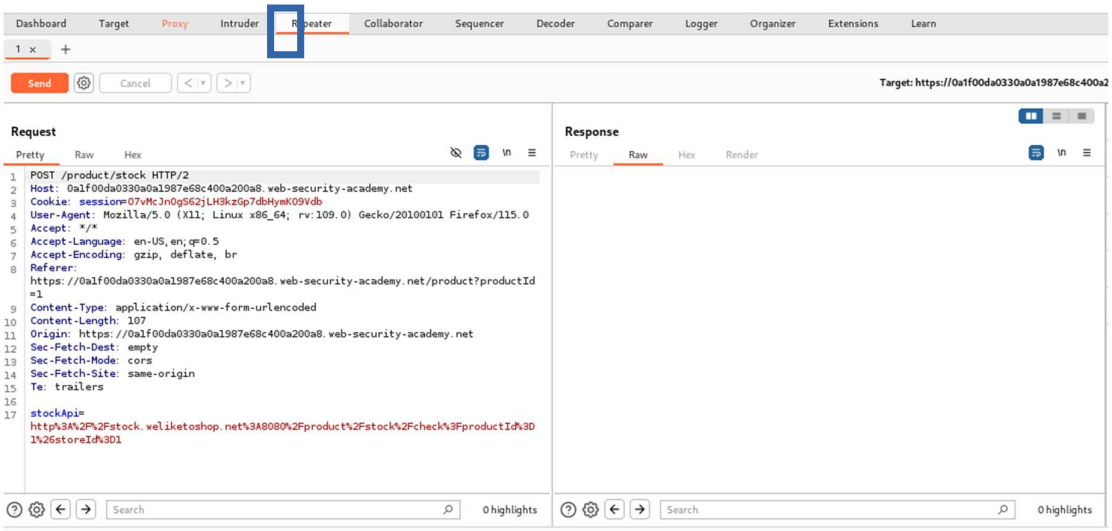
Affichage de la quantité en stock d'un produit.

Capture de la requête et envoi vers le répéteur.

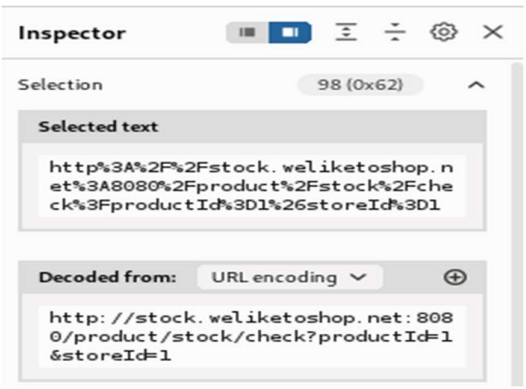




Avec le menu contextuel, on peut envoyer cette page vers le répéteur.

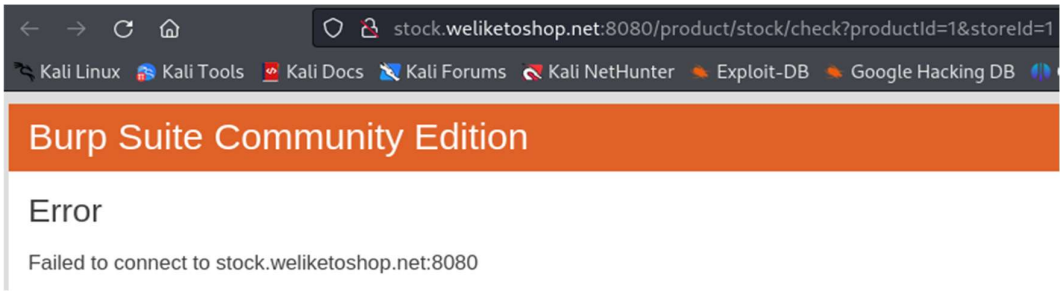


La sélection de l'URL avec la souris affiche l'outil d'inspection.



L'affichage de la quantité en stock fait appel, via une URL, à une ressource située sur un serveur local qui écoute sur le port 8080.

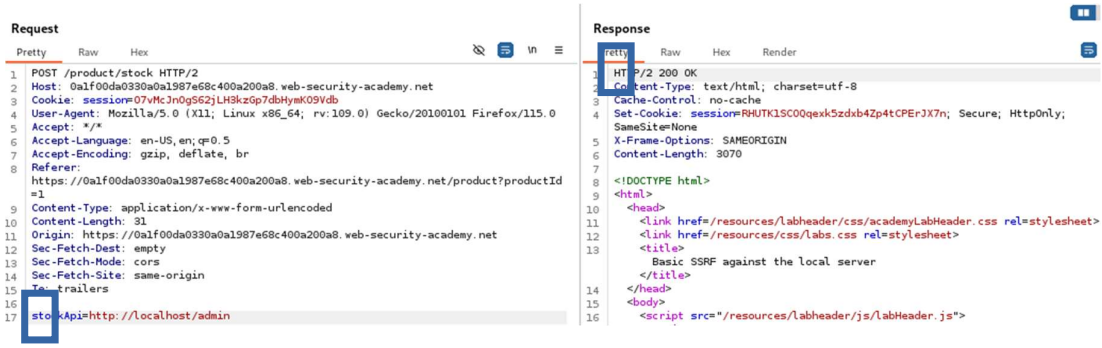
Le contenu associé à l'URL décodé n'est pas accessible directement de l'extérieur ce qui est normal car on peut supposer que la politique de filtrage l'interdise. Cette ressource interne ne devrait être accessible que depuis le serveur web qui l'appelle.



Découverte de la vulnérabilité SSRF :

L'accès donne la réponse de code 200 du serveur ce qui correspond à un succès. Le serveur autorise la manipulation de cet URL. L'URL n'étant pas vérifié il peut donc être modifié ce qui constitue un vulnérabilité SSRF. Il faut utiliser l'outil d'inspection pour modifier l'URL.

Avec localhost/admin, cela donne :

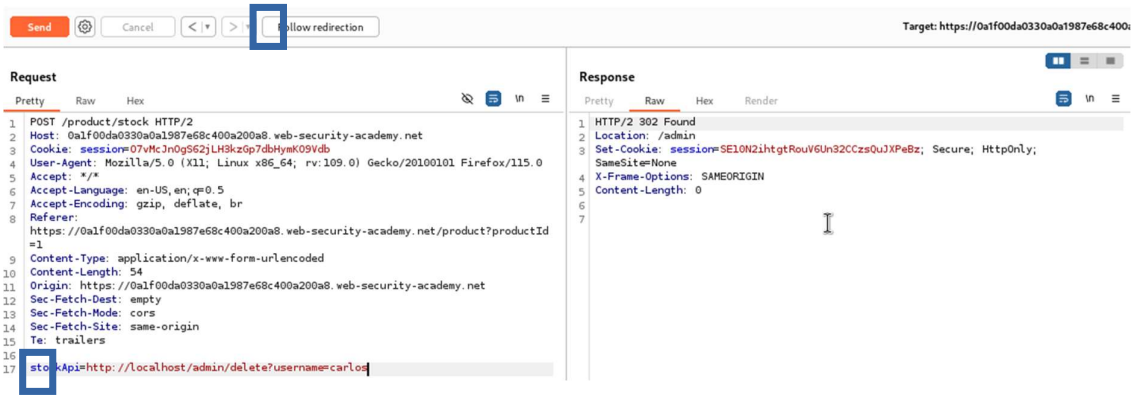


Réalisation du défi :

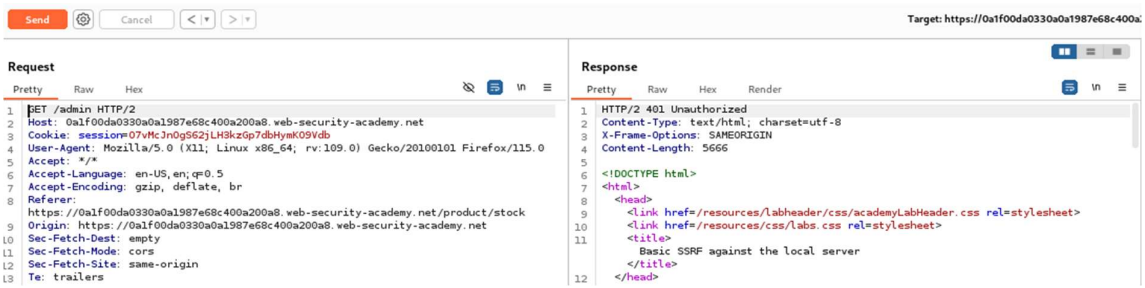
L'URL complet est visible en fouillant dans le code obtenu:

http://localhost/admin/delete?username=carlos

Envoi de l'ordre de suppression de l'utilisateur Carlos :



Suivre la redirection en cliquant Follow redirection. Une erreur 401 s'affiche mais l'utilisateur a bien été supprimé.



On peut utiliser l'onglet Render afin de le constater.