Documentation : SSRF Labs (burp suite)

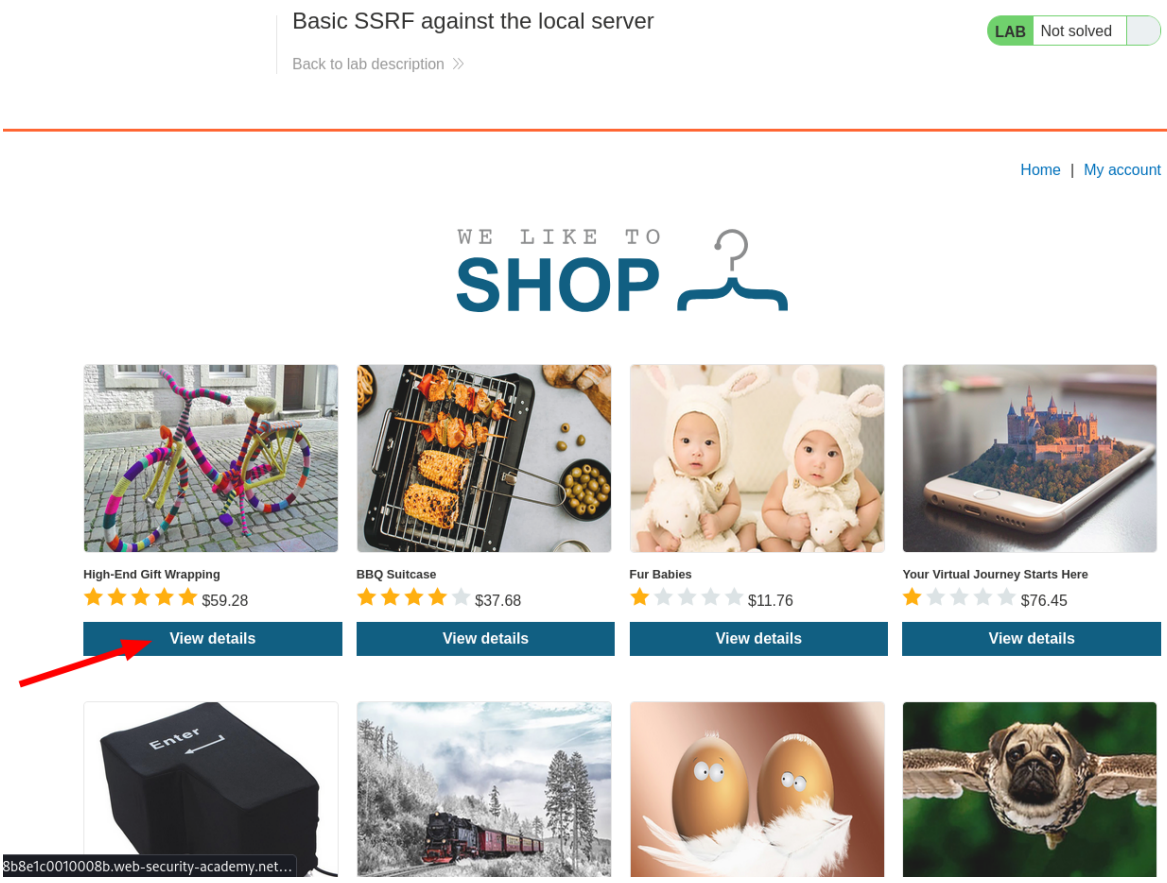
SSRF : Server-side Request Forgery

prepared by : Qasim Ali

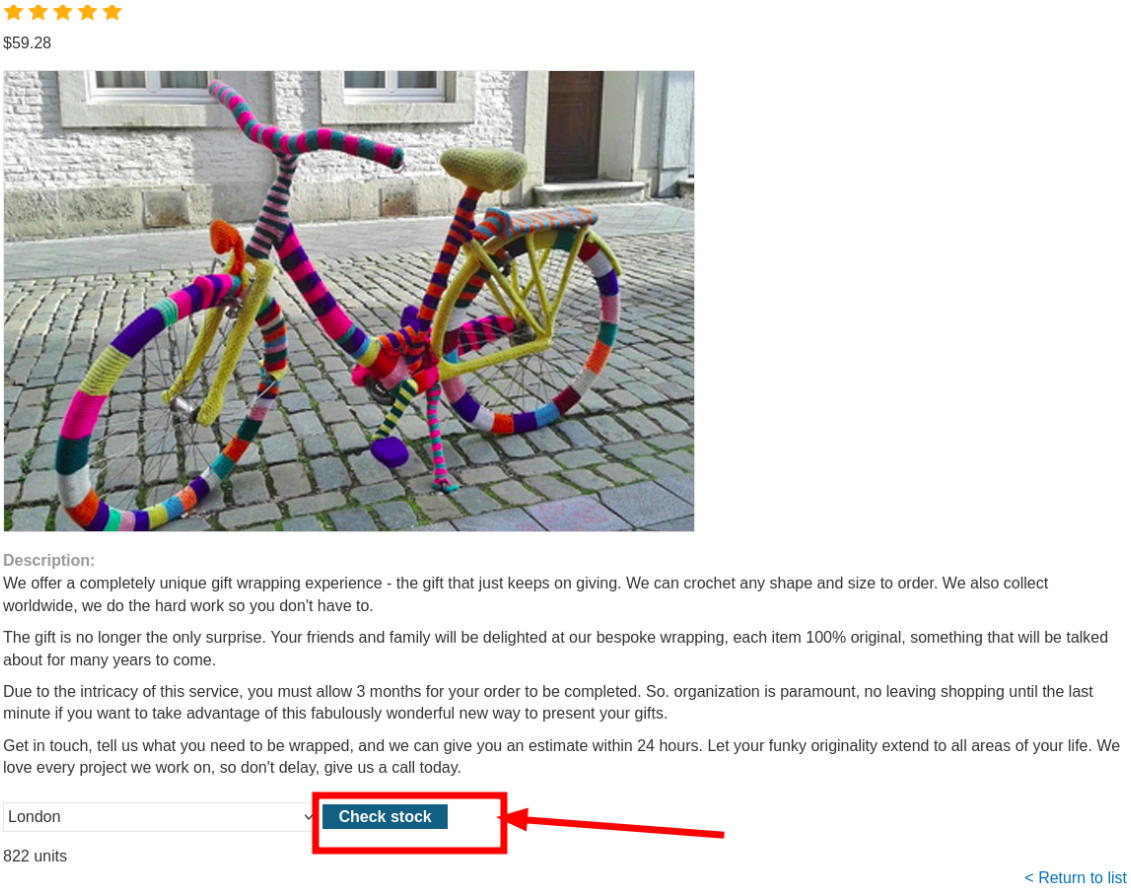
Lab: Basic SSRF against the local server

navigate home page

click on the Detail option of product



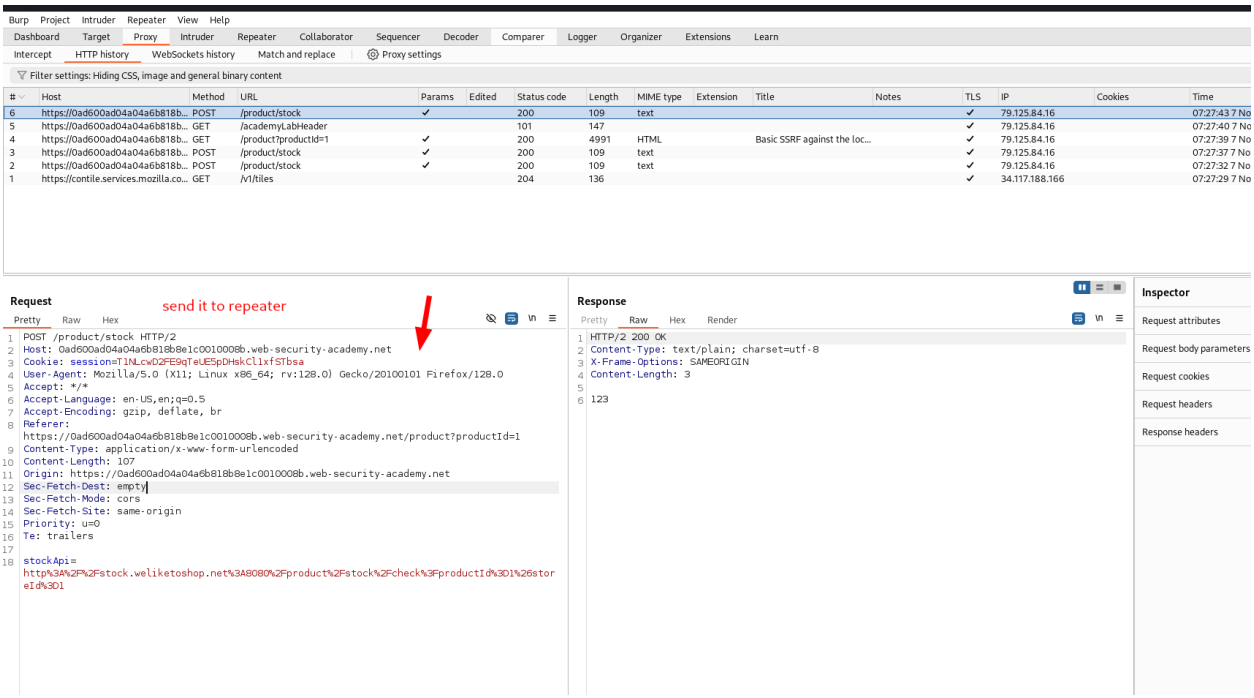
click on Stock option and check stock



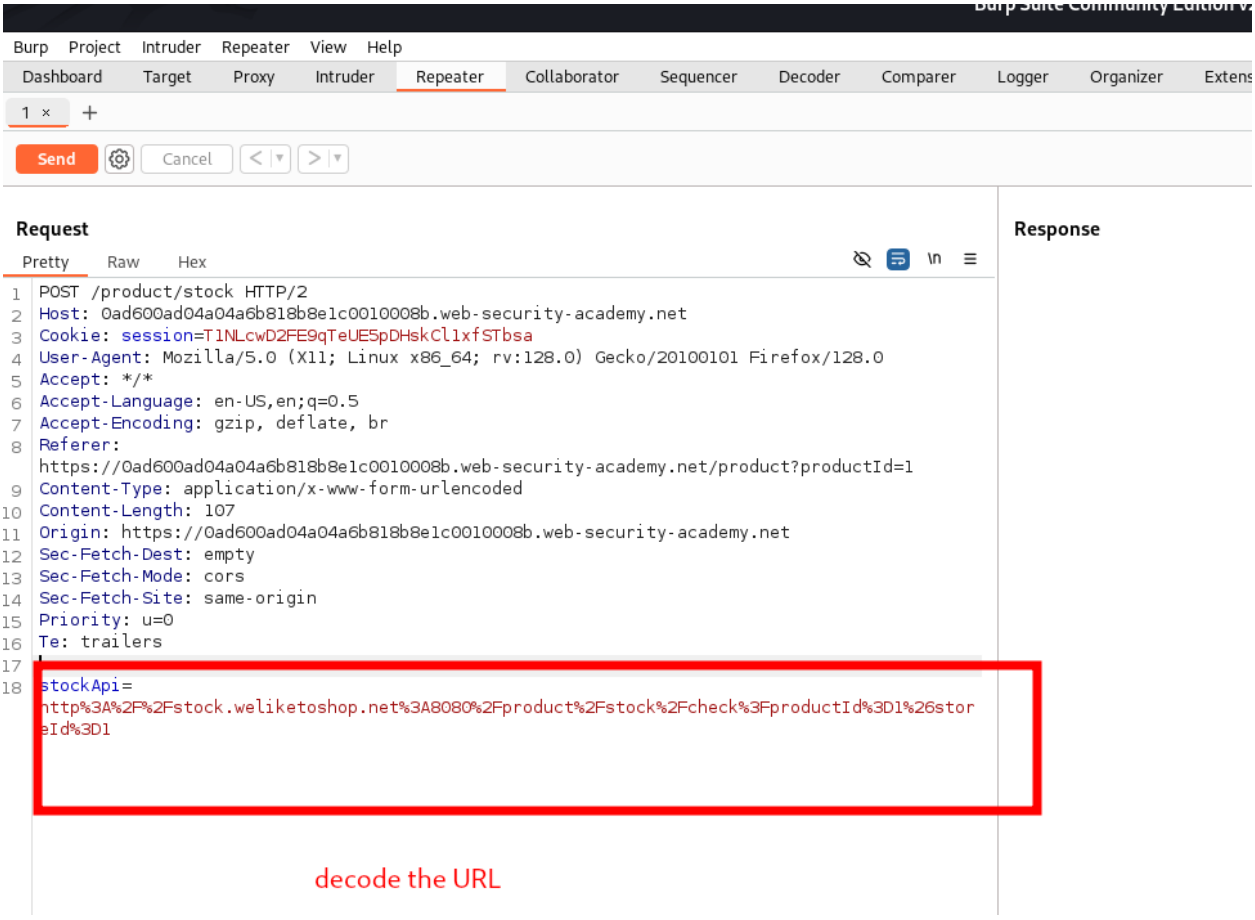
go to burp suite intercept the request in Proxy Tab (HTTP history)

note the request and right click on it and chose option

send it to Repeater

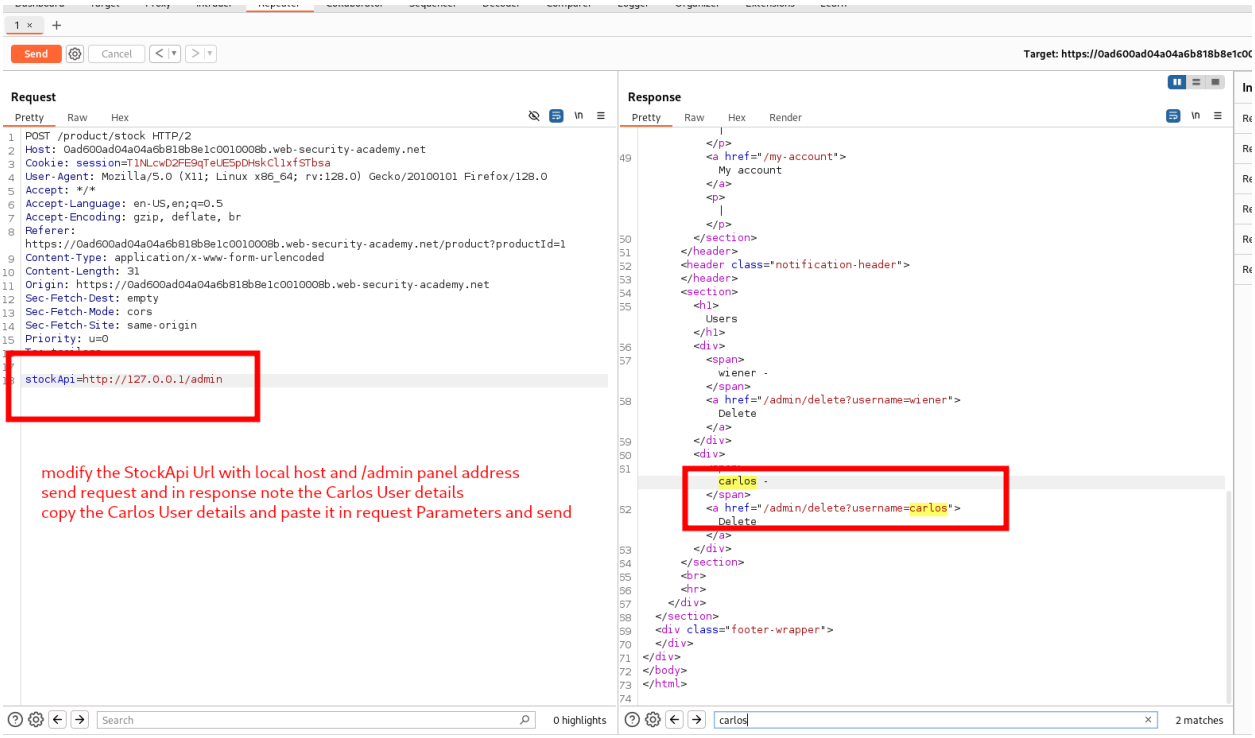


in Repeater , go to Request section and note the Request body parameters it contain StockApi URL . decode the url .



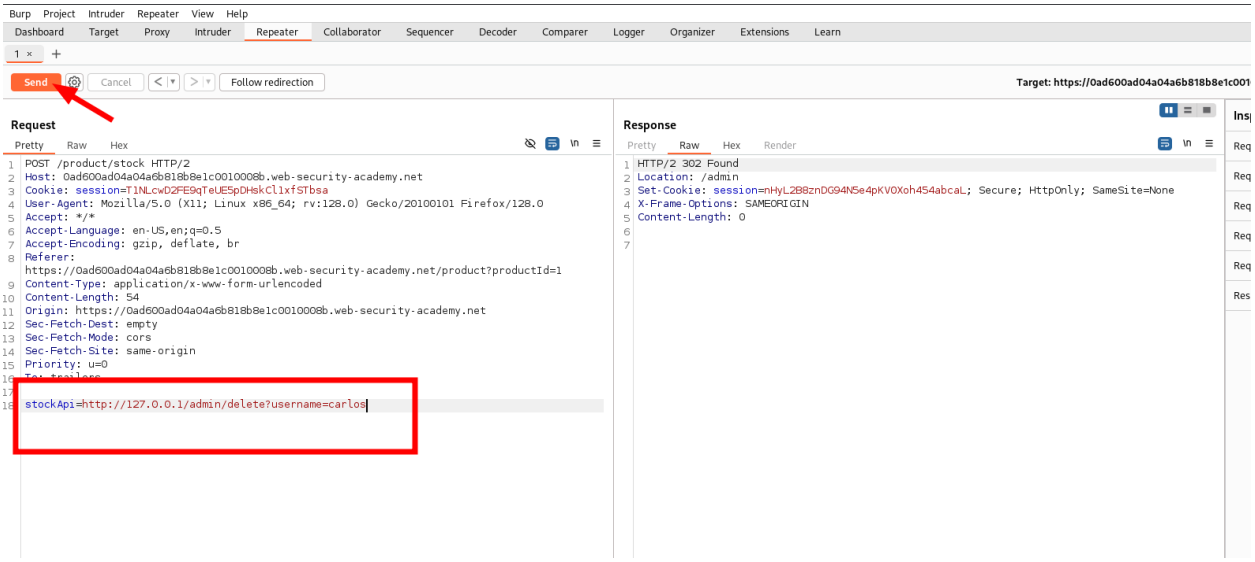
modify the StockApi URL with Local host and /admin panel address

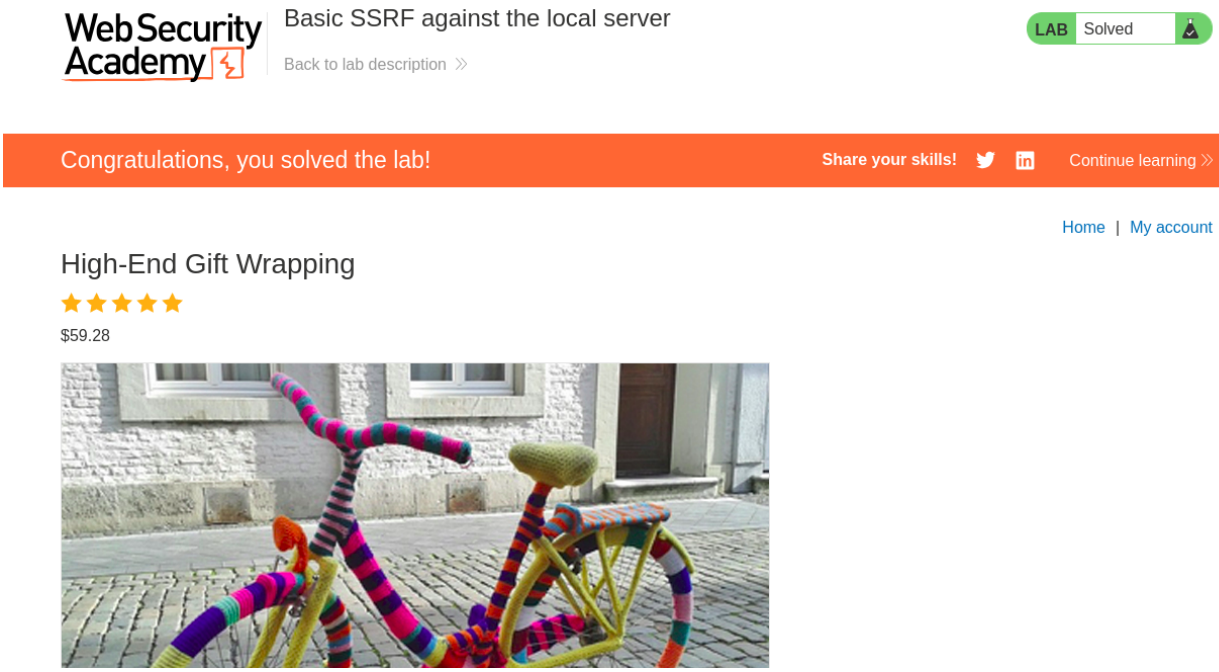
send request and in response note the Carlos user Details



copy the Carlos User details and paste it in request Parameters and send

Carlos user Deleted and Lab solved





Lab: Basic SSRF against another back-end system

navigate home page

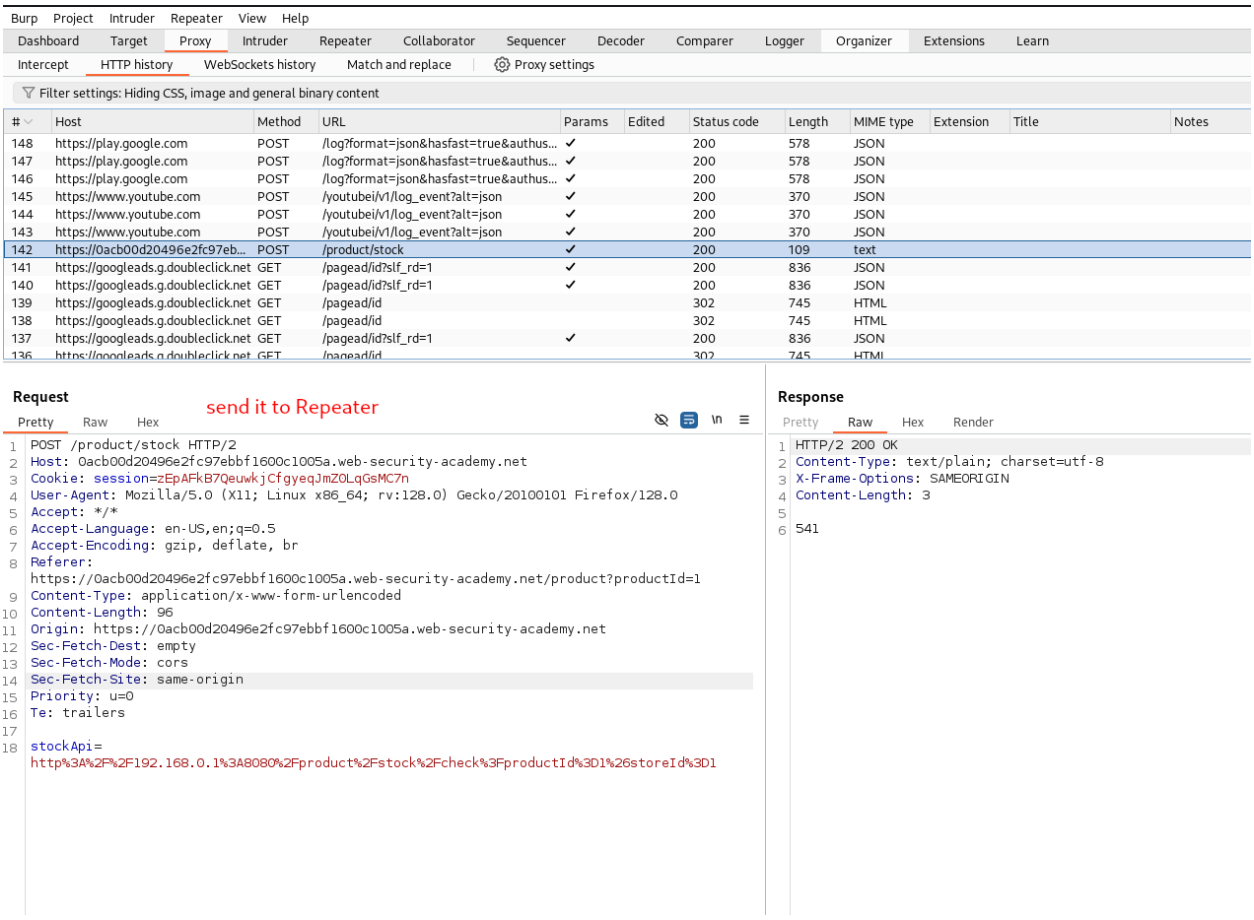
click on the Detail option of product

click on Stock option and check stock

go to burp suite intercept the request in Proxy Tab (HTTP history)

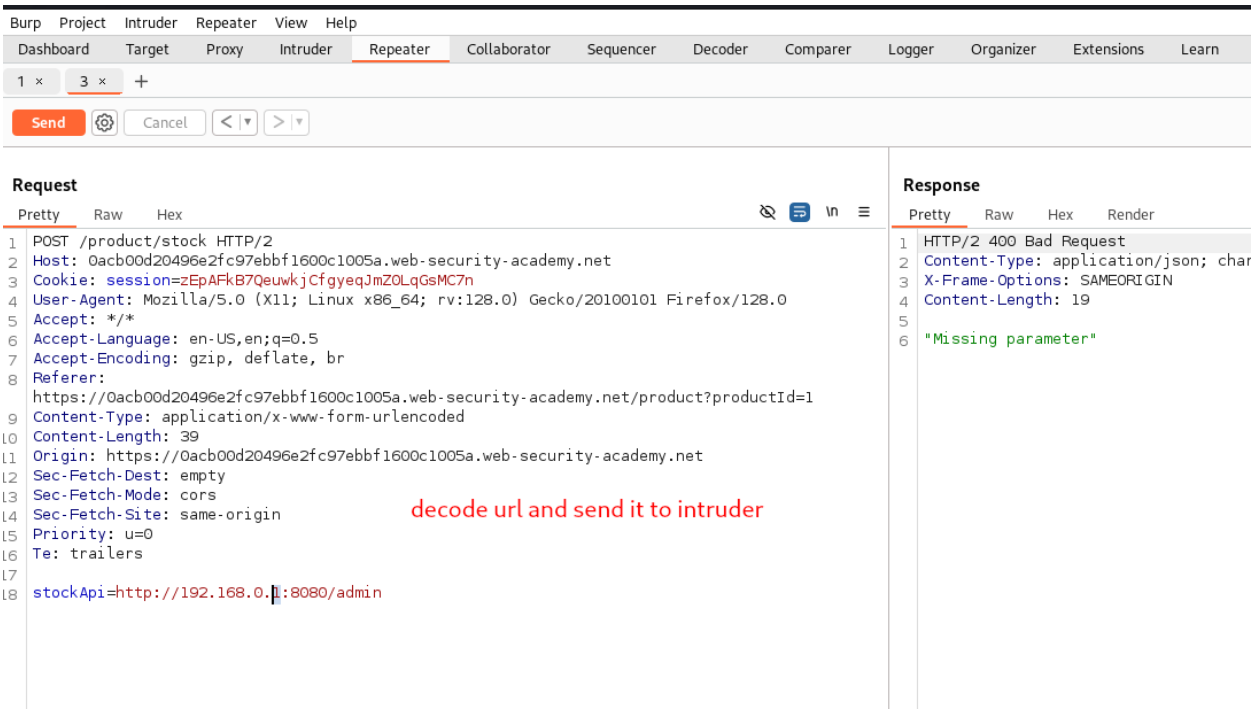
note the request and right click on it and chose option

send it to Repeater



in Repeater , go to Request Section and decode the StockApi URL

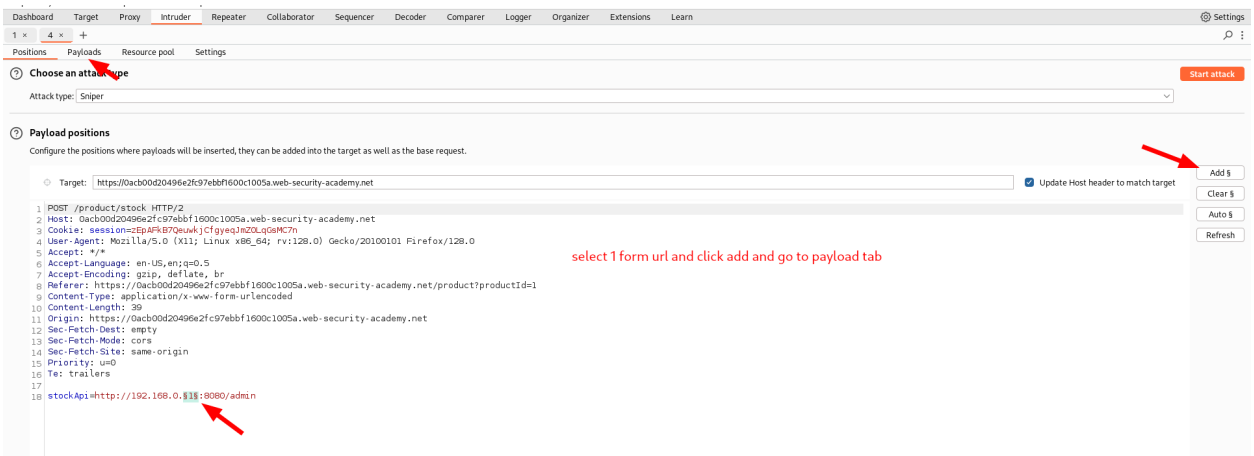
send the request with modified request body parameters by adding /admin address



send it to Intruder

in Intruder , (sub-tab) position go to StockApi and select last octet of http address

click on Add

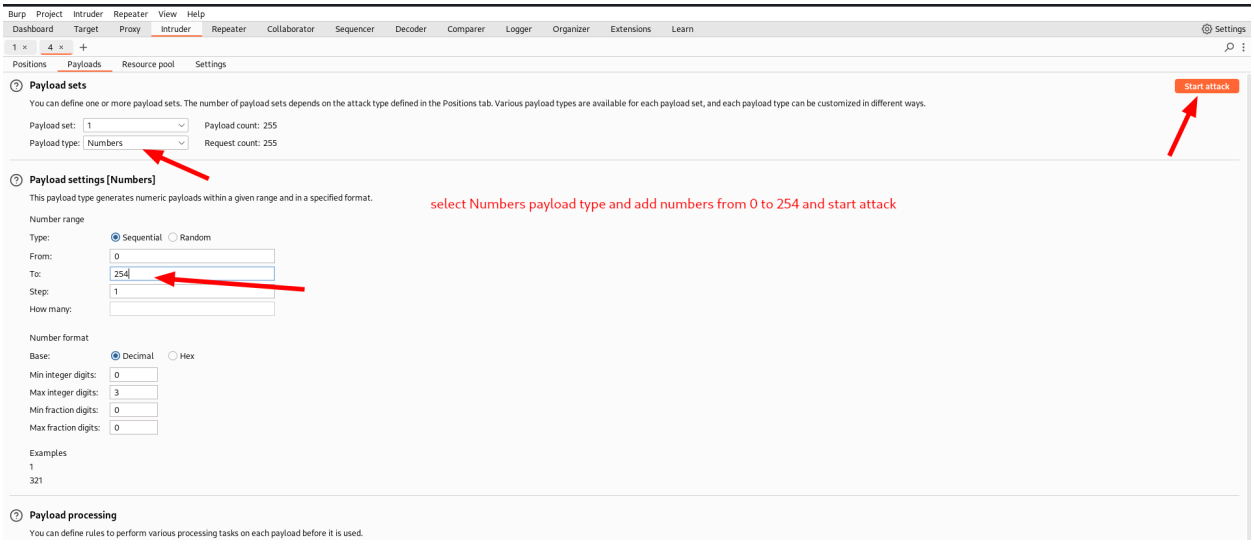


go to payload (sub-tab)

in Payloads , select Payload type = Numbers

in Payload setting , add numbers from 0 to 254

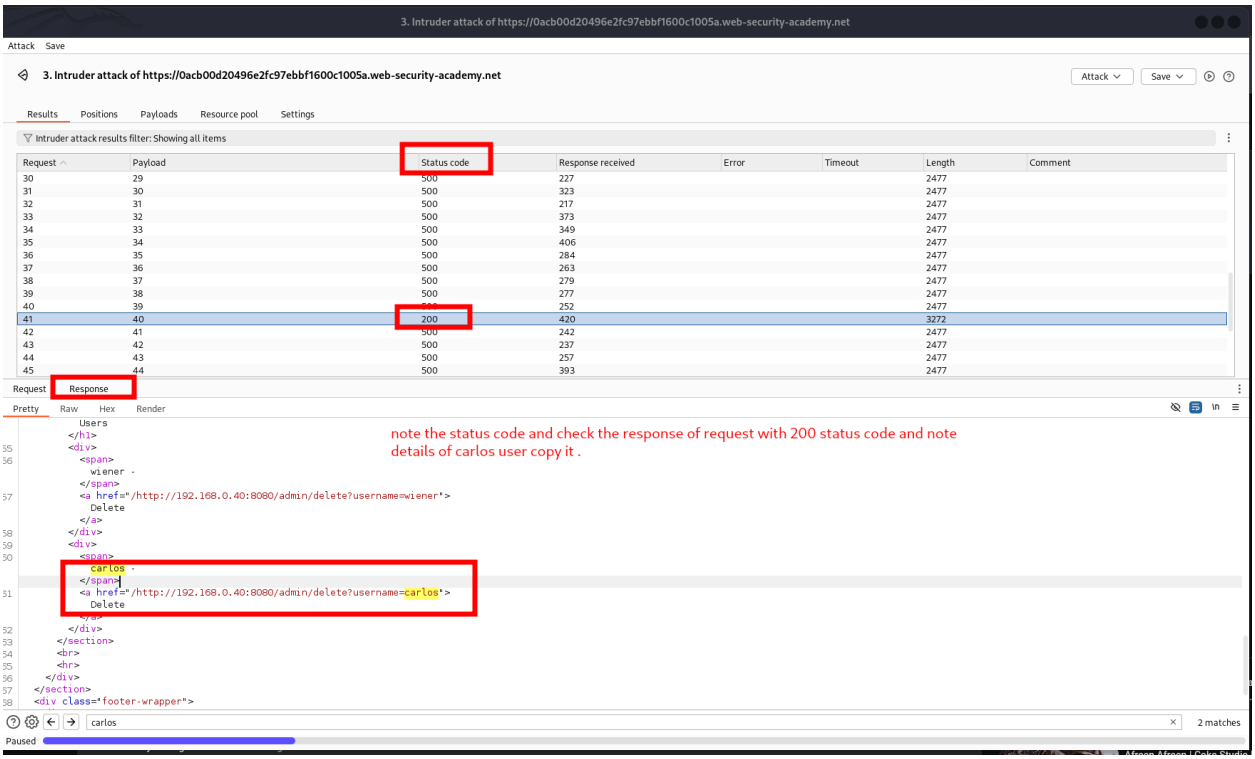
Start attack



in Attack window , note Status code of requests and veiw their response

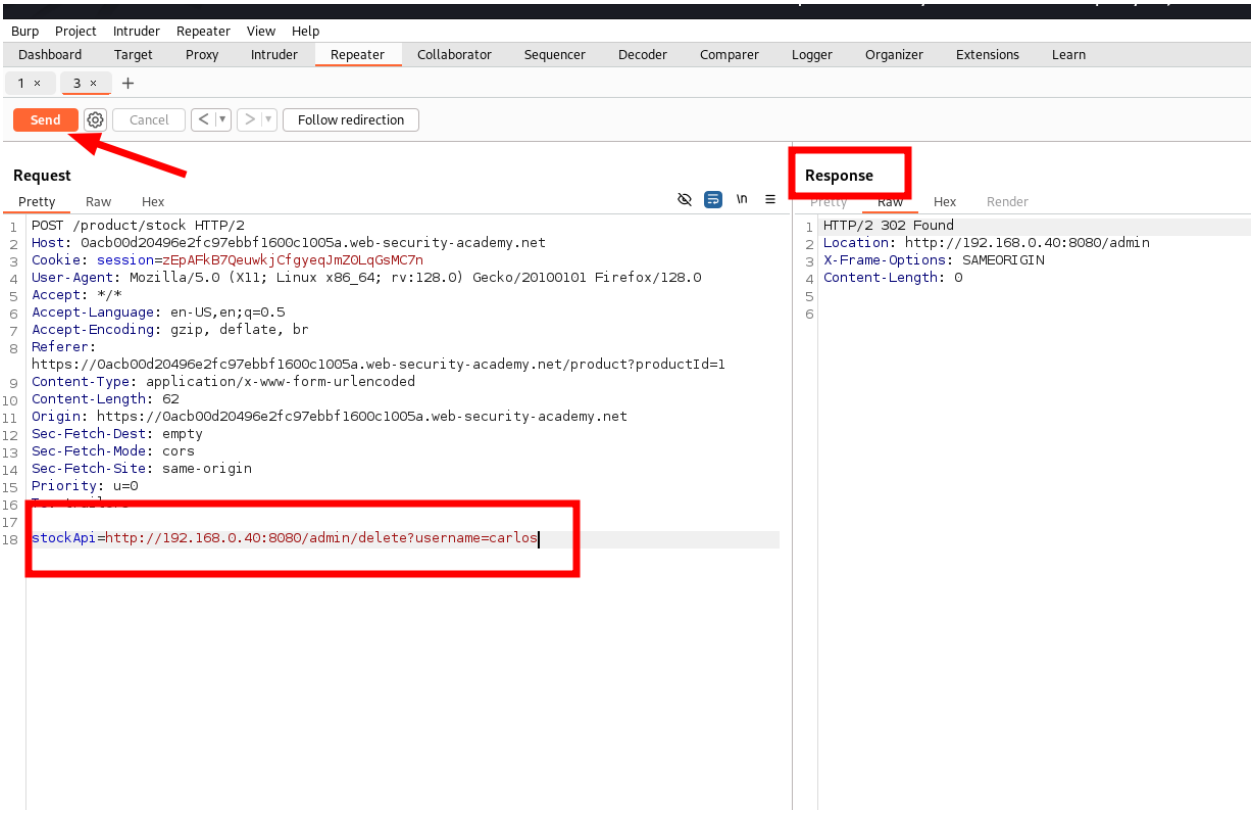
click on the Status code with 200 and veiw its response

note the Carlos user Details and copy them

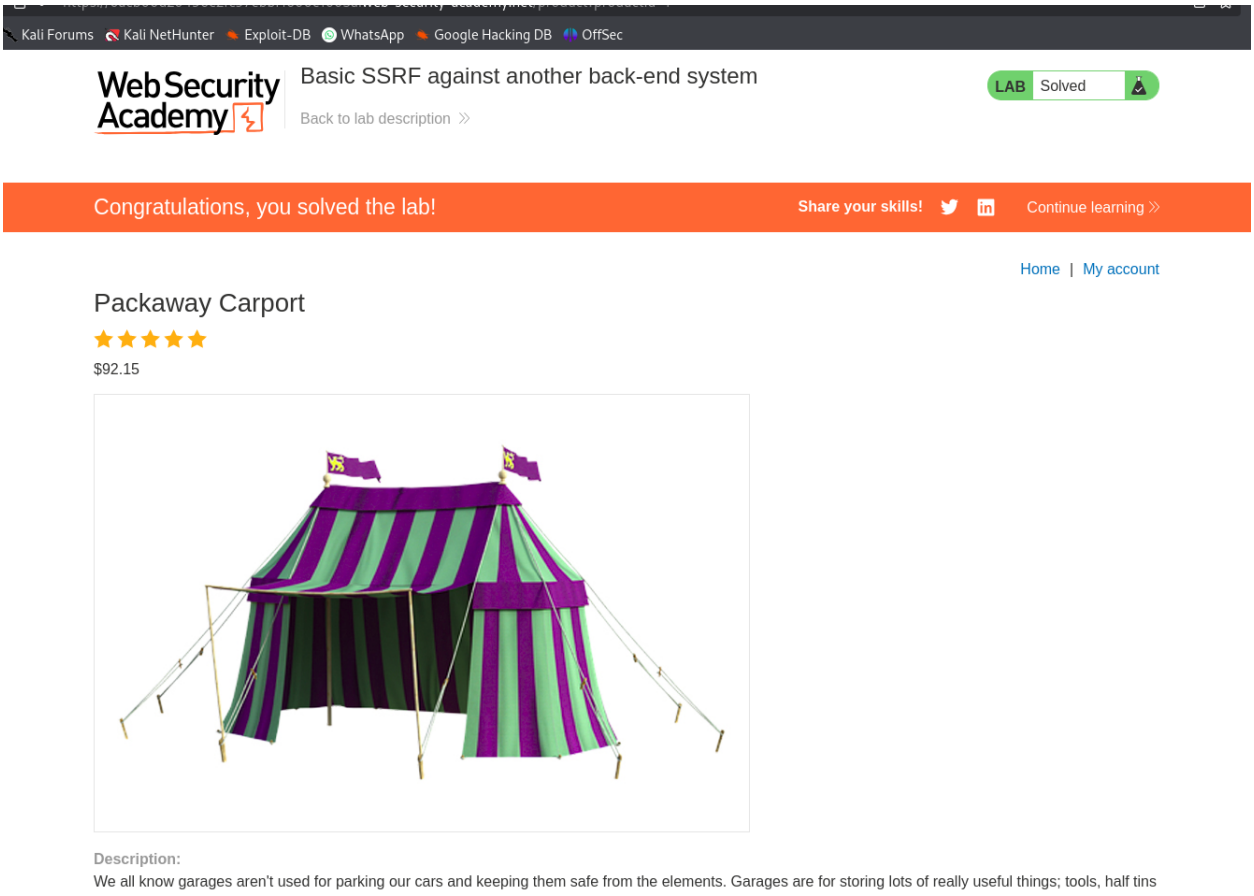


go back to Repeater and paste Carlos User Details in the StockApi URL

and send request



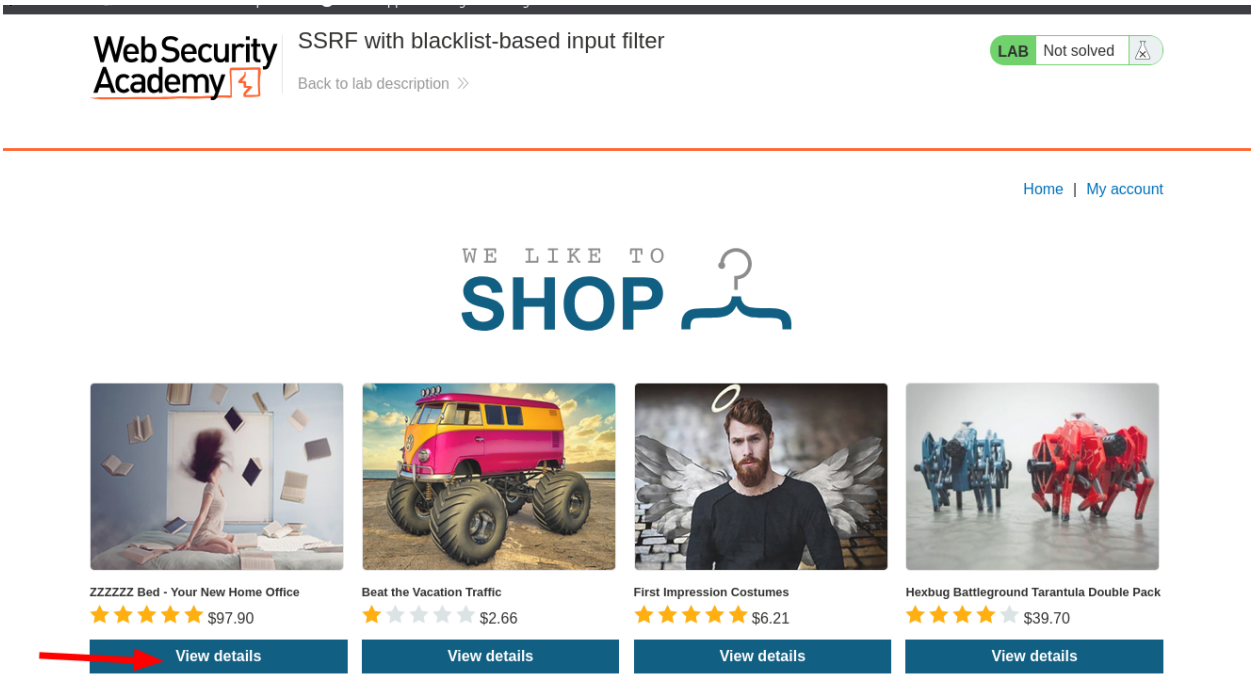
it Delete Carlos User and Lab Solved ..



Lab: SSRF with blacklist-based input filter

navigate home page

click on the Detail option of product

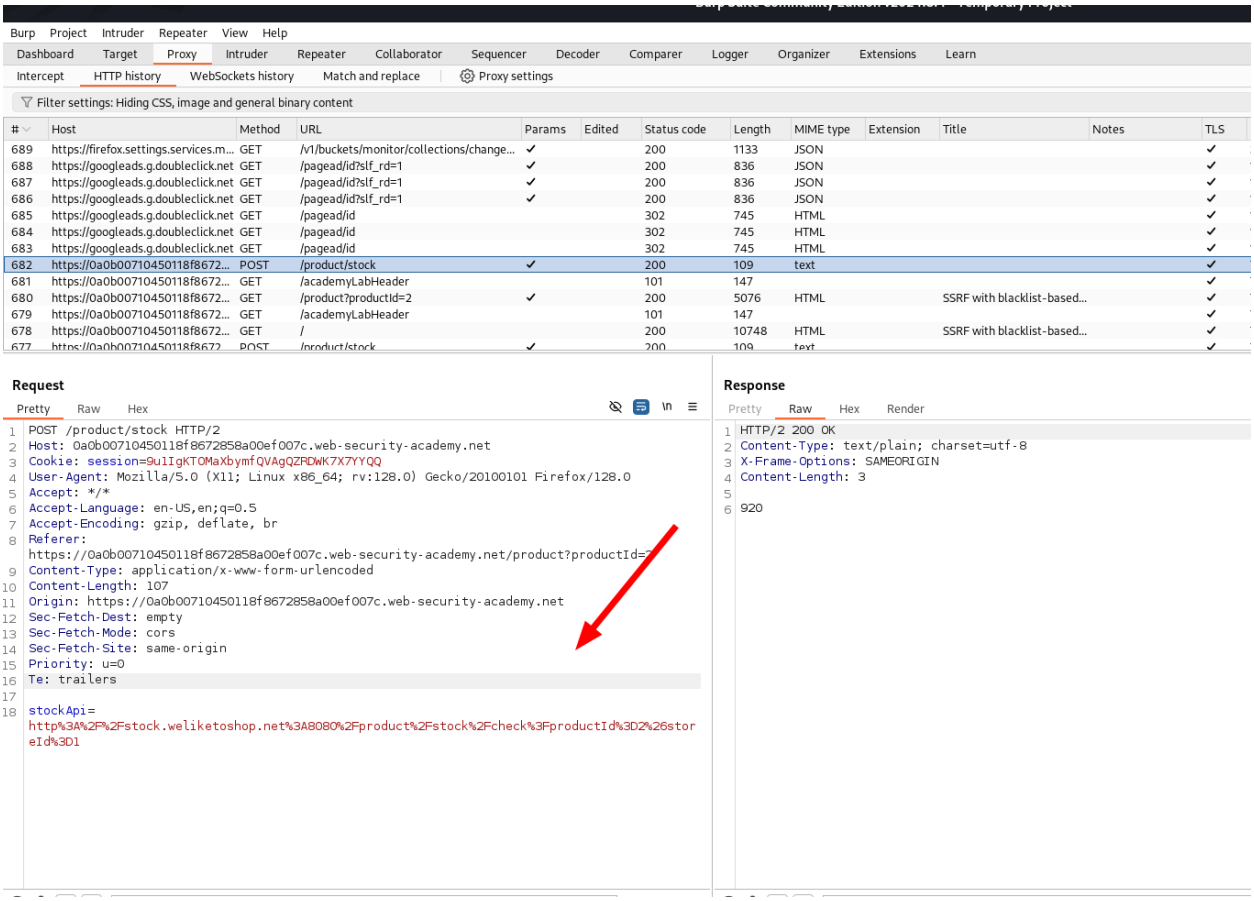


click on Stock option and check stock

go to burp suite intercept the request in Proxy Tab (HTTP history)

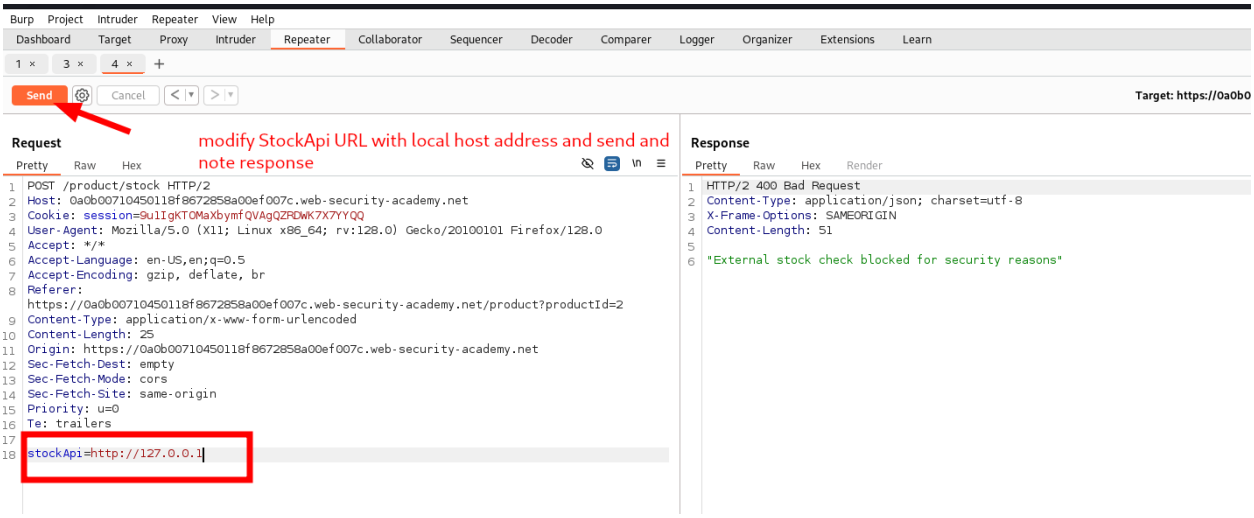
note the request and right click on it and chose option

send it to Repeater

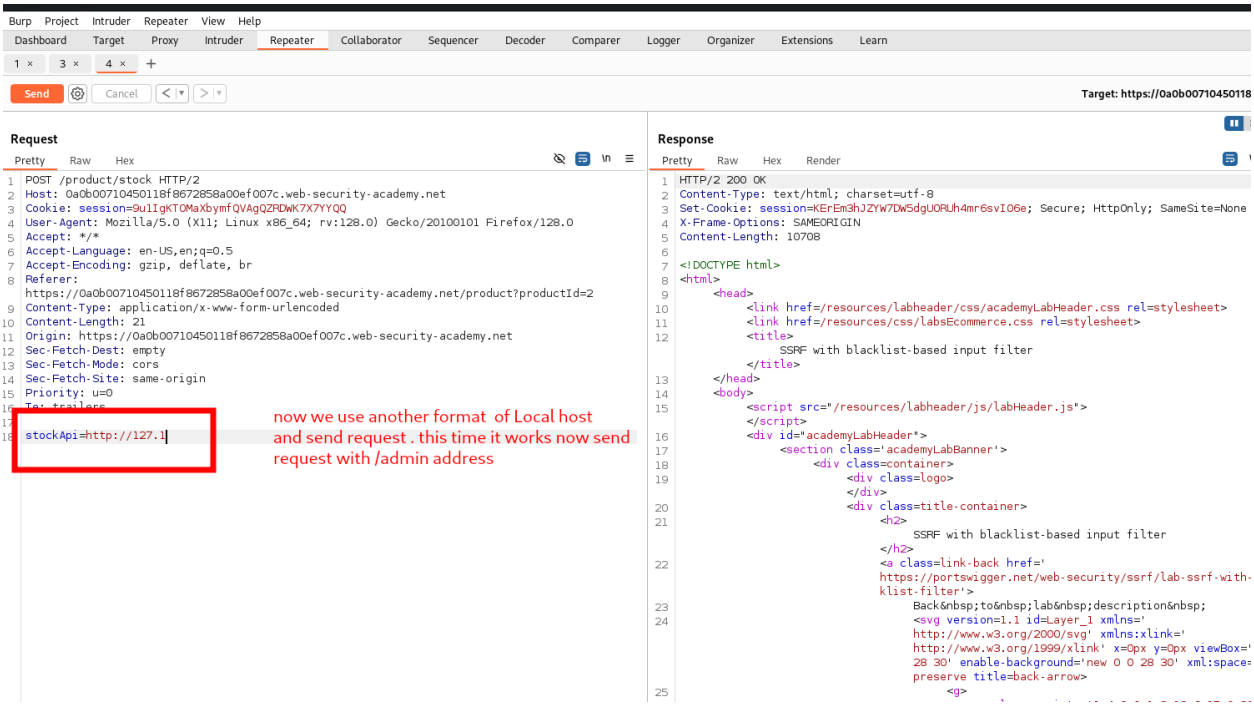


in Repeater , go to Request section and Modify the StockAPi with Local host address

and send it , note Response



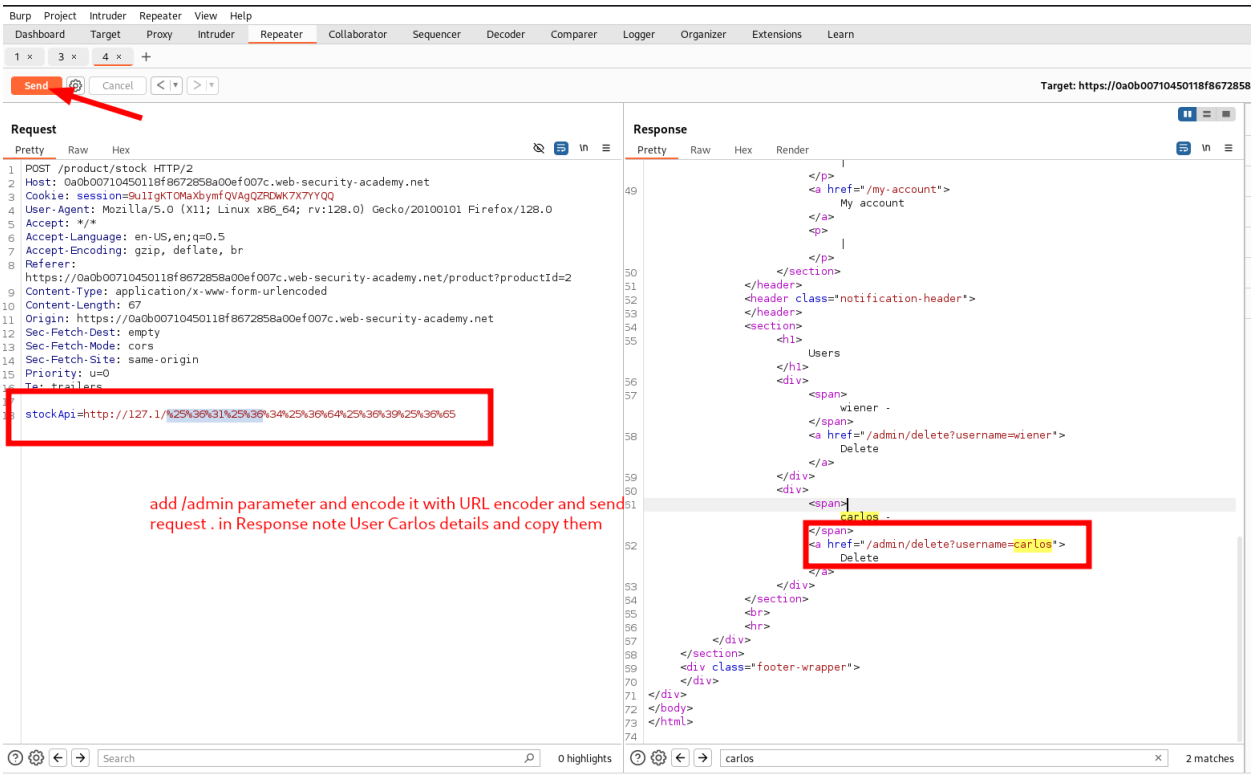
now Use another Format of Local host address and send request



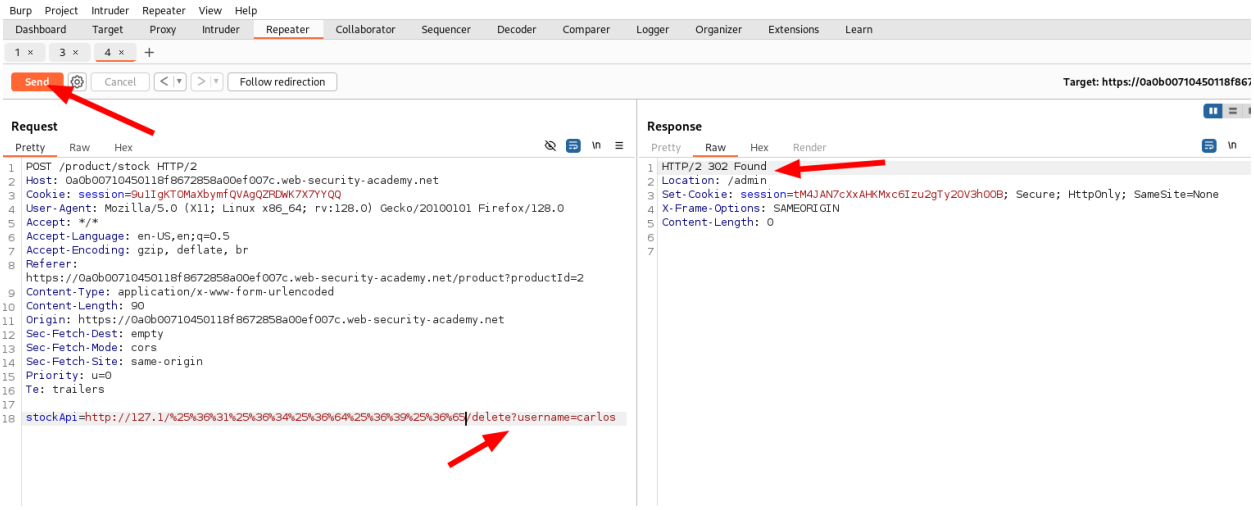
this time it works now send by adding /admin address

encode /admin parameters with URL encoder and send it

in Response ,note Carlos User Details and copy them



paste the Carlos user account Delete details in Url and send request



Carlos Delete and Lab Solved

Web Security Academy

SSRF with blacklist-based input filter

Back to lab description

LAB Solved

Congratulations, you solved the lab!

Share your skills!

Continue learning

Home | My account

Beat the Vacation Traffic

$2.66