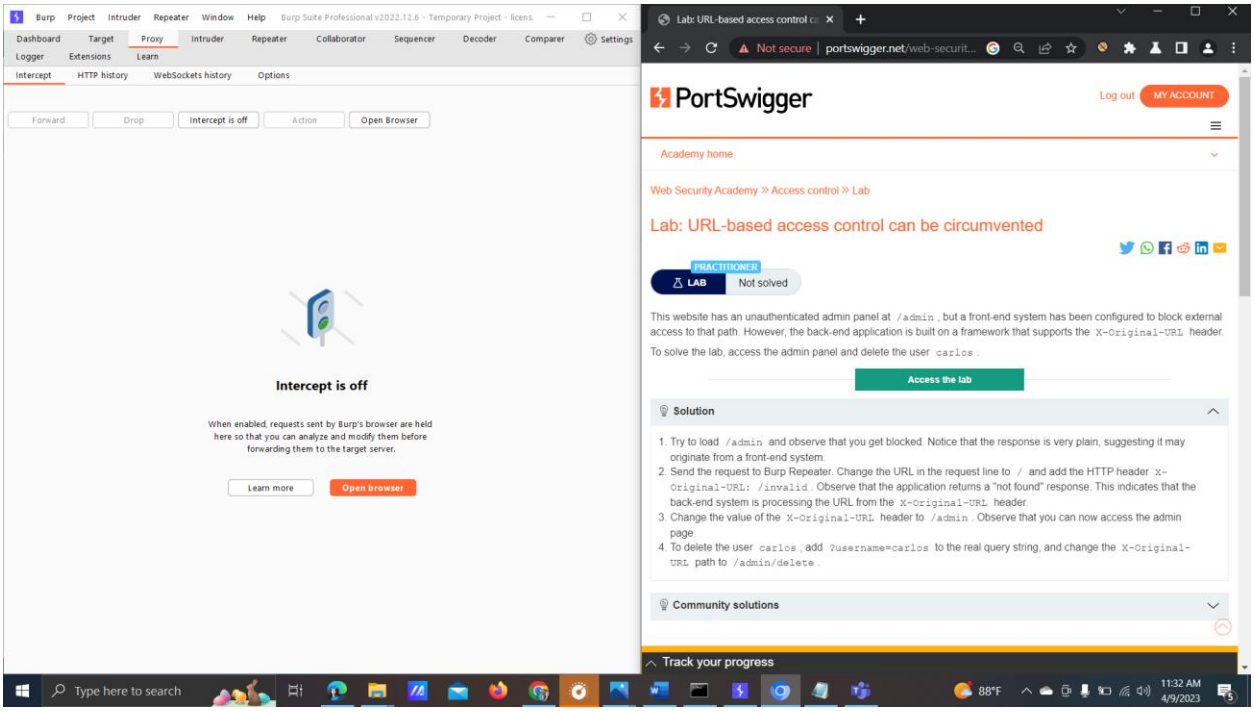
Port Swigger – Access control vulnerabilities and privilege escalation

Lab 10: URL-based access control can be circumvented



The unauthenticated admin panel for this website is located at /admin, but a front-end mechanism has been set up to prevent outside access to that path. However, the X-Original-URL header is supported by the framework on which the back-end application is constructed.

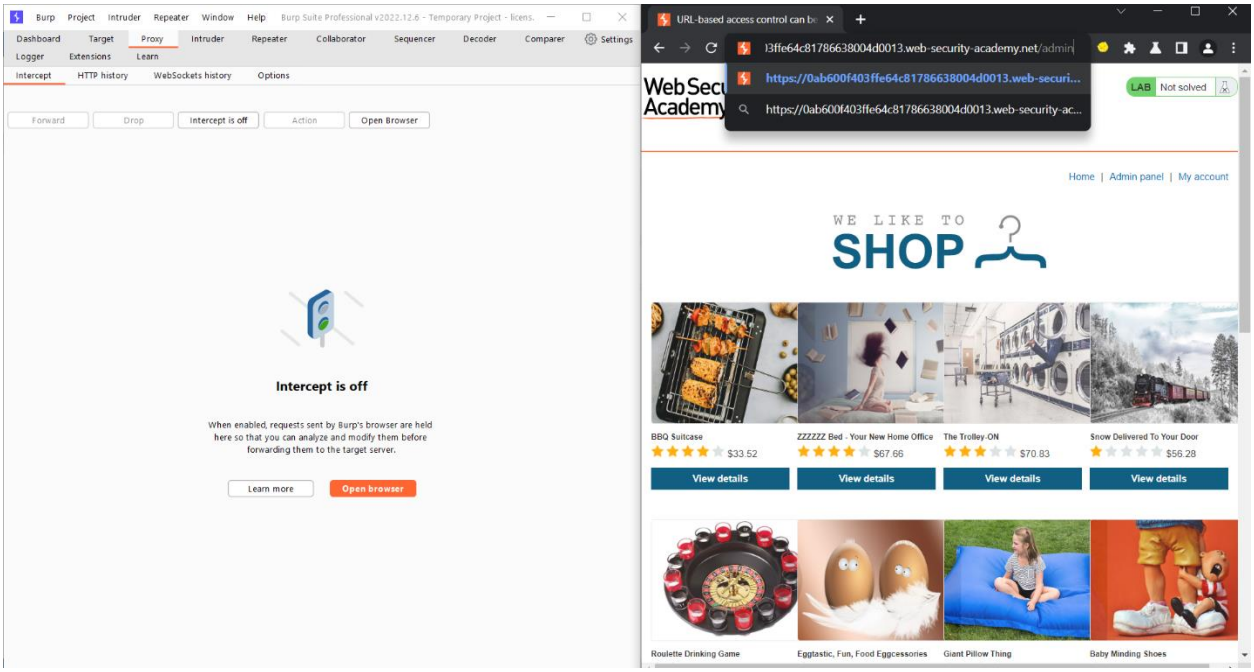
Access the admin panel and remove the user Carlos to finish the lab.

✓ How to solve this lab ?

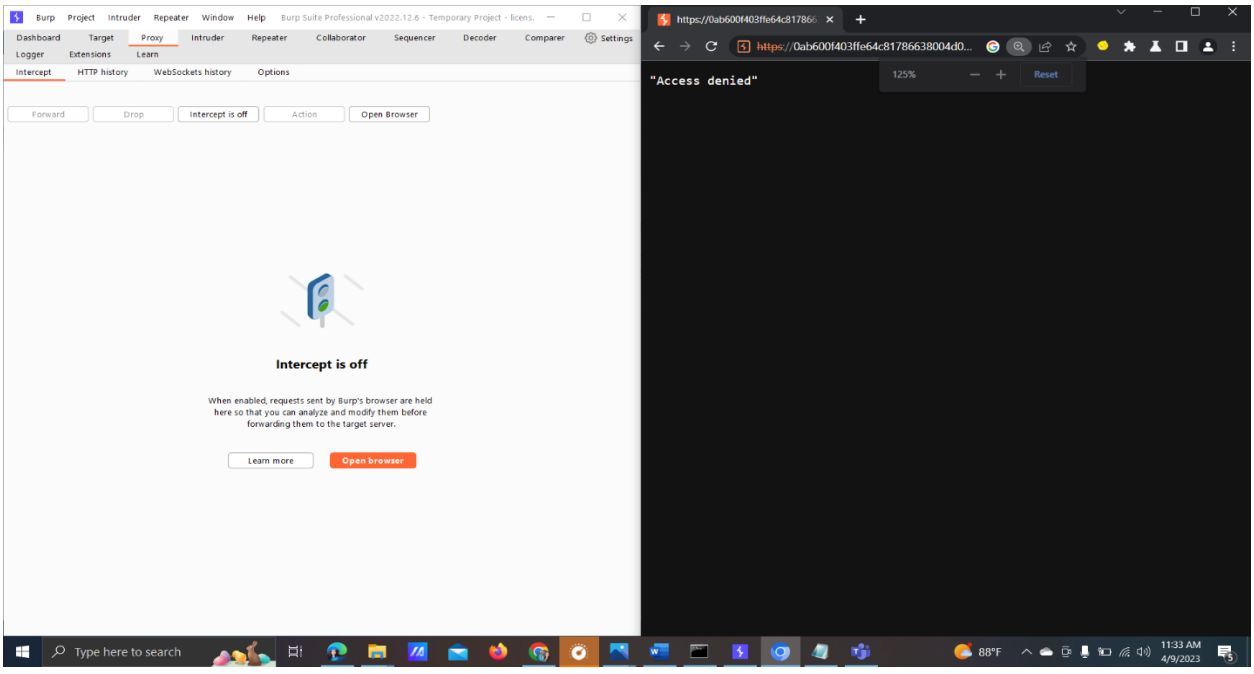
1. Try to load /admin and observe that you get blocked. Notice that the response is very plain, suggesting it may originate from a front-end system.
2. Send the request to Burp Repeater. Change the URL in the request line to / and add the HTTP header X-Original-URL: /invalid. Observe that the application returns a "not found" response. This indicates that the back-end system is processing the URL from the X-Original-URL header.
3. Change the value of the X-Original-URL header to /admin. Observe that you can now access the admin page.
4. To delete the user carlos, add ?username=carlos to the real query string, and change the X-Original-URL path to /admin/delete.

Port Swigger – Access control vulnerabilities and privilege escalation

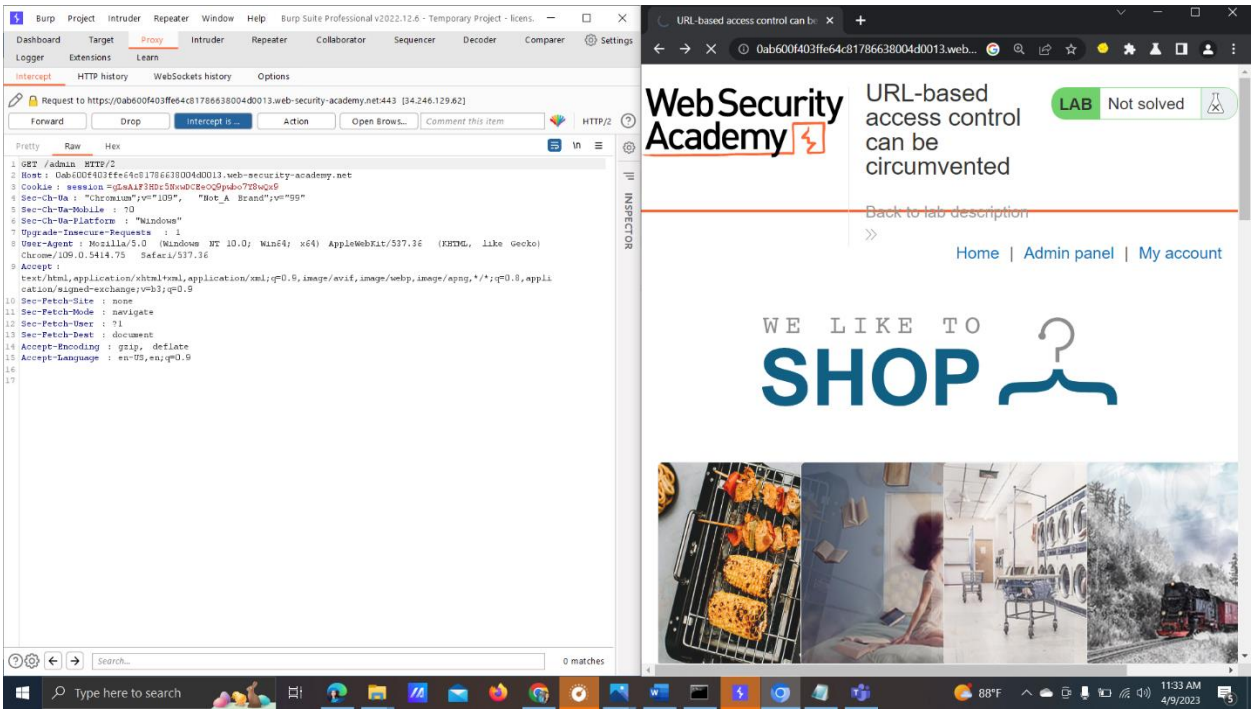
First click the "Access the lab" button and Turn on "Use proxy Burp suite for all URLs" and you can see this appearance.



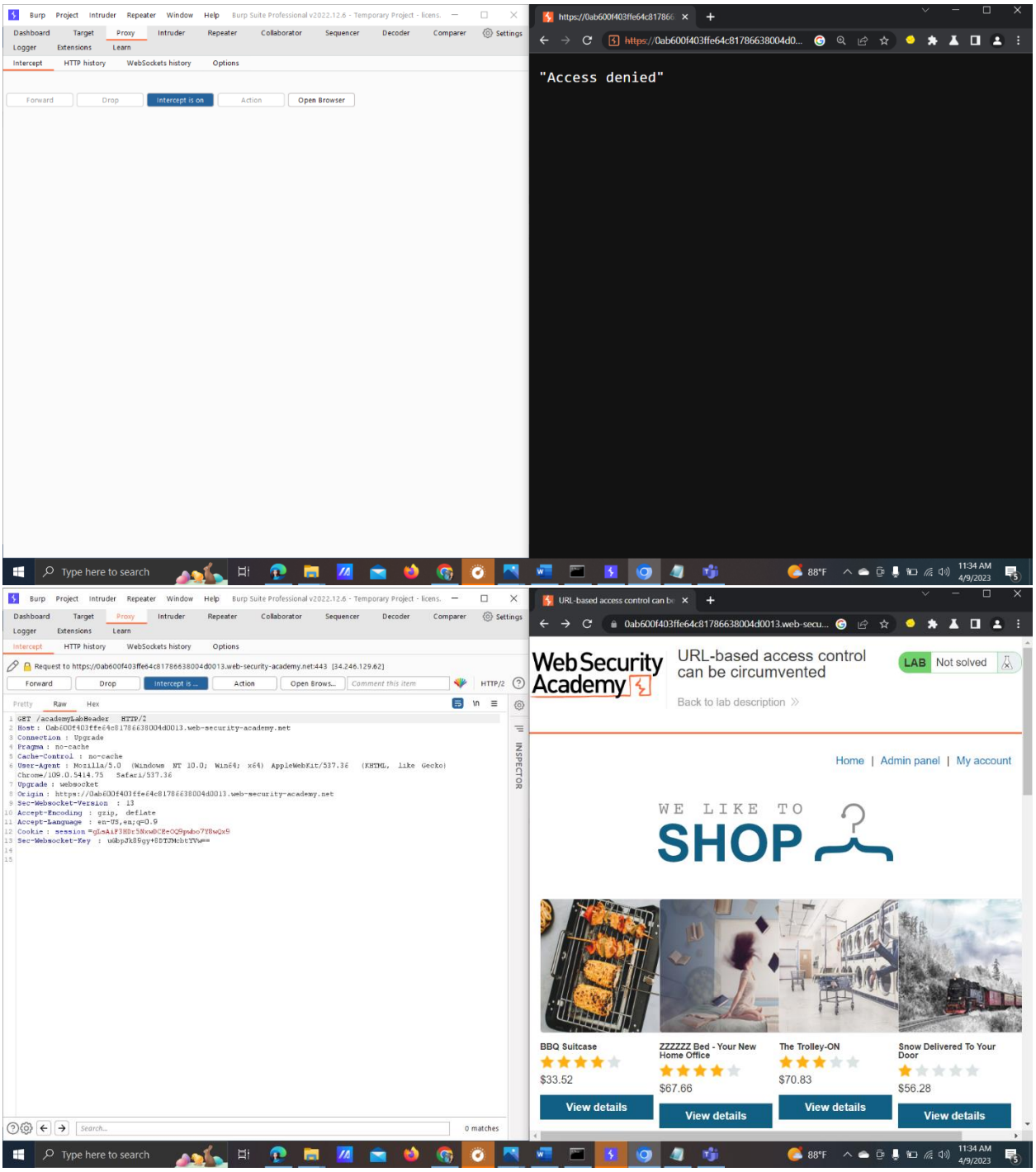
Then add "/admin" on your top-up search bar and press ENTER key. Then you can see load your browser and you can see" Access denied"



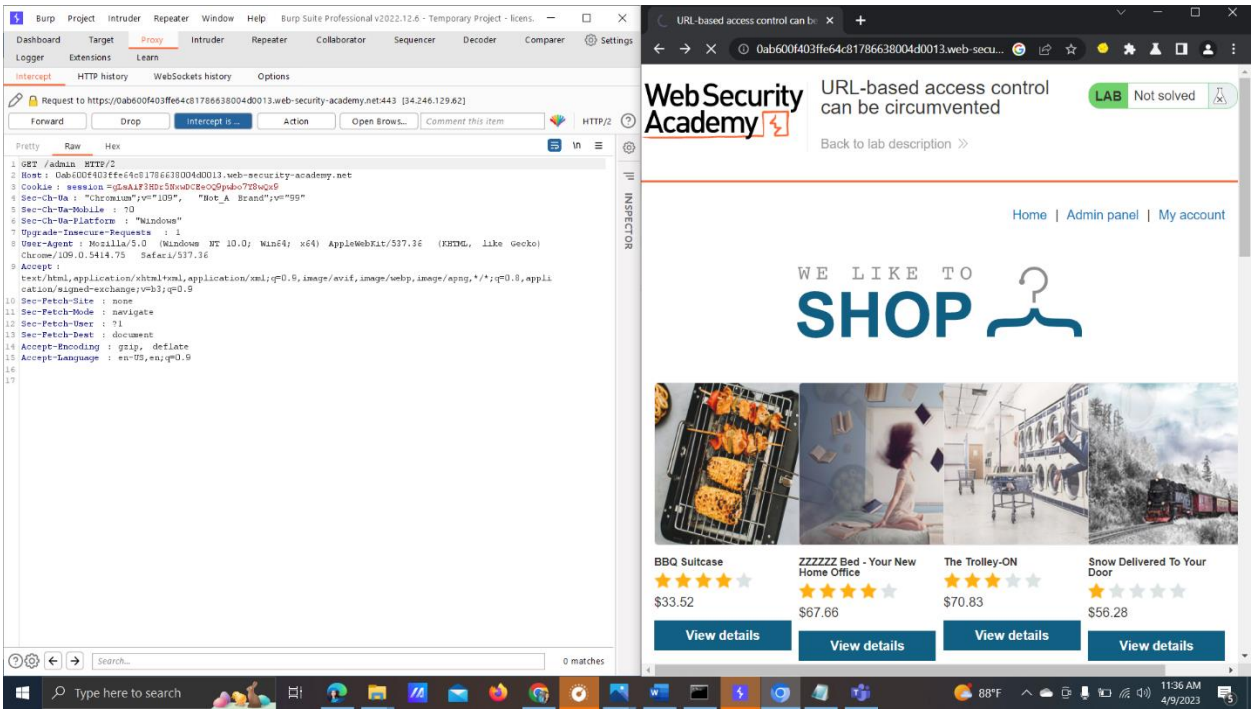
Port Swigger – Access control vulnerabilities and privilege escalation



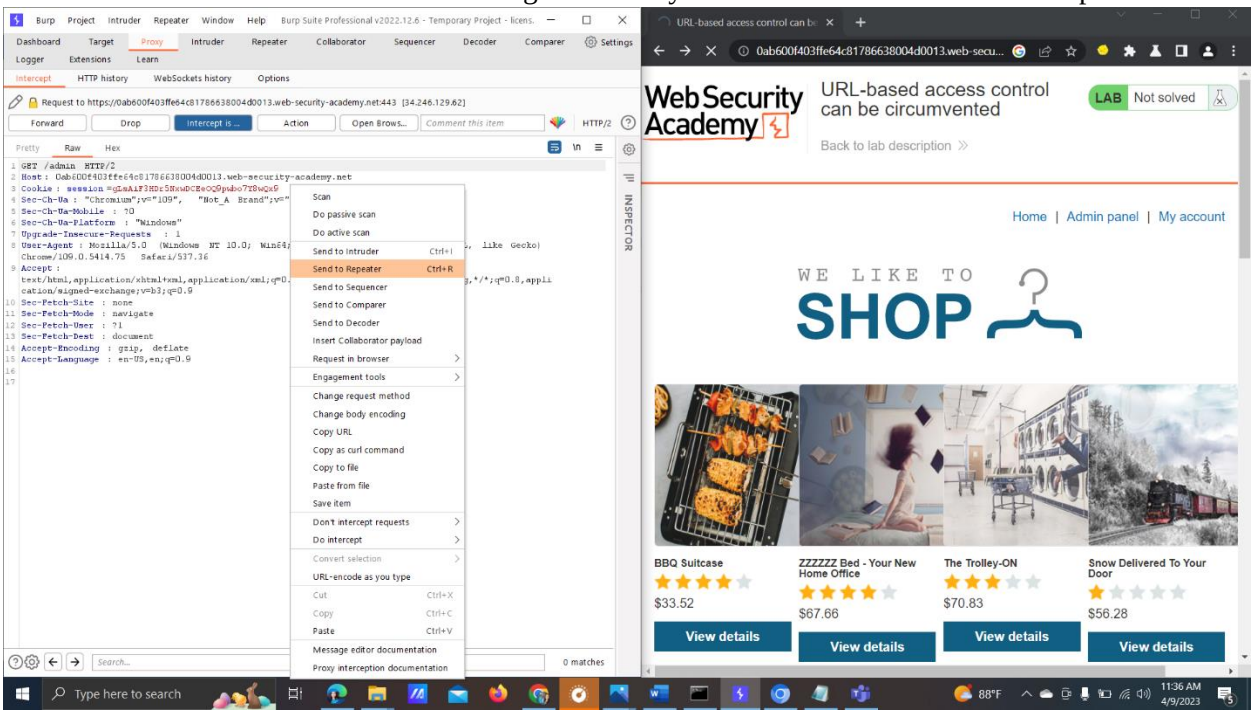
Port Swigger – Access control vulnerabilities and privilege escalation



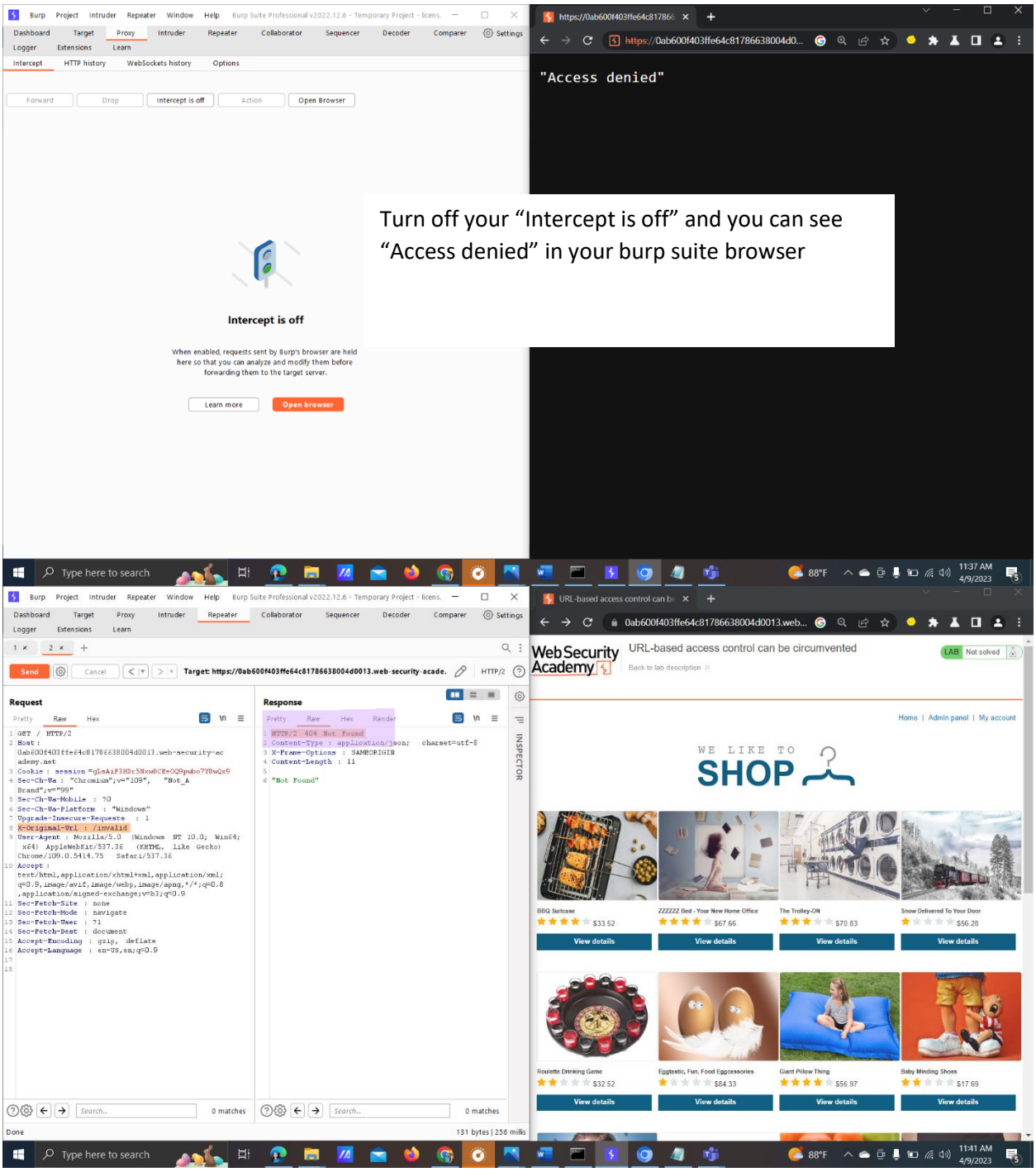
Port Swigger – Access control vulnerabilities and privilege escalation



The next level is forward and forward and right click on your mouse and select “Send to Repeater”

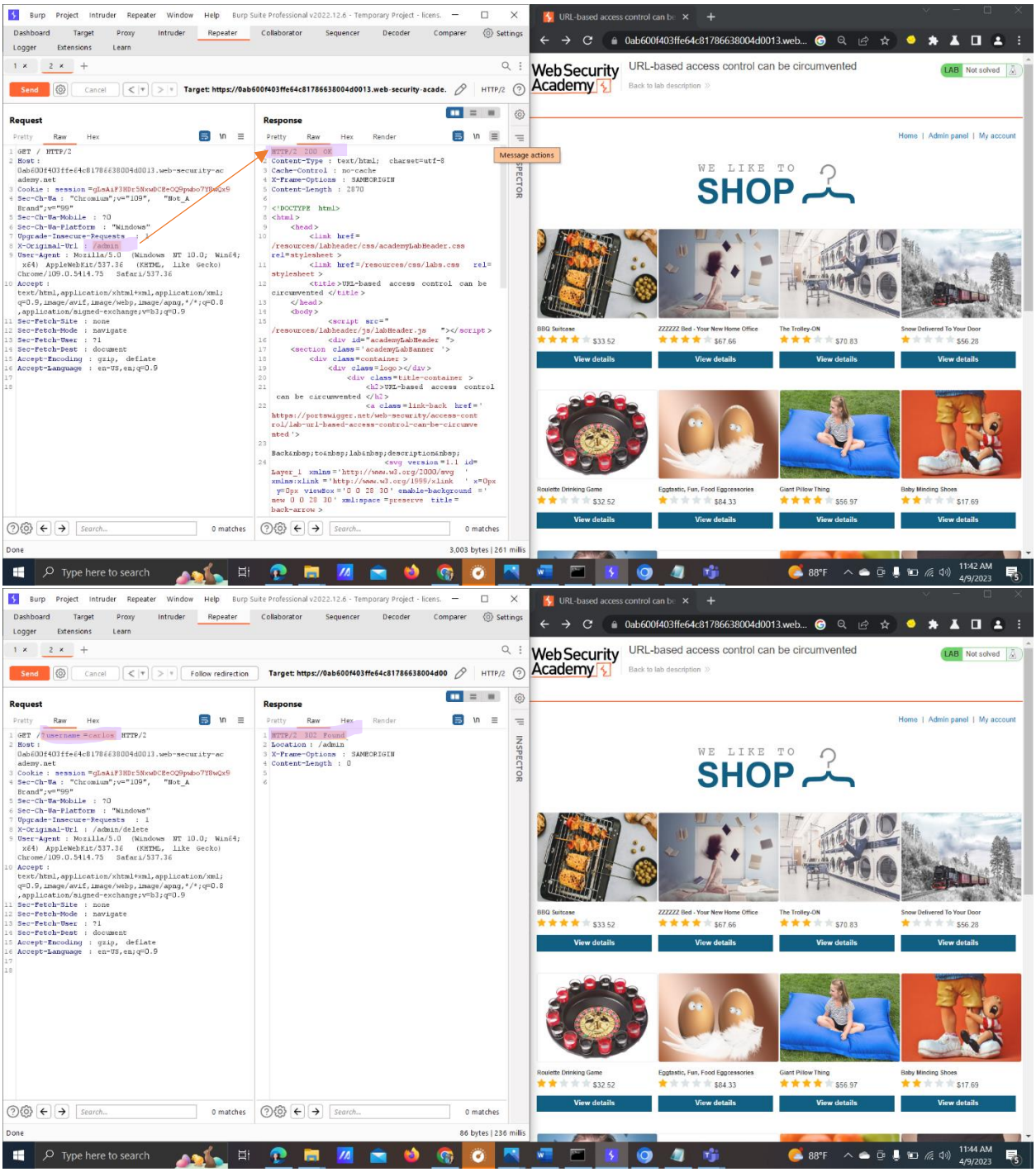


Port Swigger – Access control vulnerabilities and privilege escalation

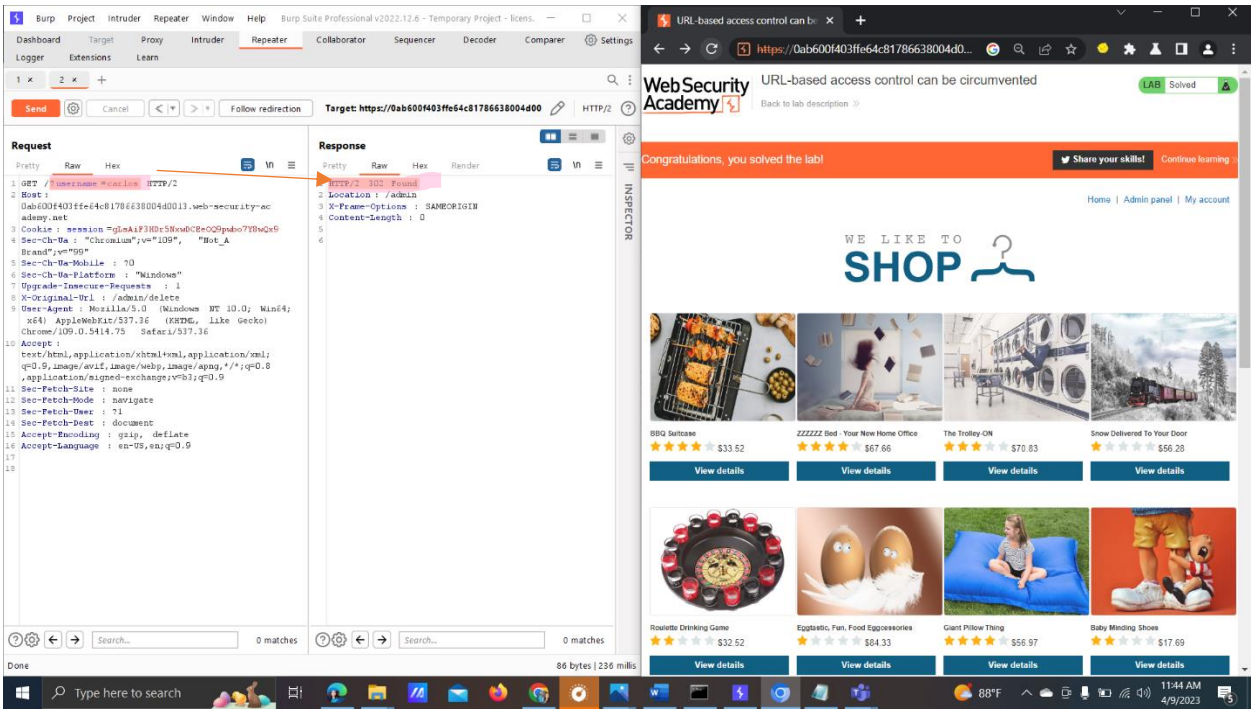


Click the "Repeater"on my burpsuite and just now you can see above this result

Port Swigger – Access control vulnerabilities and privilege escalation



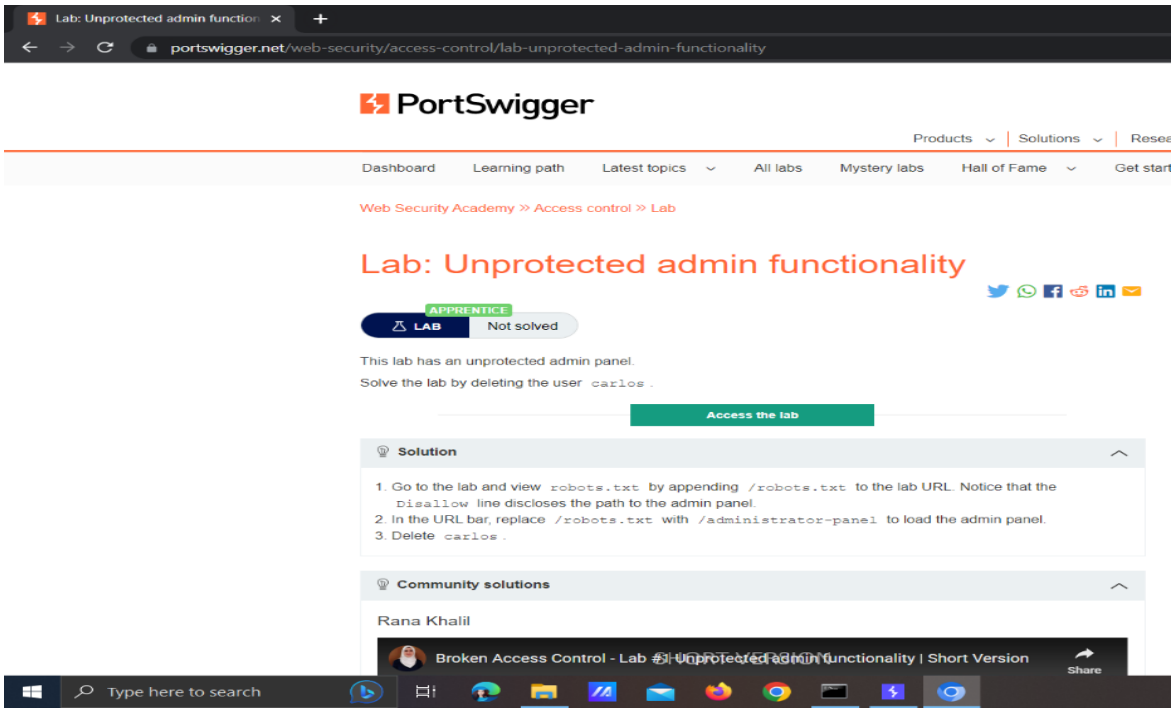
Port Swigger – Access control vulnerabilities and privilege escalation



Finally refresh your browser and you can see solved my lab.

Port Swigger – Access control vulnerabilities and privilege escalation

Lab 1: Unprotected admin functionality



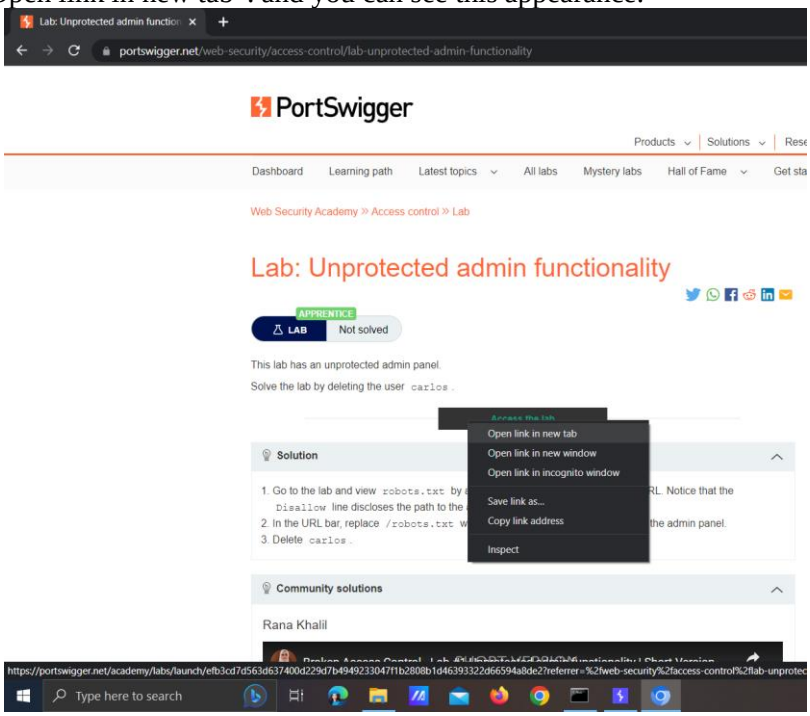
There is an open admin panel in this lab. Remove the user Carlos to finish the lab.

✓ How to solve this lab ?

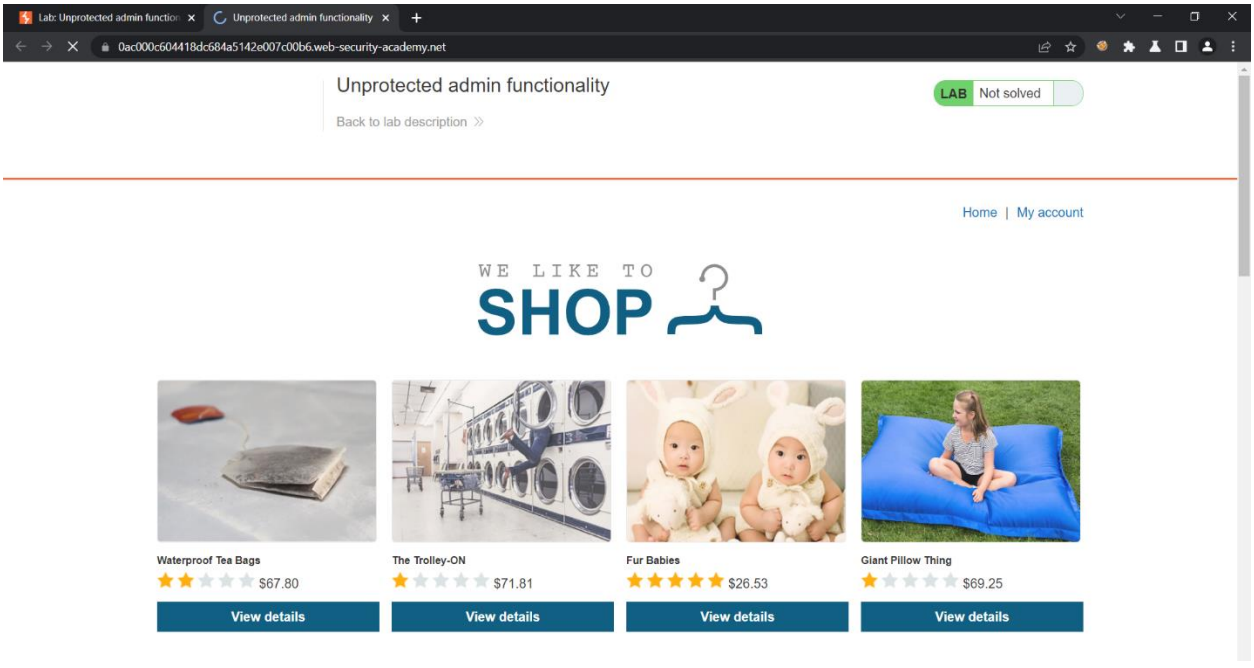
1. Go to the lab and view robots.txt by appending /robots.txt to the lab URL. Notice that the Disallow line discloses the path to the admin panel.
2. In the URL bar, replace /robots.txt with /administrator-panel to load the admin panel.
3. Delete carlos.

Port Swigger – Access control vulnerabilities and privilege escalation

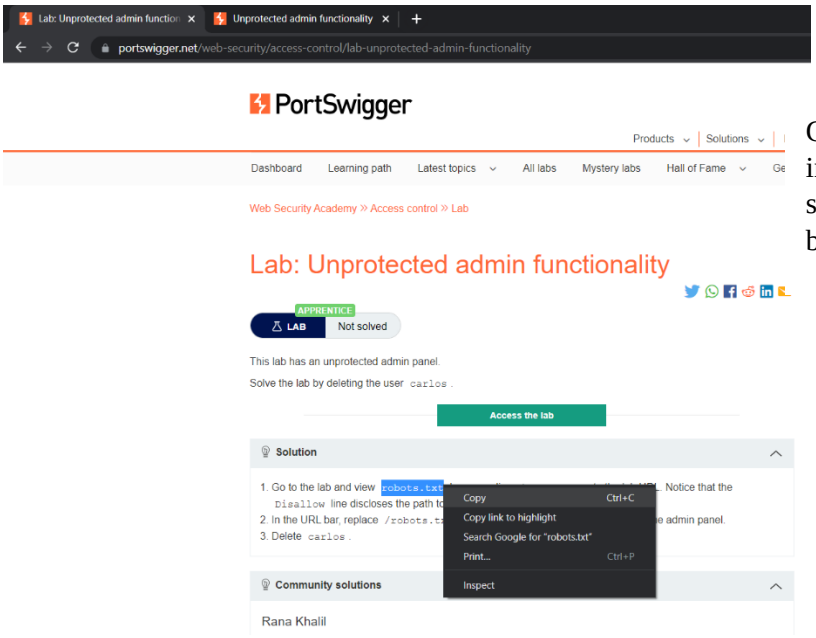
First click the "Access the lab" button and right click on this "Access the lab "button and select on this selection "Open link in new tab". and you can see this appearance.



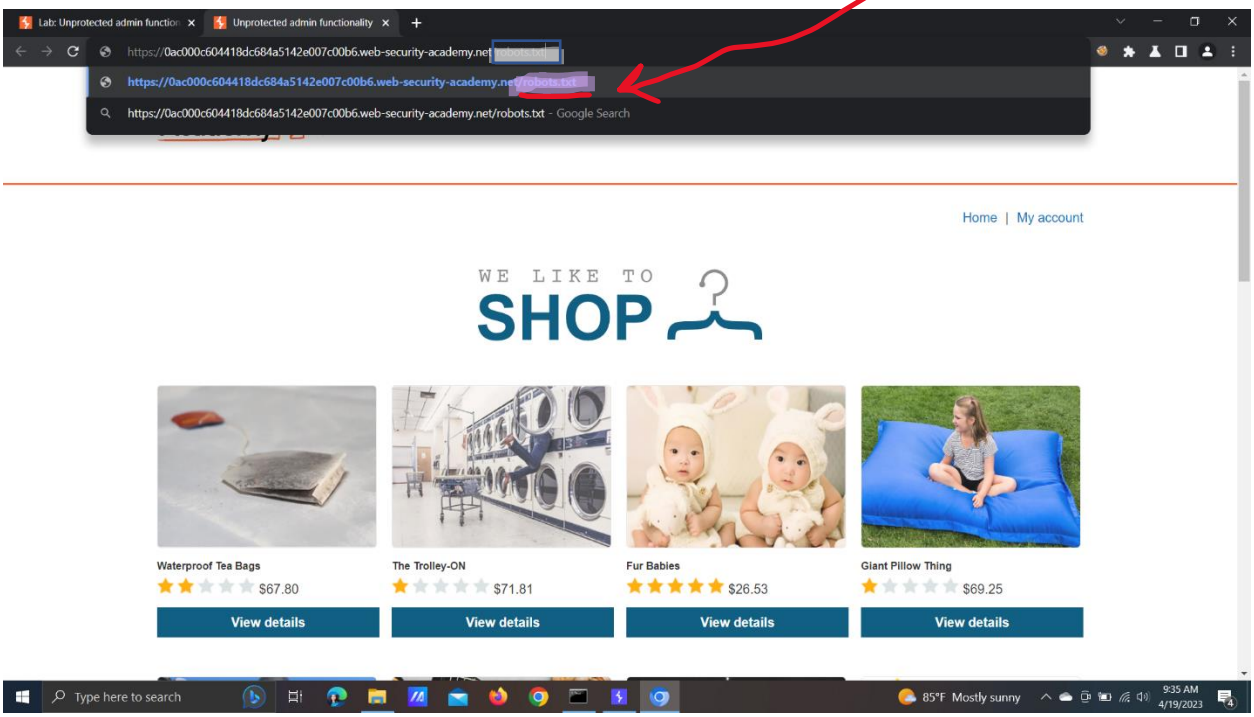
Then we can see open new tab in my burp suit browser



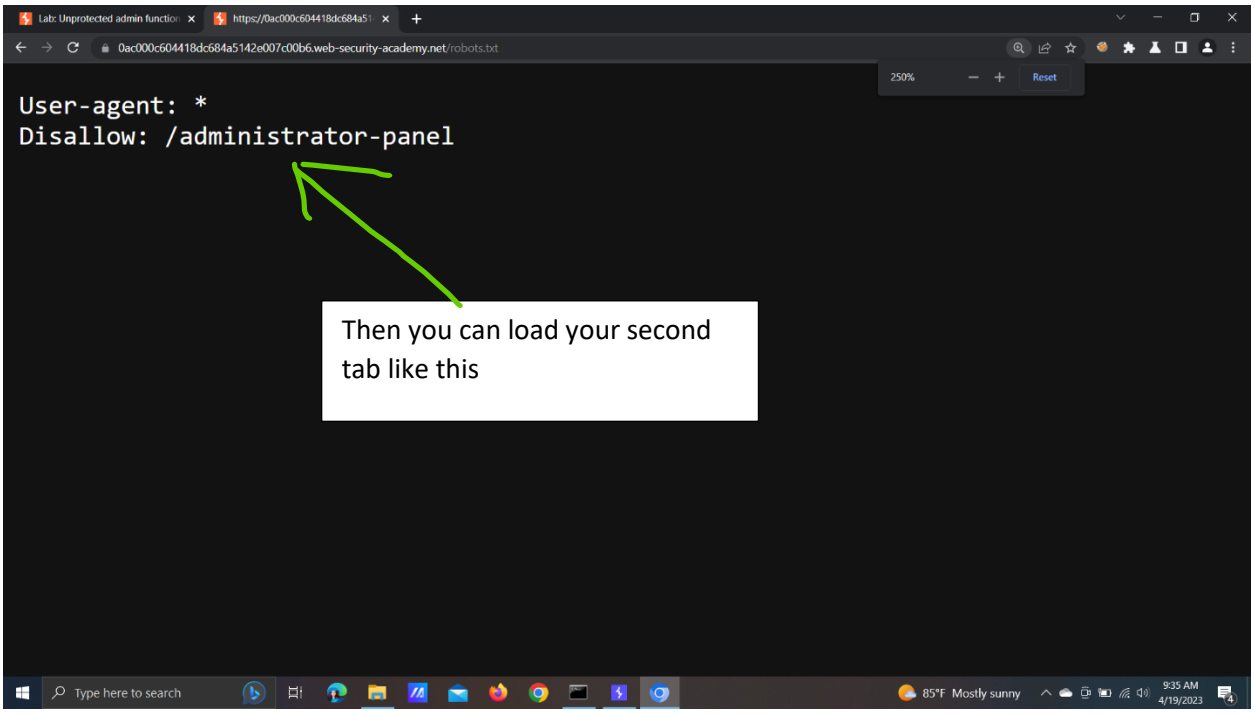
Port Swigger – Access control vulnerabilities and privilege escalation



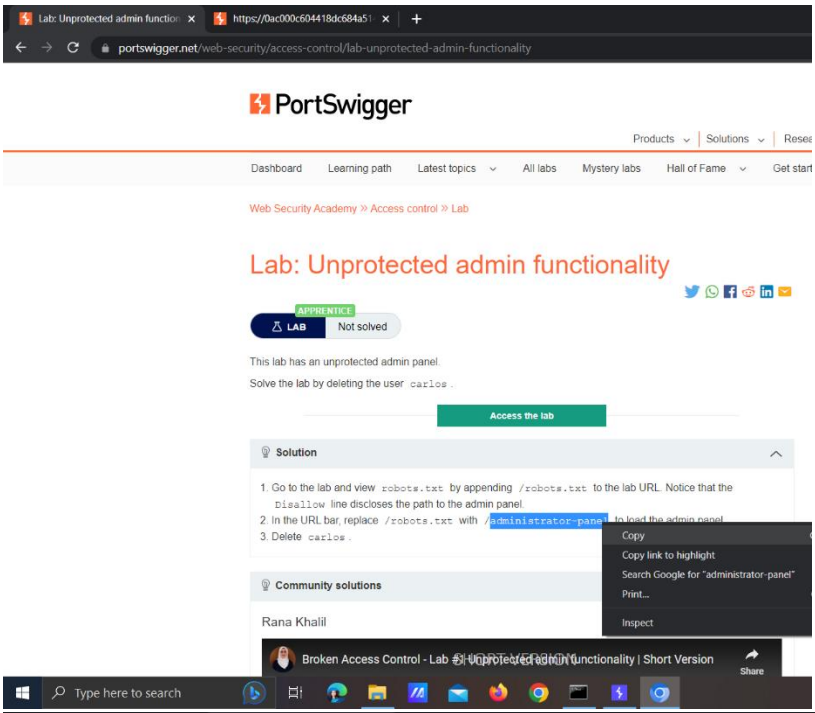
Go to first tab and read “Solution”section and in my first point ,copy the“robot.txt”and paste it second tab in search bar link end point like below this press the “Enter key”.



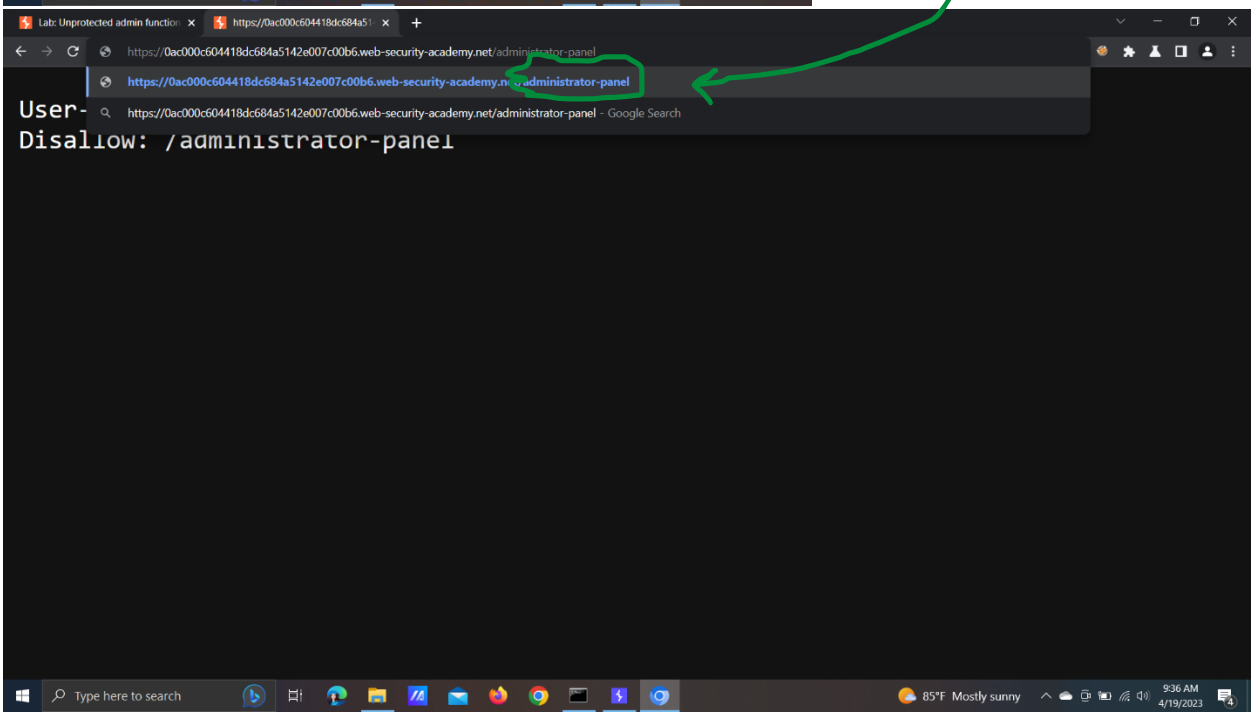
Port Swigger – Access control vulnerabilities and privilege escalation

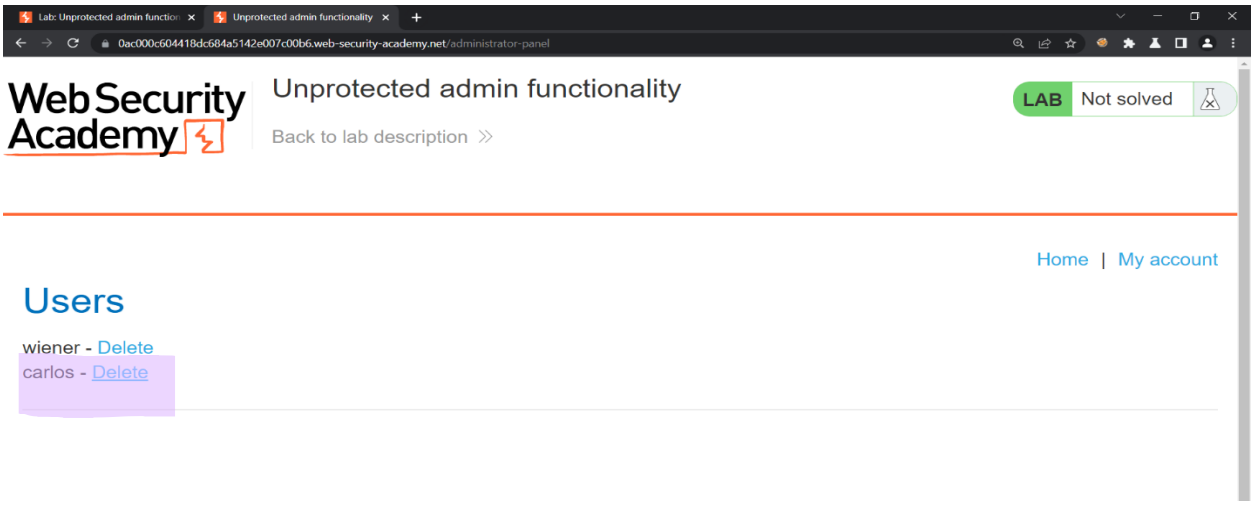


Port Swigger – Access control vulnerabilities and privilege escalation



Go to first tab and read “Solution” section and in my second point ,copy the “/administrator-panel” and paste it second tab in search bar link end point like below this press the “Enter key”.





Then load my second tab and I can show you users like wiener-delete and carlos-delete.So I delete carols's delete and Finally I can show with you my user deleted successfully and sloved my lab like this.