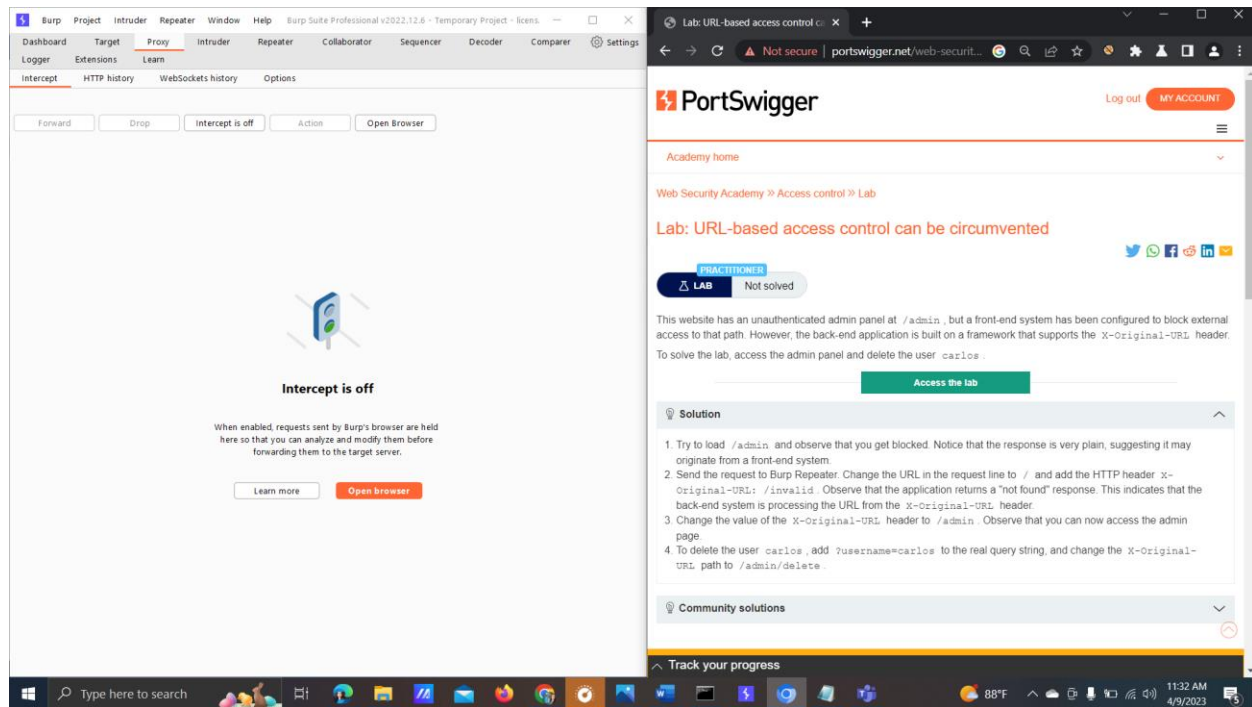


Lab 10: URL-based access control can be circumvented



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 ?

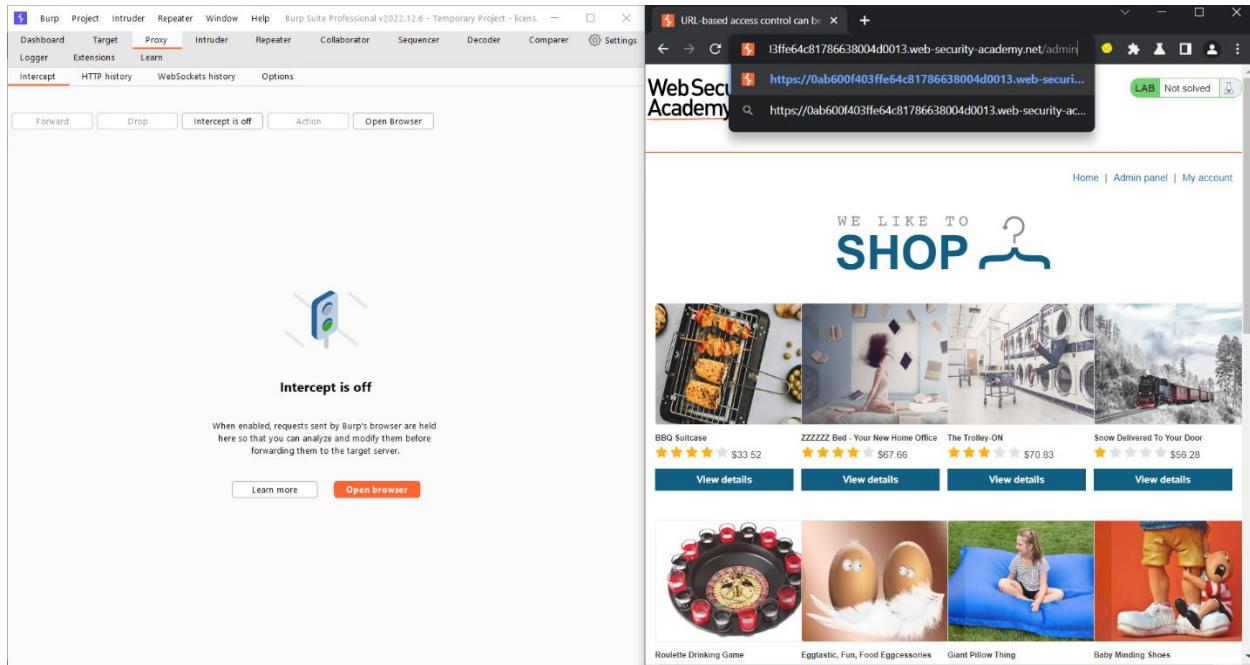
1. Try to load /admin and observe that you get blocked. Notice that the response is very plain, suggesting it may originate from a front-end system.
2. Send the request to Burp Repeater. Change the URL in the request line to / and add the HTTP header X-Original-URL: /invalid. Observe that the application 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.

BSc (Hons) in Information Technology Specializing in Cyber Security

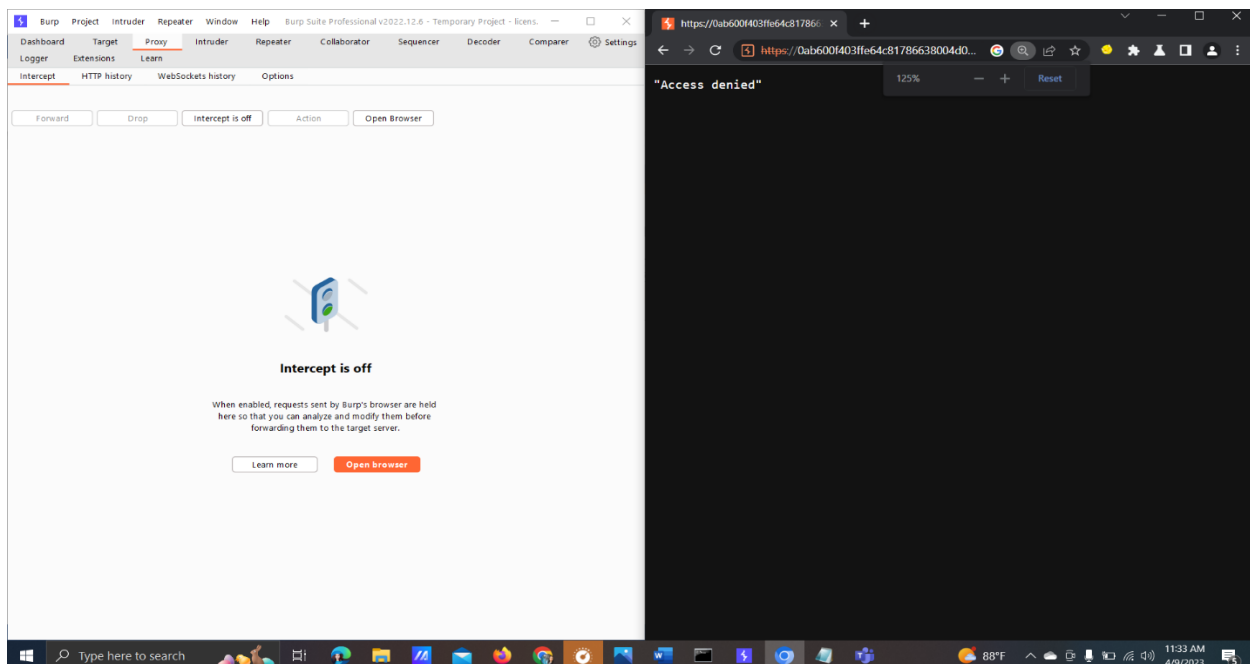
Year 2-Semester 2 IE2062-WEB SECURITY

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.



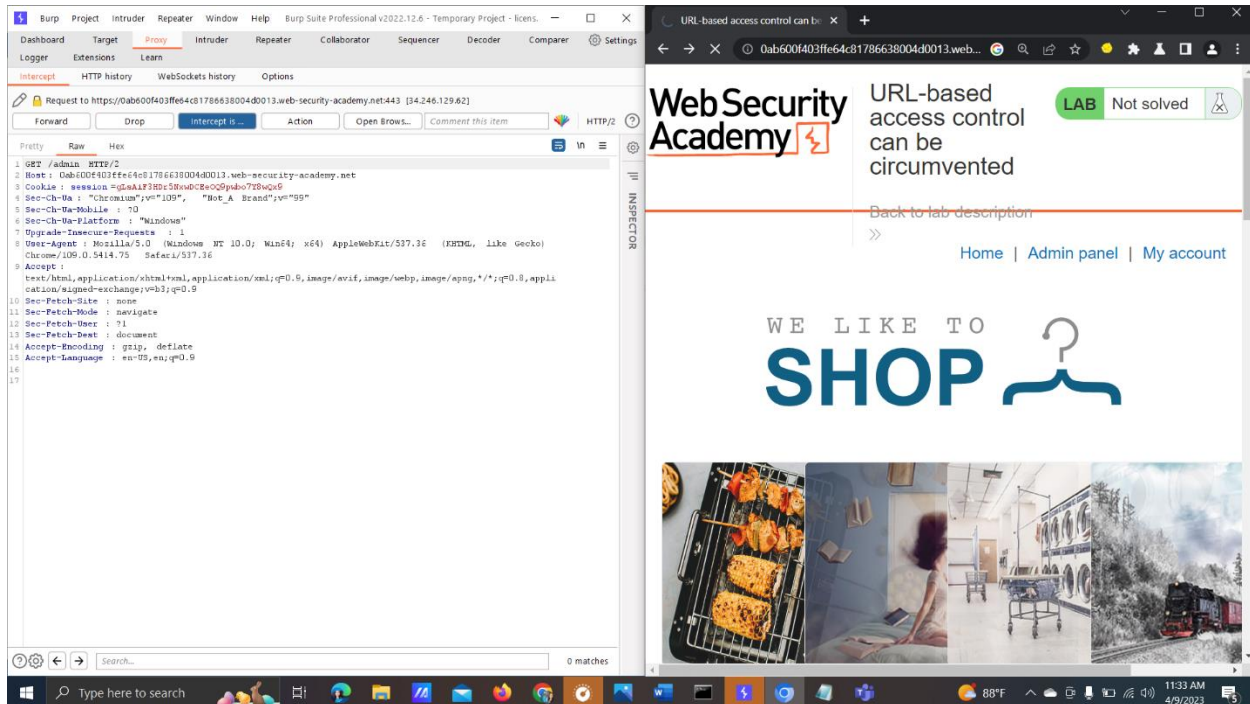
Then add “/admin” on your top-up search bar and press ENTER key. Then you can see load your browser and you can see” Access denied”



BSc (Hons) in Information Technology Specializing in Cyber Security

Year 2-Semester 2 IE2062-WEB SECURITY

Port Swigger - Access control vulnerabilities and privilege escalation



BSc (Hons) in Information Technology Specializing in Cyber Security

Year 2-Semester 2 IE2062-WEB SECURITY

Port Swigger - Access control vulnerabilities and privilege escalation

The image displays two overlapping screenshots from a Windows desktop. The top screenshot shows the Burp Suite Professional v2022.12.6 interface. The 'Intercept' tab is active, showing a list of intercepted requests. The 'Forward' button is highlighted. The bottom screenshot shows a web browser window. The address bar displays the URL 'https://0ab600f403ffe64c81786638004d0013.web-security-academy.net'. The page content shows a 'WebSecurity Academy' logo and a 'SHOP' section with various products. The products listed are:

Product	Price	Rating	Action
BBQ Suitcase	\$33.52	4.5 stars	View details
ZZZZZZ Bed - Your New Home Office	\$67.66	4.5 stars	View details
The Trolley-ON	\$70.83	4.5 stars	View details
Snow Delivered To Your Door	\$56.28	4.5 stars	View details

BSc (Hons) in Information Technology Specializing in Cyber Security

Year 2-Semester 2 IE2062-WEB SECURITY

Port Swigger - Access control vulnerabilities and privilege escalation

The screenshot shows the Burp Suite interface on the left and a web browser on the right. The browser displays a challenge from Web Security Academy titled "URL-based access control can be circumvented". The challenge page has a header "WE LIKE TO SHOP" with a shopping cart icon. Below the header, there are four product listings: "BBQ Suitcase" for \$33.52, "ZZZZZZ Bed - Your New Home Office" for \$67.66, "The Trolley-ON" for \$70.83, and "Snow Delivered To Your Door" for \$56.28. Each listing has a "View details" button. The Burp Suite interface shows a request to "https://0ab600f403ffe4c81786638004d0013.web-security-academy.net:443". The request is an HTTP GET for "/admin". The response is a 200 status code with a content type of "text/html". The Burp Suite interface also shows a "Send to Repeater" button in the context menu.

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

This screenshot is similar to the one above, but it shows the Burp Suite interface with the "Send to Repeater" button highlighted in the context menu. The web browser still shows the same challenge from Web Security Academy. The Burp Suite interface shows the same request to "https://0ab600f403ffe4c81786638004d0013.web-security-academy.net:443". The request is an HTTP GET for "/admin". The response is a 200 status code with a content type of "text/html". The Burp Suite interface also shows a "Send to Repeater" button in the context menu.

BSc (Hons) in Information Technology Specializing in Cyber Security

Year 2-Semester 2 IE2062-WEB SECURITY

Port Swigger - Access control vulnerabilities and privilege escalation

Turn off your "Intercept is off" and you can see "Access denied" in your burp suite browser

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

The image displays two screenshots from the Burp Suite Professional v2022.12.6 interface. The top screenshot shows the 'Intercept' tab with a message 'Intercept is off' and a button to 'Open browser'. The bottom screenshot shows the 'Repeater' tab with a request and response for a URL-based access control vulnerability. The response is 'Access denied'. The bottom screenshot also shows a browser window displaying 'Access denied' and a list of products from 'WebSecurity Academy'.

BSc (Hons) in Information Technology Specializing in Cyber Security

Year 2-Semester 2 IE2062-WEB SECURITY

Port Swigger - Access control vulnerabilities and privilege escalation

The image displays a screenshot of a computer screen with two windows open. The top window is Burp Suite Professional v2022.12.6, showing a HTTP request and response. The request is a GET to `https://0ab600f403ffe4c81786638004d0013.web-security-academy`. The response is a 200 OK from the same URL. The response body contains HTML with a title "URL-based access control can be circumvented" and a description. The bottom window is a web browser showing the "WebSecurity Academy" website. The page title is "URL-based access control can be circumvented" and it features a "SHOP" section with various items for sale.

Burp Suite Request:

```
1 GET / HTTP/2
2 Host: 0ab600f403ffe4c81786638004d0013.web-security-academy.net
3 Cookie: session=glaiaf3H0c58w0CReQ0pabo70bWQ9
4 Sec-Ch-Ua: "Chromium";v="109", "Not_A
5 Brand";v="99"
6 Sec-Ch-Ua-Mobile: ?0
7 Upgrade-Insecure-Requests: 1
8 X-Original-Url: /admin/delete
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.5414.75 Safari/537.36
10 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=0.9
11 Sec-Fetch-Site: none
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
```

Burp Suite Response:

```
1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 Cache-Control: no-cache
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 2870
6
7 <!DOCTYPE html>
8 <html>
9 <head>
10 <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
11 <link href=/resources/css/labs.css rel=stylesheet>
12 <title>URL-based access control can be circumvented</title>
13 </head>
14 <body>
15 <script src=/resources/labheader/js/labHeader.js></script>
16 <div id=academyLabHeader>
17 <div class=academyLabBanner>
18 <div class=container>
19 <div class=title=container>
20 <h2>URL-based access control can be circumvented</h2>
21 https://portswigger.net/web-security/access-control/lab-url-based-access-control-can-be-circumvented
22 </div>
23 </div>
24 </div>
25 </div>
26 </div>
27 </div>
28 </div>
29 </div>
30 </div>
31 </div>
32 </div>
33 </div>
34 </div>
35 </div>
36 </div>
37 </div>
38 </div>
39 </div>
40 </div>
41 </div>
42 </div>
43 </div>
44 </div>
45 </div>
46 </div>
47 </div>
48 </div>
49 </div>
50 </div>
51 </div>
52 </div>
53 </div>
54 </div>
55 </div>
56 </div>
57 </div>
58 </div>
59 </div>
60 </div>
61 </div>
62 </div>
63 </div>
64 </div>
65 </div>
66 </div>
67 </div>
68 </div>
69 </div>
70 </div>
71 </div>
72 </div>
73 </div>
74 </div>
75 </div>
76 </div>
77 </div>
78 </div>
79 </div>
80 </div>
81 </div>
82 </div>
83 </div>
84 </div>
85 </div>
86 </div>
87 </div>
88 </div>
89 </div>
90 </div>
91 </div>
92 </div>
93 </div>
94 </div>
95 </div>
96 </div>
97 </div>
98 </div>
99 </div>
100 </div>
```

Web Security Academy Page:

URL-based access control can be circumvented

Home | Admin panel | My account

WE LIKE TO SHOP

BBQ Sausage \$33.52

ZZZZZ (bed) - Your New Home Office \$67.66

The Trolley-ON \$70.83

Snow Delivered To Your Door \$56.28

Roulette Drinking Game \$32.52

Eggtronic, Fun, Food Eggcessories \$64.33

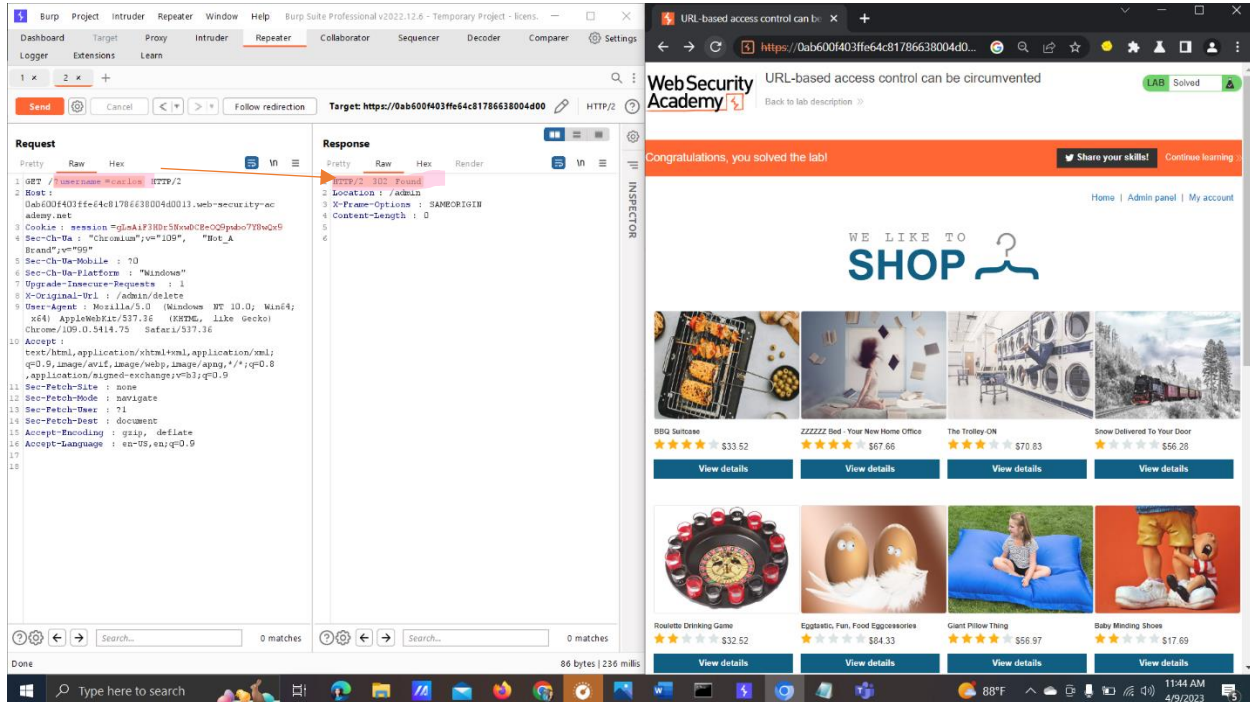
Giant Pillow Thing \$56.97

Baby Minding Shoes \$17.69

BSc (Hons) in Information Technology Specializing in Cyber Security

Year 2-Semester 2 IE2062-WEB SECURITY

Port Swigger - Access control vulnerabilities and privilege escalation



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

Port Swagger - Access control vulnerabilities and privilege escalation

Lab 1: Unprotected admin functionality

The screenshot shows the PortSwagger web security lab interface. The browser address bar displays 'portswigger.net/web-security/access-control/lab-unprotected-admin-functionality'. The page header includes the PortSwagger logo and navigation links: Products, Solutions, and Reset. Below the header, there are tabs for Dashboard, Learning path, Latest topics, All labs, Mystery labs, Hall of Fame, and Get started. The main content area is titled 'Lab: Unprotected admin functionality' and includes a 'Web Security Academy >> Access control >> Lab' breadcrumb. A 'LAB' button is labeled 'APPRENTICE' and 'Not solved'. The lab description states: 'This lab has an unprotected admin panel. Solve the lab by deleting the user carlos.' A green 'Access the lab' button is present. Below the description, the 'Solution' section lists three steps: 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. The 'Community solutions' section shows a solution by Rana Khalil. The Windows taskbar at the bottom shows the search bar and various application icons.

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

✓ How to solve this lab ?

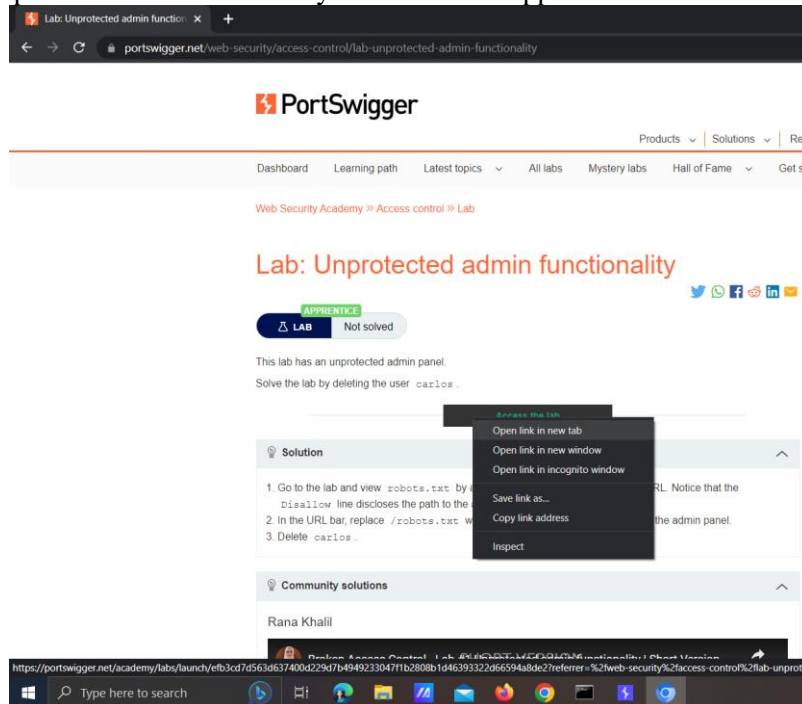
1. Go to the lab and view robots.txt by appending /robots.txt to the lab URL. Notice that the Disallow line discloses the path to the admin panel.
2. In the URL bar, replace /robots.txt with /administrator-panel to load the admin panel.
3. Delete carlos.

BSc (Hons) in Information Technology Specializing in Cyber Security

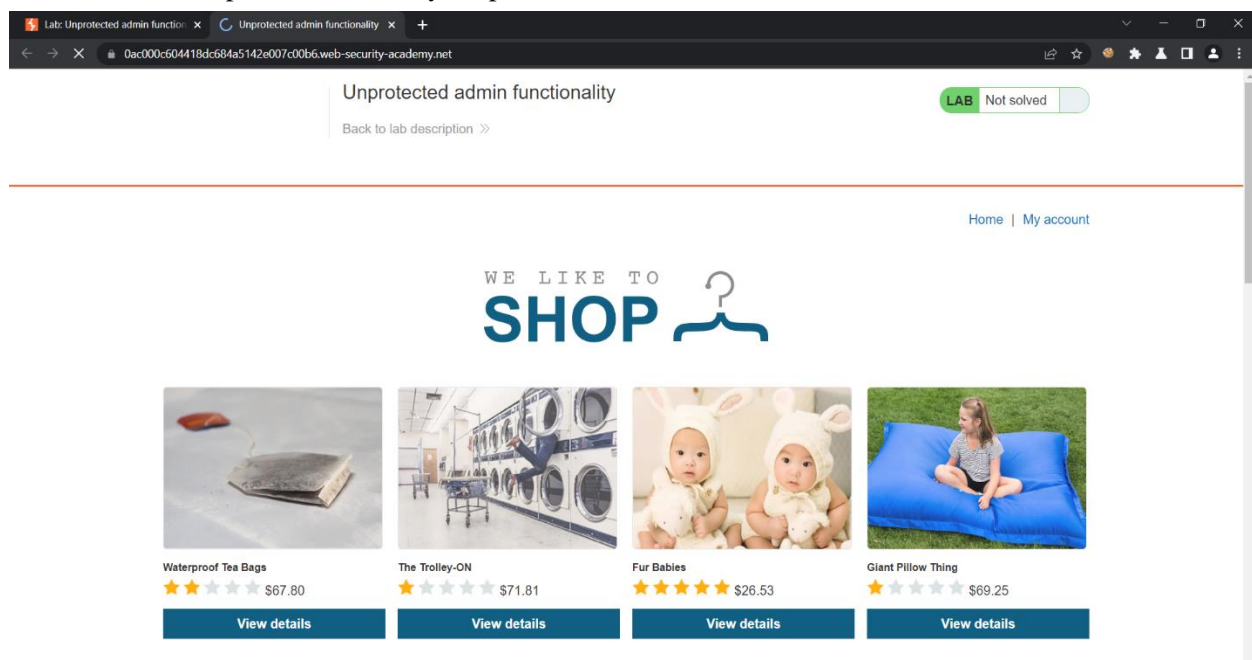
Year 2-Semester 2 IE2062-WEB SECURITY

Port Swagger - Access control vulnerabilities and privilege escalation

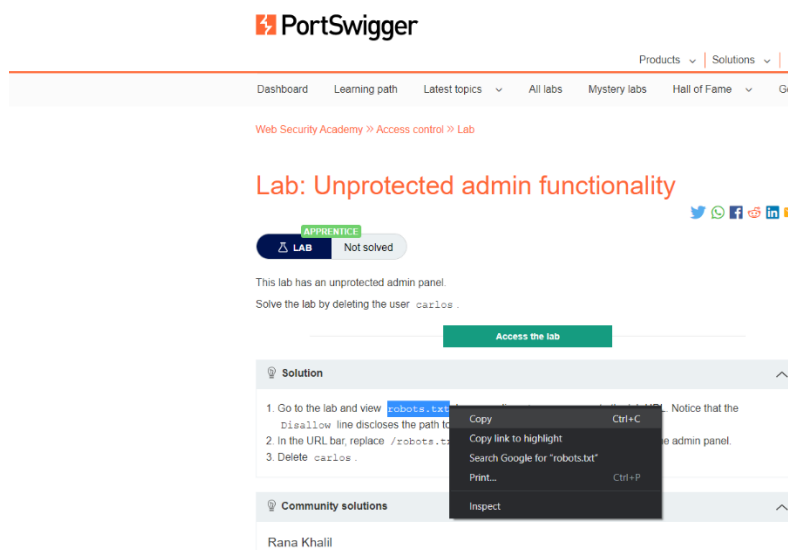
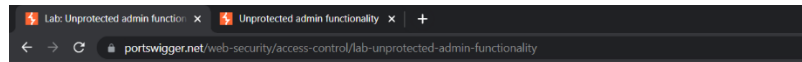
First click the “Access the lab” button and right click on this “Access the lab “button and select on this selection “Open link in new tab”. and you can see this appearance.



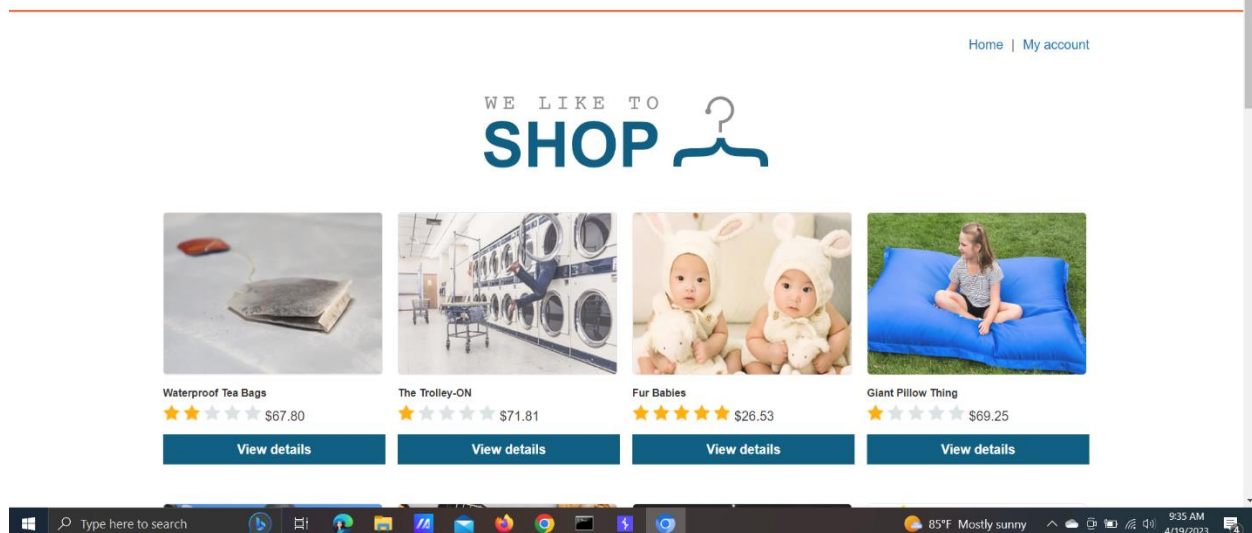
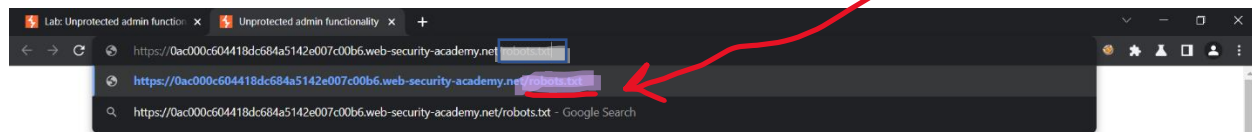
Then we can see open new tab in my burp suit browser



Port Swagger - Access control vulnerabilities and privilege escalation



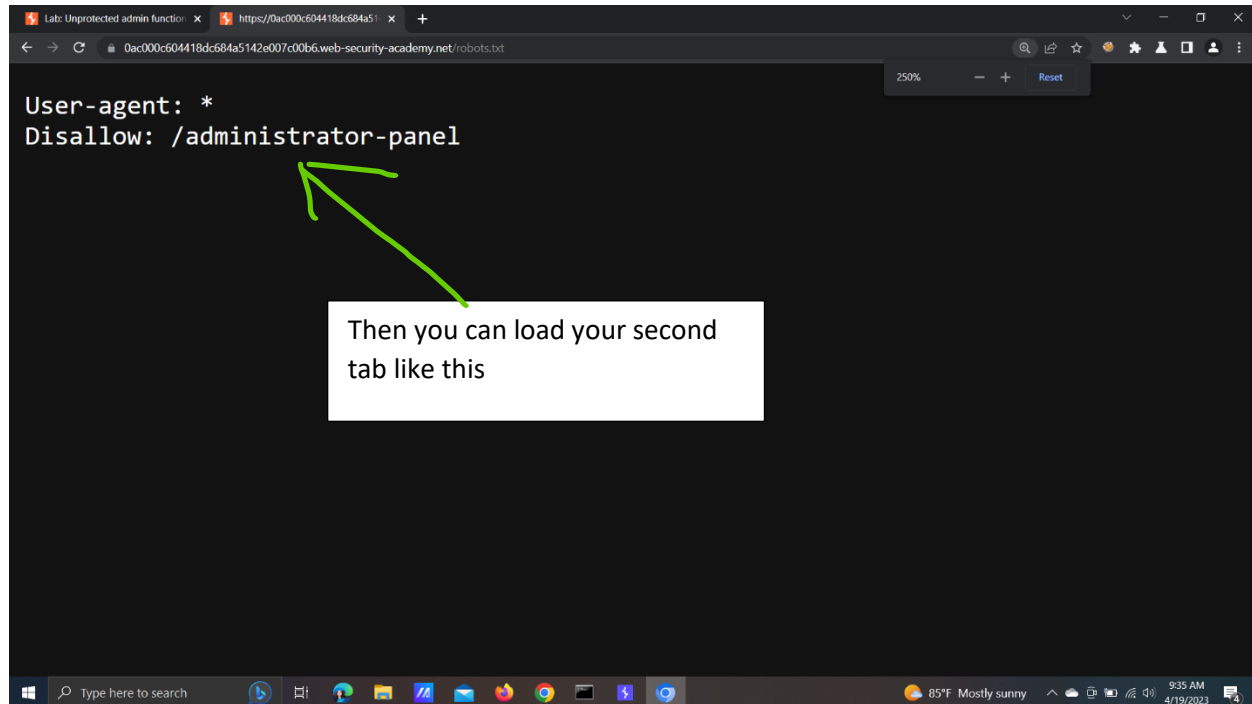
Go to first tab and read “Solution” section and in my first point ,copy the“robot.txt”and paste it second tab in search bar link end point like below this press the “Enter key”.



BSc (Hons) in Information Technology Specializing in Cyber Security

Year 2-Semester 2 IE2062-WEB SECURITY

Port Swigger - Access control vulnerabilities and privilege escalation



BSc (Hons) in Information Technology Specializing in Cyber Security

Year 2-Semester 2 IE2062-WEB SECURITY

Port Swigger - Access control vulnerabilities and privilege escalation

The screenshot shows the PortSwigger web security academy interface. The top navigation bar includes 'Products', 'Solutions', and 'Reset'. The main content area is titled 'Lab: Unprotected admin functionality' and includes a 'Solution' section with the following steps:

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.

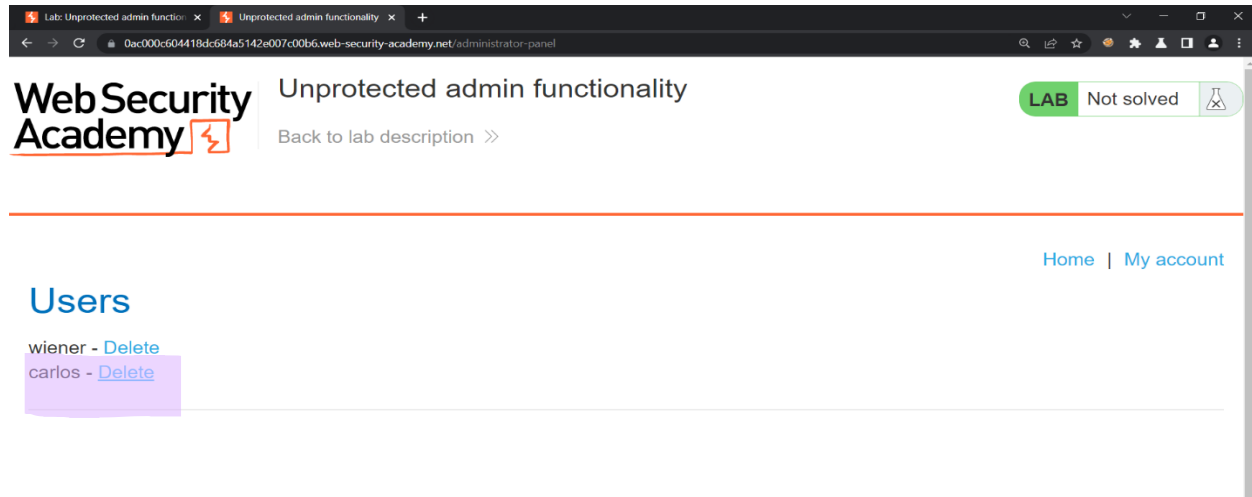
Below the solution section, there is a 'Community solutions' section with a user named Rana Khalil. A green arrow points from the 'Solution' section to a browser window. The browser window shows the URL <https://0ac00c604418dc684a5142e007c00b6.web-security-academy.net/administrator-panel> in the address bar. The browser also shows a search bar with the text 'User: Disallow: /administrator-panel' and a search result for 'https://0ac00c604418dc684a5142e007c00b6.web-security-academy.net/administrator-panel - Google Search'.

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”.

BSc (Hons) in Information Technology Specializing in Cyber Security

Year 2-Semester 2 IE2062-WEB SECURITY

Port Swigger - Access control vulnerabilities and privilege escalation



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

