Lab 7 - User ID controlled by request parameter, with unpredictable user IDs

Ahmed Khaled Saad Ali

ID:1809799

Lab Progress & Screenshots:

Logged in as wiener.

Web Security Academy 5	User ID controlled by request parameter, with IDs Submit solution Back to lab description >>	th unpredictable user LAB Not solved
		Home My account Log out
My Account		
Your username is: wiener Your API Key is: aOGs6Ne32	TeO5rHgemR8nry2h2zGYPfl	
Email		
Update email		

We found out carlos has written a blog, so we turn Intercept ON and see what we get in request.

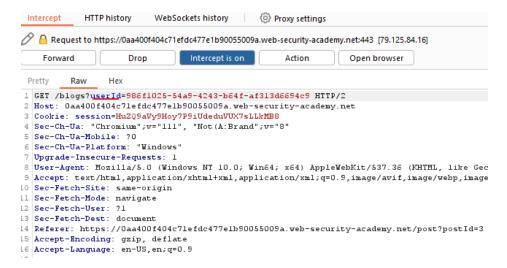


The Digital Fairytale

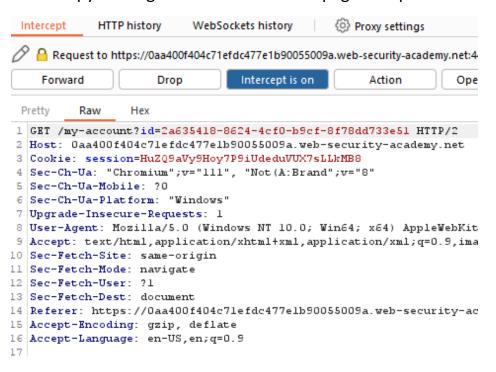
carlos | 28 February 2023

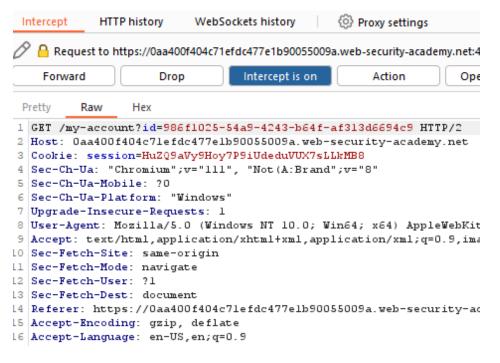
Once upon a time'

We find carlos's userId.



so we copy it and go to wiener's account page to replace it with wiener's userld.





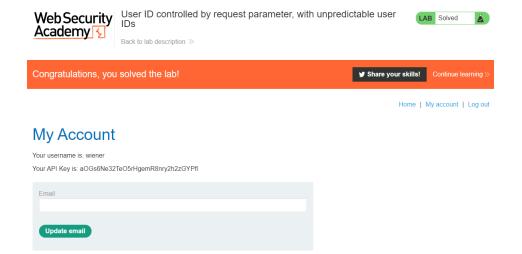
Carlos's account page accessed, API Key copied, lab solved.



Home | My account | Log out

My Account

Your username is: carlos
Your API Key is: 1EOOtOJONuiPHCDdYtBJ4dGgpX1ZjF8e
Email



Lessons:

- 1) Make sure that when a user clicks to view another user they don't send identifiers to that user in requests.
- 2) Don't simply include identifiers of a user in when he sends a request.