Lab 4 - User role can be modified in user profile

Ahmed Khaled Saad Ali

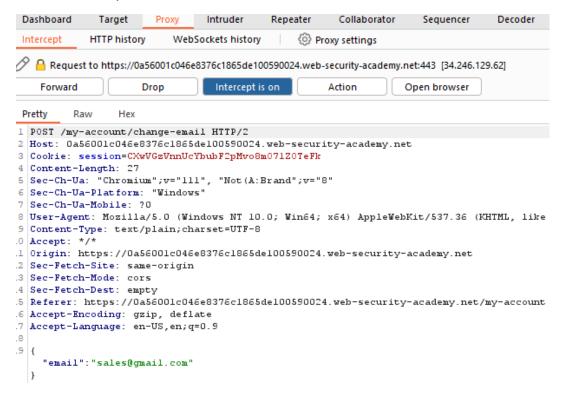
ID:1809799

Lab Progress & Screenshots:	
Logging in as wiener Web Security Academy Back to lab description >>	orofile LAB Not solved 🐰
Login	Home My account
Username wiener Password Log in	

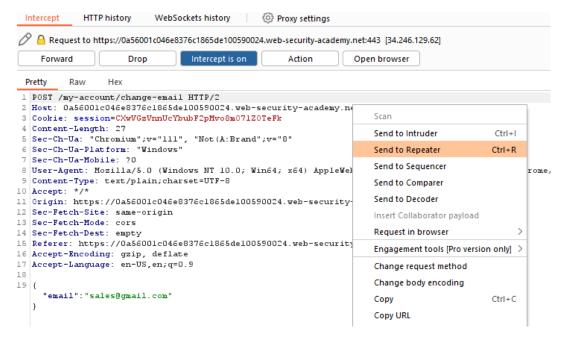
We will turn Intercept ON, and enter an email and press "Update Email"

Web Security Academy 5 User role can be modified in user profile Back to lab description >>	LAB Not solved
	Home My account Log out
My Account	
Your username is: wiener	
Your email is: wiener@normal-user.net	
Email sales@gmail.com Update email	

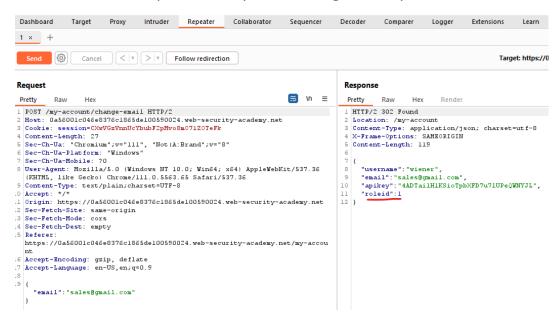
This POST request needs to be sent.



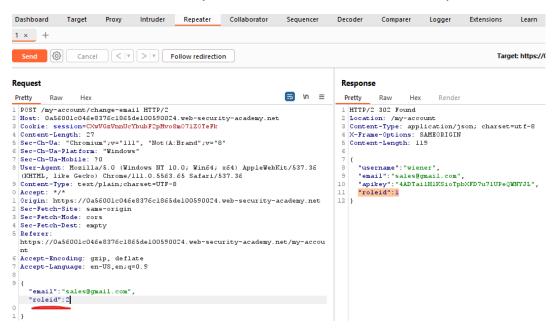
We will take it to the "Repeater" and turn Intercept OFF



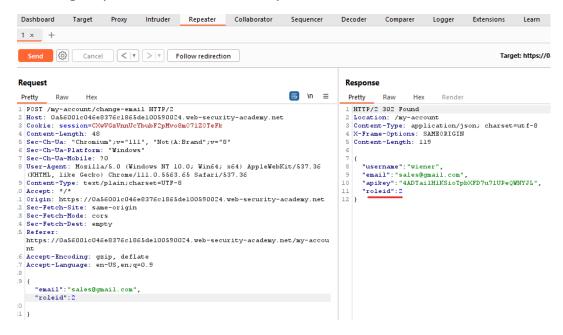
When we send Request in "Repeater" we get a Response with "roleid" of the user



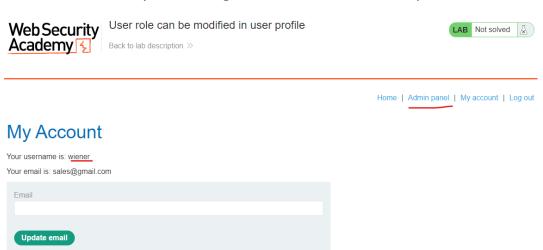
So, we can add in the Request "roleid:2" to access admin panel.



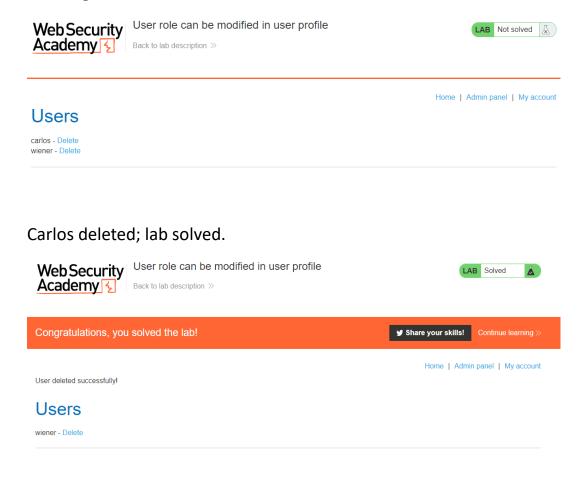
Sending request will result in a response with Admin roleid.



Back to website, by refreshing we find we have Admin panel



Deleting Carlos.



Lessons:

- 1) Hide identifiers like roleid even for normal users, because as soon as admin's id is known normal users will be used as a vulnerability.
- 2) Check for buttons and features even if they appear not related to admin's account