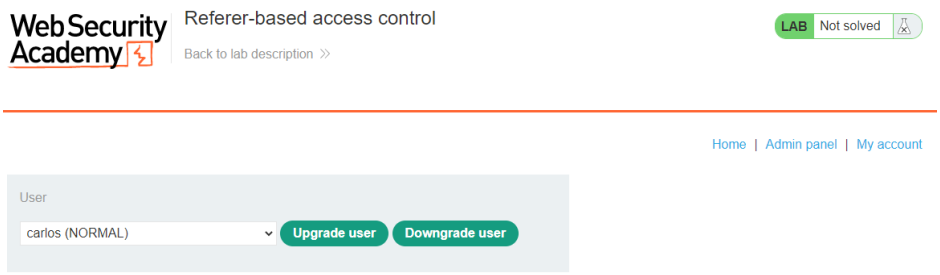
Lab 12 - Referer-based access control

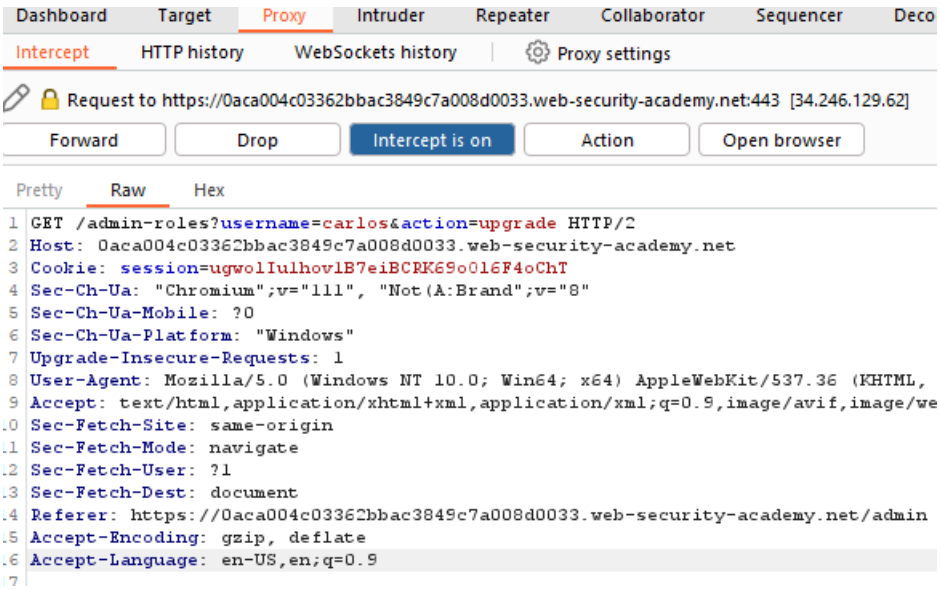
Ahmed Khaled Saad Ali ID:1809799

Lab Progress & Screenshots:

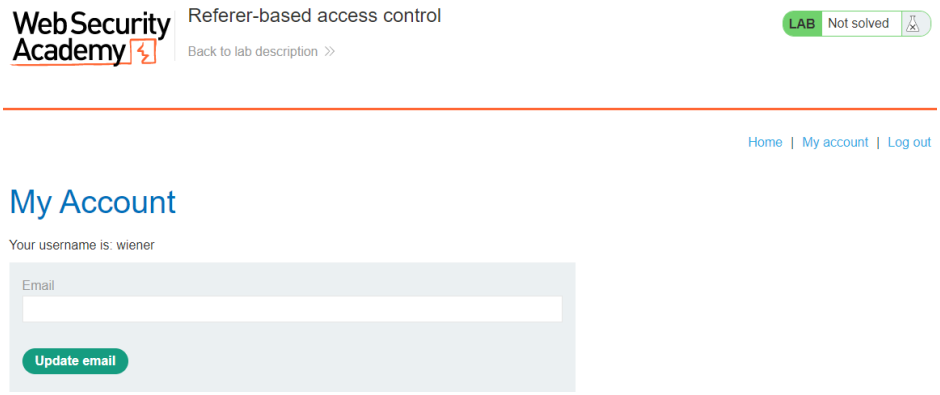
Logged in as administrator to search for vulnerabilities in admin panel.



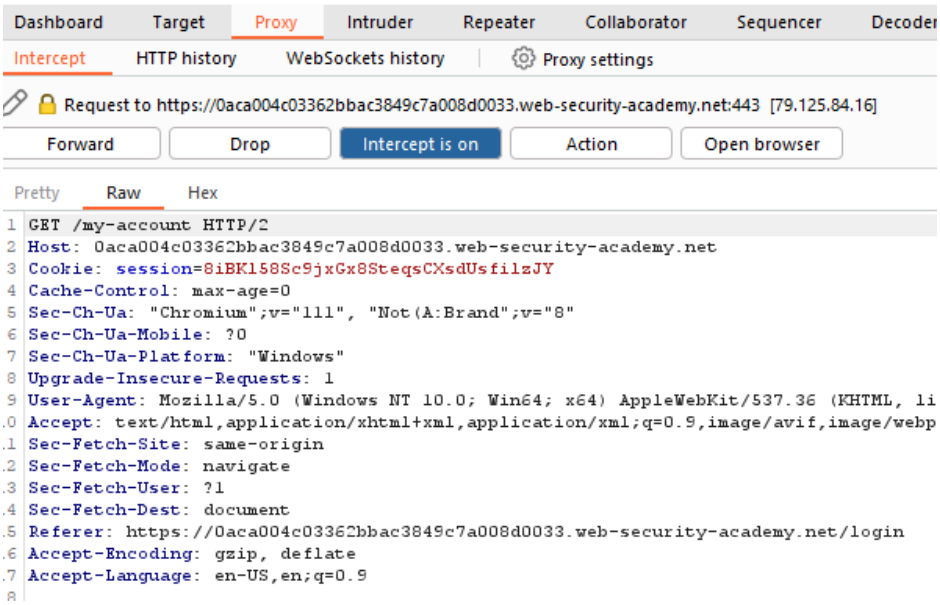
We will try “Upgrade user” on Carlos with Intercept ON to see what is in the request. This is the request; we will send it to the “Repeater”.



Now, we will try to take request above and send it from wiener's page with some edits in the request, So we will login as wiener.

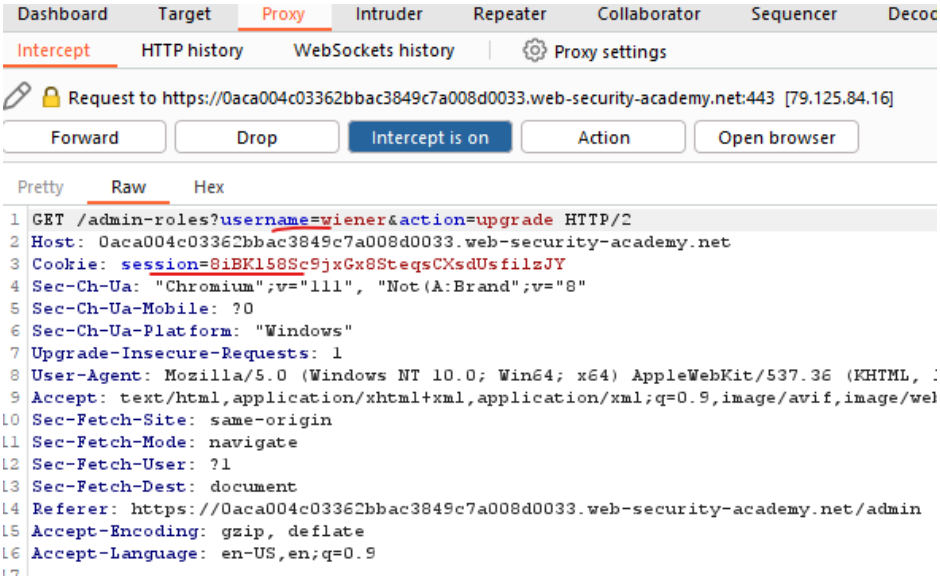


Refresh account page with intercept ON.

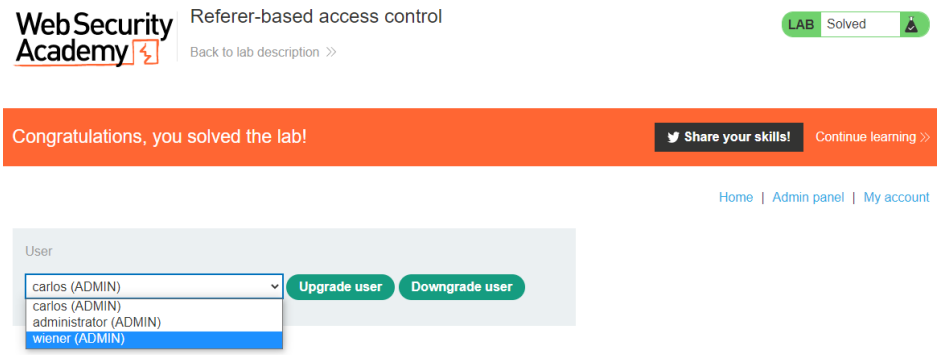


We will replace it completely by GET request /admin-roles, but with two edits.

Put Cookie session of wiener and write wiener in “username” field instead of Carlos. Then forward.



Wiener is an ADMIN now and lab is solved.



Lessons:

Admin’s cookie session shouldn’t be shown in request of an admin-only feature, because as we saw replacing it with any user’s cookie session results in such vulnerability.