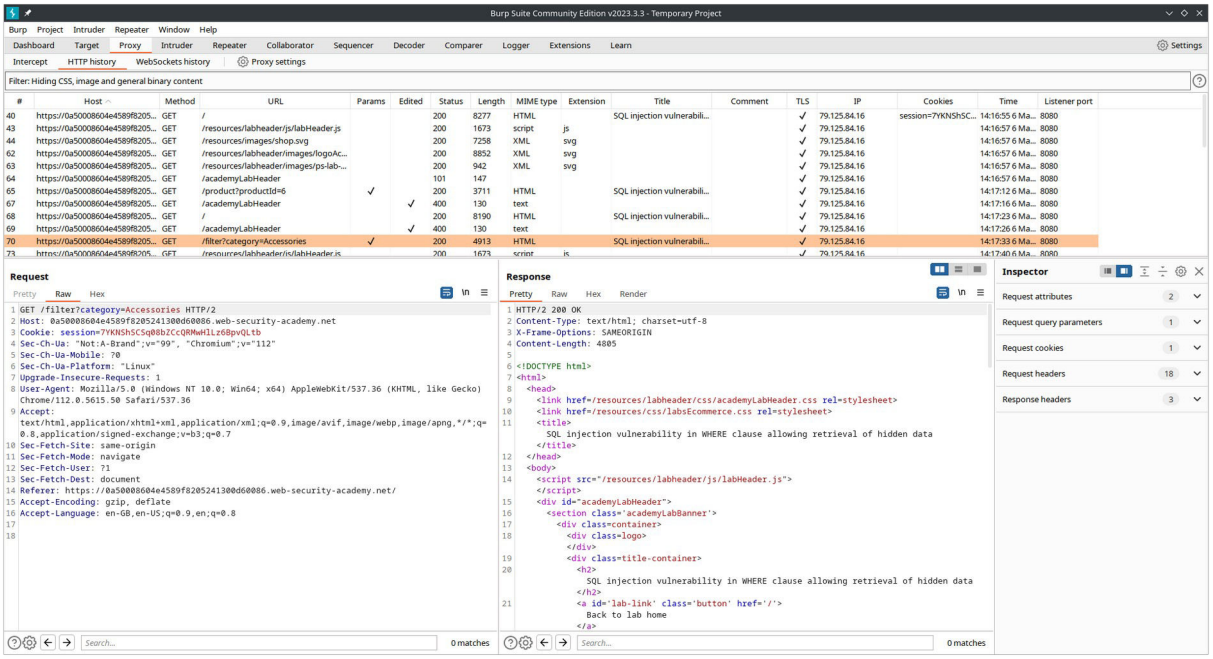
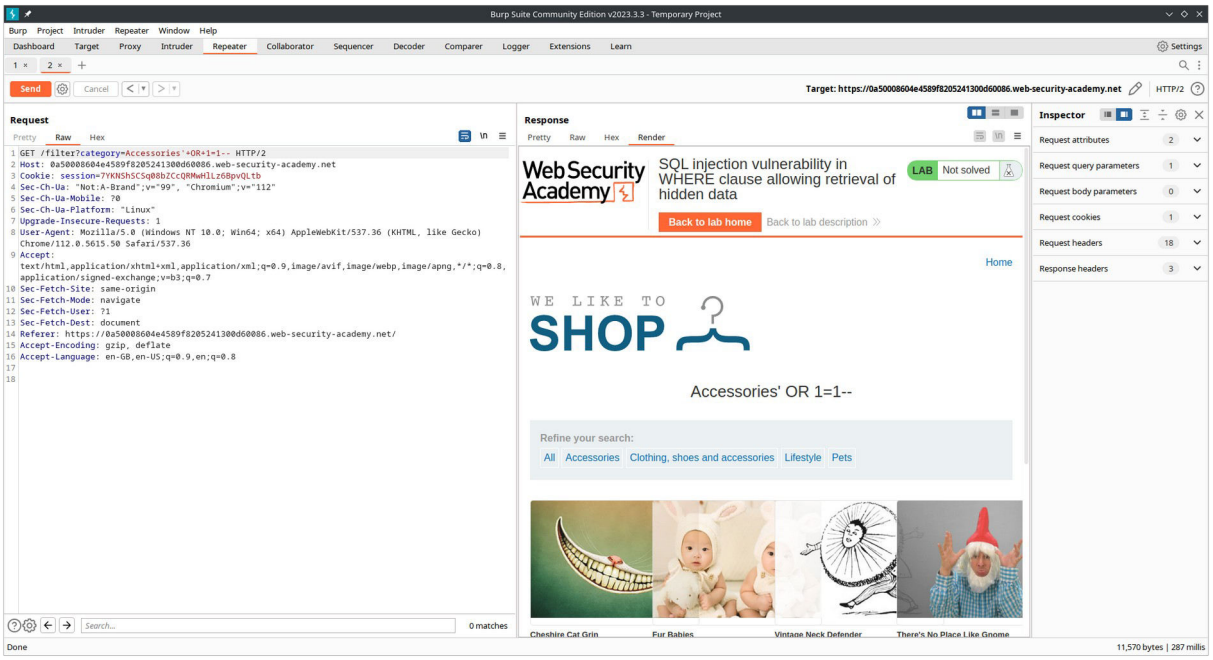
Lab: SQL injection vulnerability in WHERE clause allowing retrieval of hidden data

Open the burpsuite and turn on the intercept in the proxy. Forward the product request to the repeater. In the repeater append the value '+OR+1=1-- in the category parameter value field. Now send the modified request all the products will be displayed.





Lab: SQL injection vulnerability allowing login bypass

Open the burpsuite and turn on the intercept in the proxy. Login with some random credentials and forward this request from the proxy to the repeater. Now change the username parameter as administrator'-- and send this modified request. You will be logged in as the administrator.