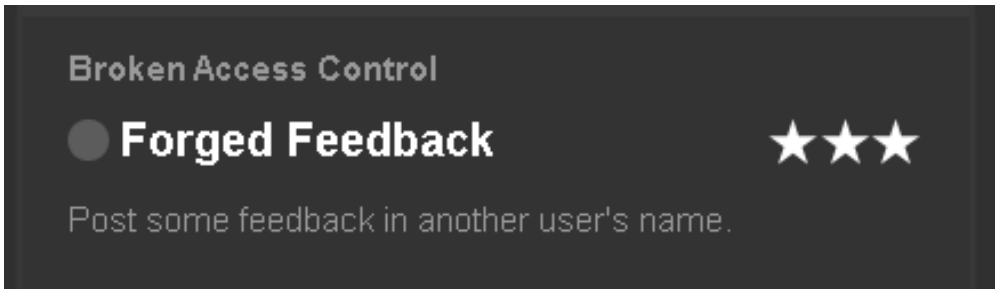
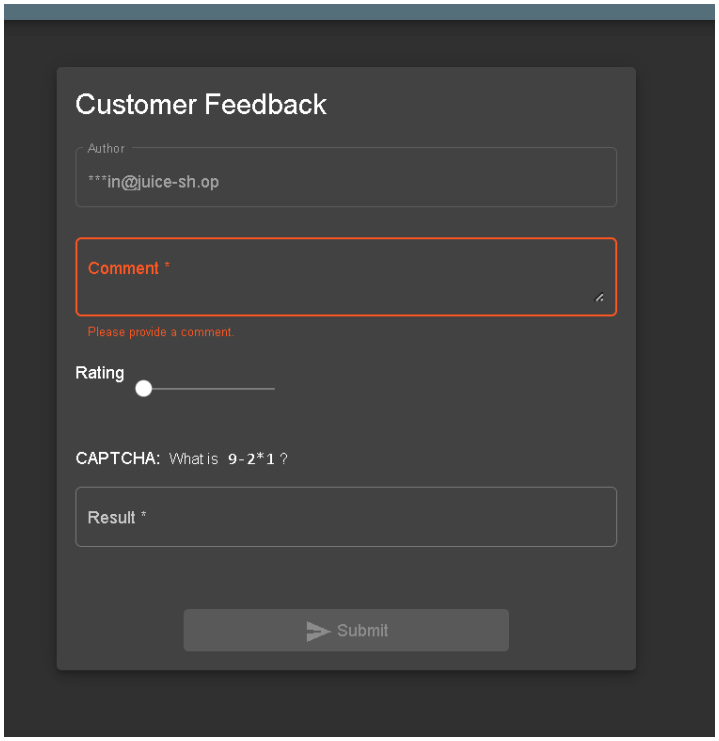
Broken Access Control in OWASP Juice Shop



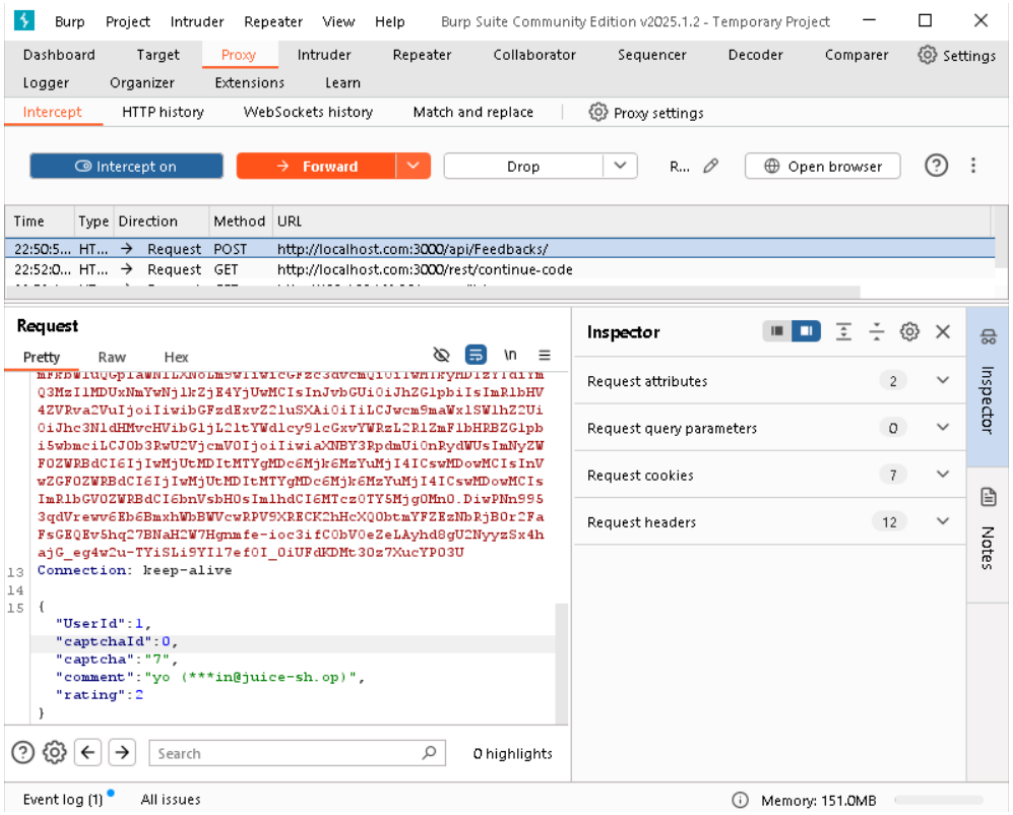
Here we need to post some feedback with another user's name by exploiting the broken access control vulnerability in OWASP juice shop

Going to the page where users can send their feedback

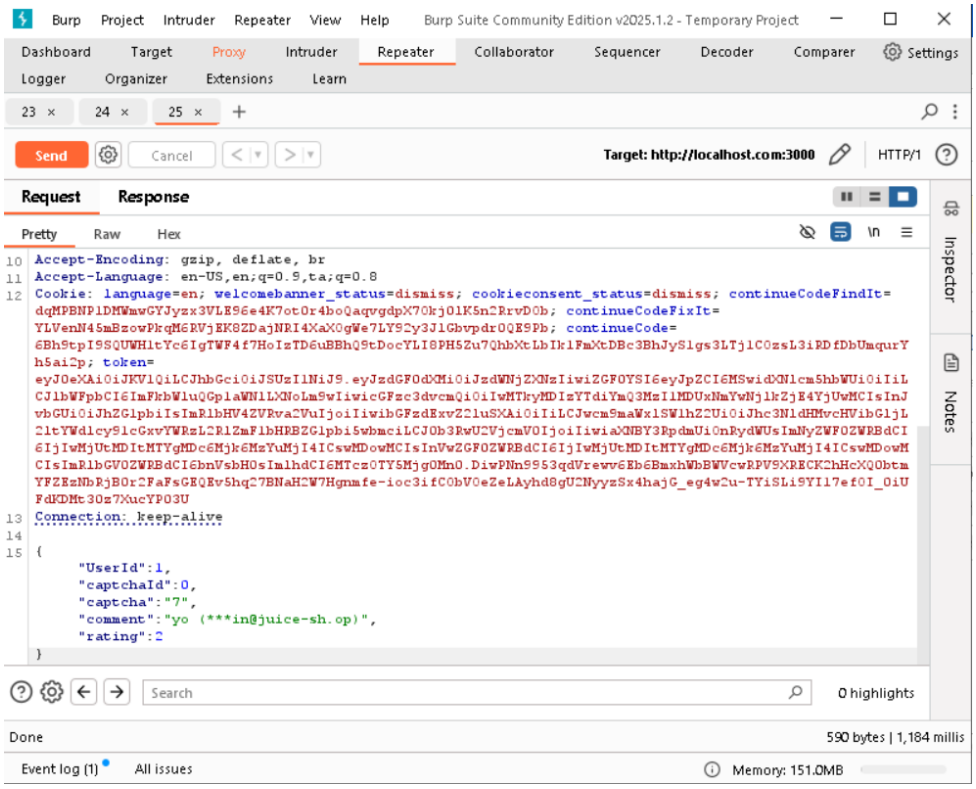


here we can't update the username,

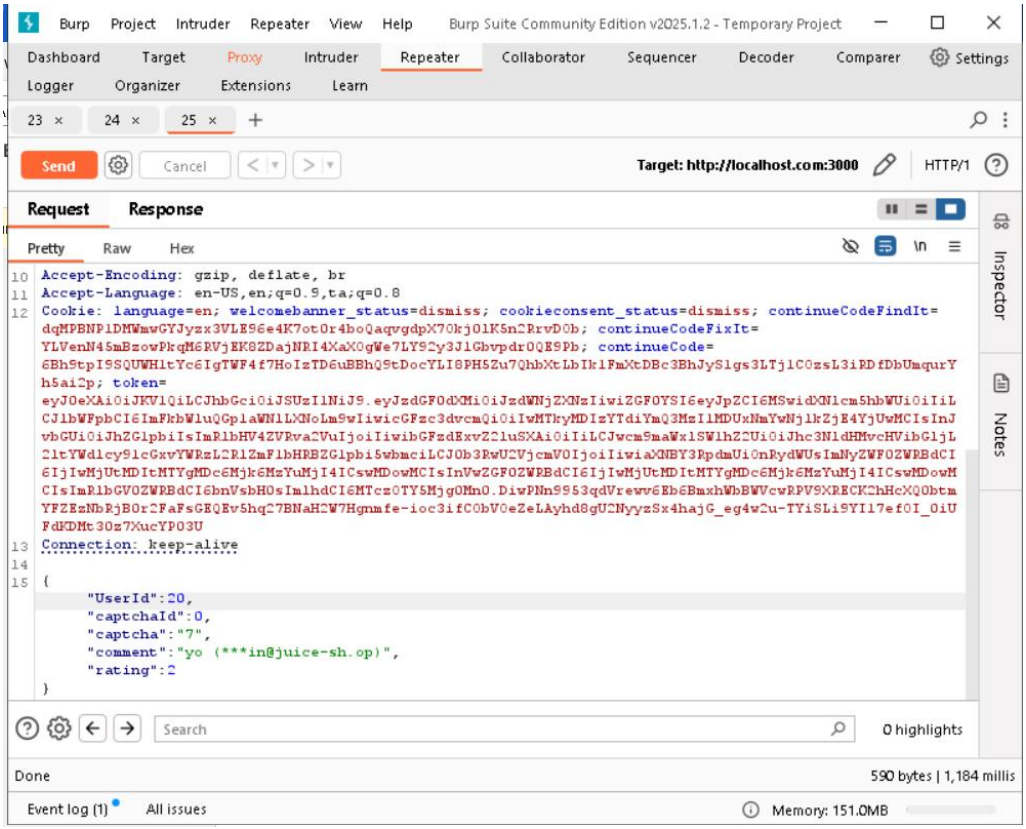
Intercepting the request using burp suite



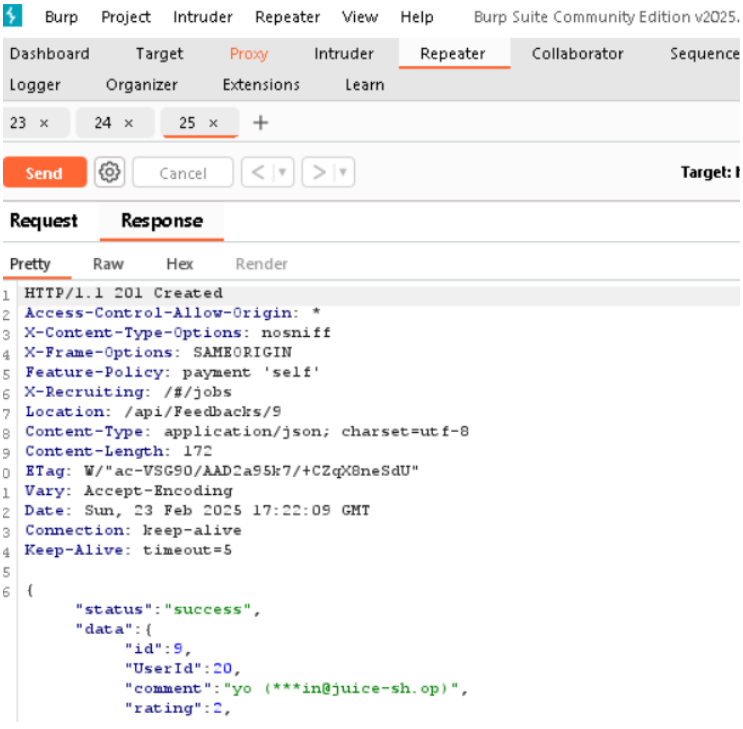
Sending the request to repeater



Changing the UserID from 1 to any other number



and sending the request



The request is success
we successfully forged the feedback exploiting the Broken access control vulnerability

Potential Damage:

By exploiting this vulnerability attackers can send feedback on behalf of other user with their userID

To Prevent:

The Web application should authorize the user properly before executing the request in the server.