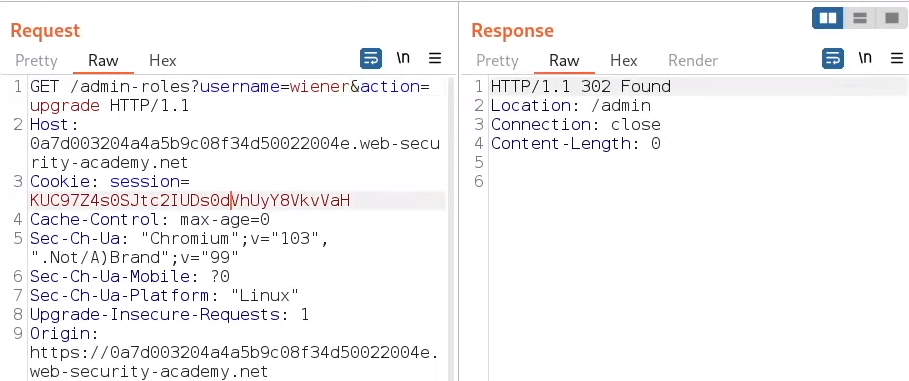
**SCENARIO**

This lab implements access controls based partly on the HTTP method of requests. Familiarize yourself with the admin panel using the credentials administrator:admin. The objective is to log in with the credentials wiener:peter and exploit the flawed access controls to promote yourself to administrator status.

**PROCEDURE**

1. Log in to the application using the administrator credentials (administrator:admin).
2. Navigate to the admin panel and attempt to promote the user 'carlos'.
3. Send the HTTP request for this action to Burp Repeater.
4. Open a private or incognito browser window and log in using the non-administrator credentials (wiener:peter).
5. Using Burp Repeater, attempt to re-promote 'carlos' using the non-admin user's session cookie. Note that the response indicates "Unauthorized".
6. In the Repeater, change the HTTP method of the request from POST to POSTX. Observe the "missing parameter" response.
7. Convert the request to the GET method using Burp Repeater's "Change request method" feature.
8. Modify the 'username' parameter in the request to reflect your username, and resend the request.
9. As a summary: The initial action was logging in as an administrator and trying to promote a user. This request was captured and modified in BurpSuite’s Repeater, changing the POST request to a GET request. Additionally, the session ID was swapped to the administrator's, and the username was changed to the target user's name.

**PAYLOAD**

**PROOF OF CONCEPT**

**REMEDIATION**

1. **Consistent Access Controls:** Ensure that access controls apply consistently across different HTTP methods.
2. **Session Management:** Properly validate session tokens and ensure that actions can't be performed merely by changing the session ID.
3. **Limit HTTP Methods:** Disable unnecessary HTTP methods that the application doesn't require. Ensure that critical actions cannot be performed using methods like GET, which are designed for data retrieval and not actions that change server state.