**SCENARIO**

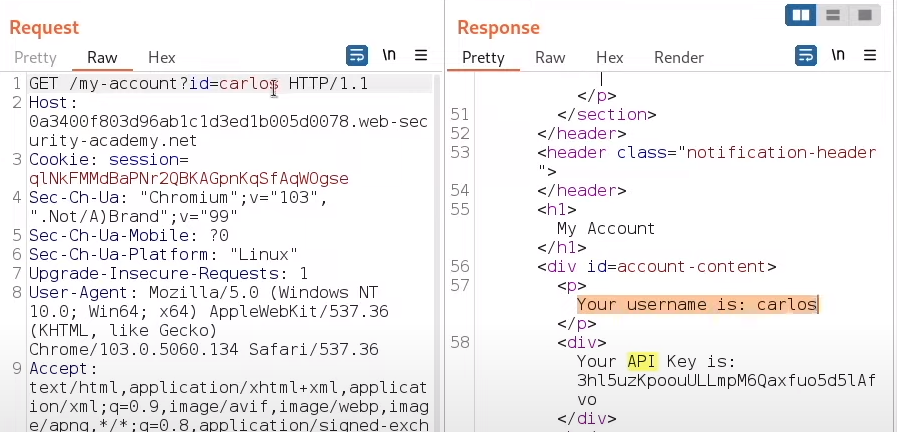
This lab has a horizontal privilege escalation vulnerability on the user account page. The objective is to solve the lab by obtaining the API key for the user 'carlos' and submitting it.

**PROCEDURE**

1. Log in using the provided credentials (wiener:peter) and navigate to the account page.
2. Observe that the URL contains your username in the "id" parameter.
3. Intercept the request using a tool like Burp Suite and send it to the Repeater.
4. In the intercepted request, modify the "id" parameter value from your username to "carlos".
5. Forward the modified request to retrieve the account details of "carlos".
6. Extract the API key for "carlos" from the response.
7. Submit the extracted API key as the solution to the lab.

**PAYLOAD**

Modifying the "id" parameter in the URL or intercepted request to target a different user account, in this case, "id=carlos".

**PROOF OF CONCEPT**

**REMEDIATION**

1. **Parameterized User Data:** Ensure that user data is parameterized, and direct modifications in the URL or request shouldn't change the user context.
2. **Implement Strong Access Controls:** Users should only be able to access their own data. Implement server-side checks to validate whether the authenticated user has the right to access the requested data.
3. **Session Management:** Ensure that session management is robust, and each session is strictly tied to the authenticated user. This will prevent users from accessing data not tied to their session.
4. **Regular Security Audits:** Frequently perform security audits and tests to identify and rectify such vulnerabilities.