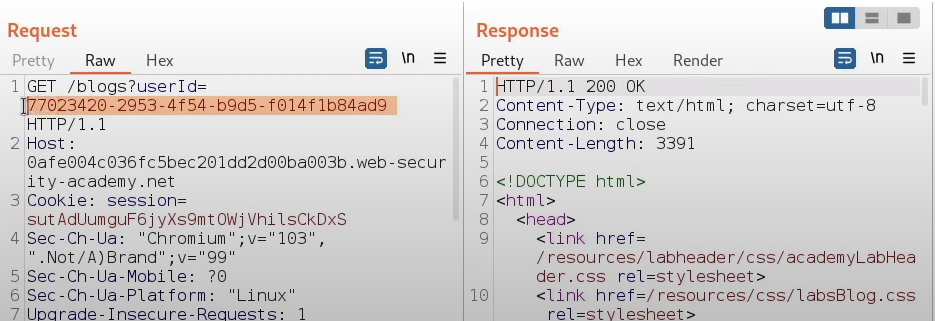
**SCENARIO**

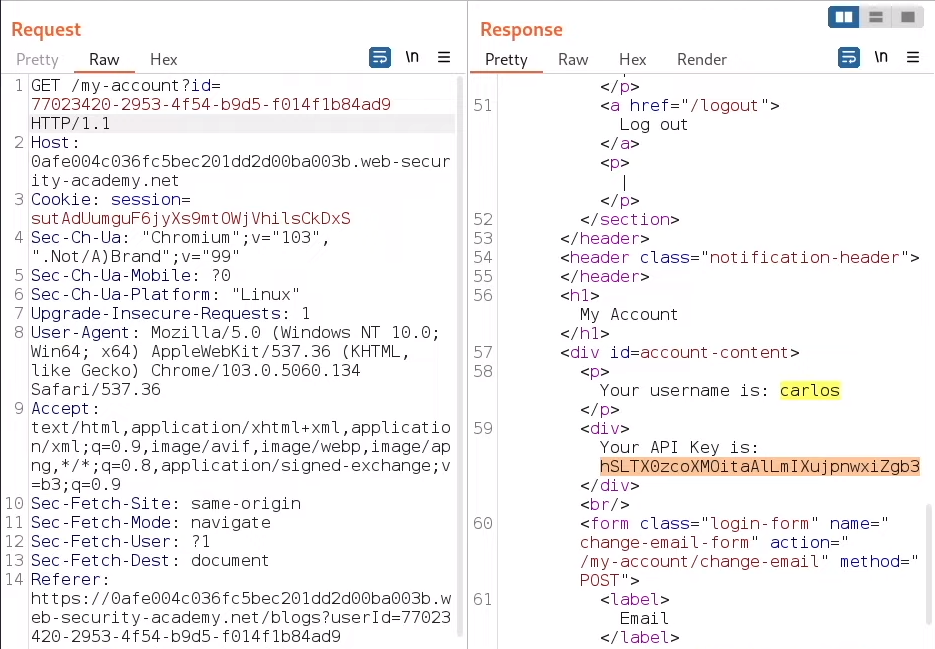
This lab has a horizontal privilege escalation vulnerability on the user account page. However, users are identified using GUIDs. The objective is to find the GUID for 'carlos' and then submit his API key as the solution. Credentials provided for login: wiener:peter.

**PROCEDURE**

1. Locate a blog post authored by 'carlos'.
2. Click on the 'carlos' name or link, leading you to his profile or related page.
3. Observe the URL closely; it should contain a unique identifier, which is the GUID for 'carlos'. Make a note of this GUID.
4. Log into the platform using the provided credentials (wiener:peter) and navigate to your account or profile page.
5. In the URL or request parameters, find the "id" parameter which contains your own GUID.
6. Replace your GUID with the earlier noted GUID of 'carlos'.
7. Access the modified URL or send the modified request. You should now be viewing 'carlos'' account page.
8. Locate and retrieve the API key for 'carlos'.
9. Finally, submit the retrieved API key as the solution to the lab.

**PAYLOAD**

**PROOF OF CONCEPT**

****

**REMEDIATION**

1. **Strong Authorization Checks:** Always ensure that users can only access data that they are authorized to view. Implement backend checks to verify if the user making the request has the necessary permissions.
2. **Avoid Using Predictable IDs:** Consider using unpredictable, random, and long GUIDs/UUIDs for user identifiers. This makes them hard to guess.
3. **Session Management:** Implement robust session management. Ensure that each session is tied to the user's permissions and that session tokens can't be easily manipulated to access other accounts.
4. **Monitoring & Logging:** Keep detailed logs of user activities, especially critical actions. This can help detect and mitigate any unauthorized access attempts.