**SCENARIO**

This lab contains an access control vulnerability where sensitive information is leaked in the body of a redirect response. The objective is to obtain the API key for the user 'carlos' and submit it as the solution.

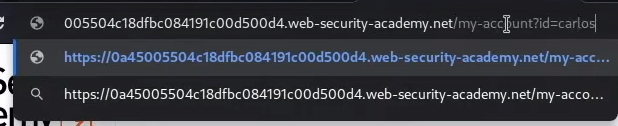
**PROCEDURE**

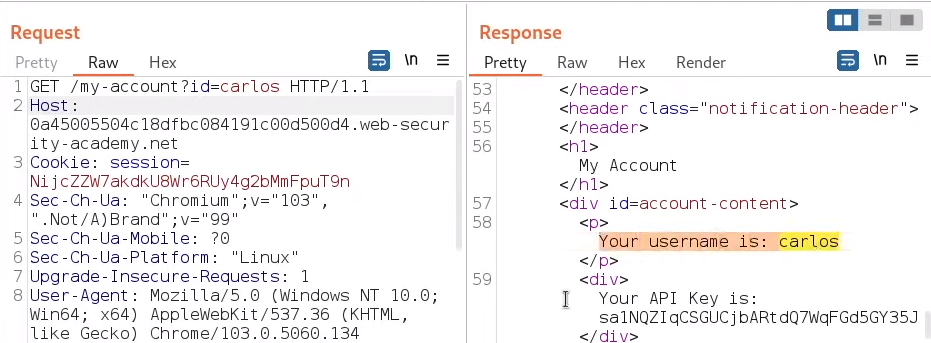
1. Log in to the application using the supplied credentials: wiener:peter.
2. Navigate to your account page.
3. Send the account page request to Burp Repeater.
4. In the Burp Repeater, modify the "id" parameter value to 'carlos'.
5. Analyze the response. Even if it redirects to the home page, check the response body for the API key that belongs to 'carlos'.
6. Extract and submit the discovered API key as the solution.

**PAYLOAD**

The primary payload here involves changing the "id" parameter to target another user, in this case: id=carlos.

**PROOF OF CONCEPT**

****

****

**REMEDIATION**

1. **Ensure Proper Access Control:** Implement access controls to verify that the logged-in user is authorized to view the requested information.
2. **Strip Response Bodies Before Redirects:** Ensure that response bodies containing sensitive data are emptied or stripped before sending a redirect header.
3. **Audit and Monitor:** Regularly audit and monitor server responses to detect and rectify inadvertent data leaks.
4. **Implement Proper Error Handling:** Ensure that errors or unauthorized requests do not lead to the disclosure of sensitive data.