**SCENARIO**

This lab features an admin panel located at /admin. Access to this panel is restricted to users who are logged in and possess a roleid of 2. The goal is to gain access to this admin panel and utilize it to delete the user 'carlos'. For this task, you have access to an account with the credentials: wiener:peter.

**PROCEDURE**

1. Log in to the lab application using the given credentials (wiener:peter).
2. Navigate to your account page within the application.
3. Utilize the available feature to modify the email address associated with your account.
4. Monitor the response of this action, specifically looking for details concerning your user's role ID.
5. Intercept the request responsible for the email modification using a tool like Burp Suite, and send this request to the Burp Repeater tool.
6. Modify the request within Burp Repeater, adding "roleid":2 to the JSON payload in the request body, and resend this modified request.
7. Analyze the response to confirm your roleid has been successfully changed to 2.
8. Navigate to the /admin path within the application.
9. Identify and delete the user 'carlos'.

**PAYLOAD**

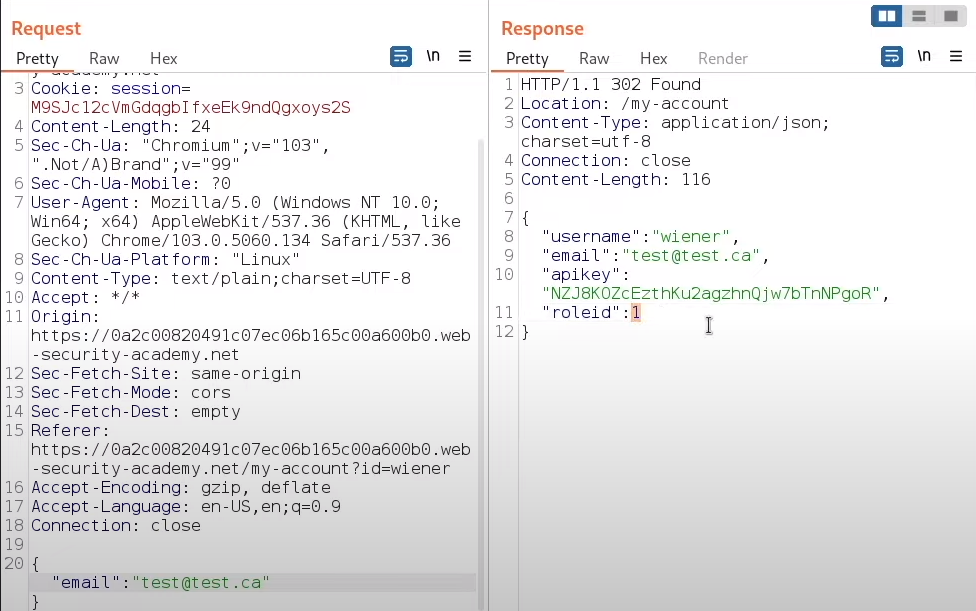
{

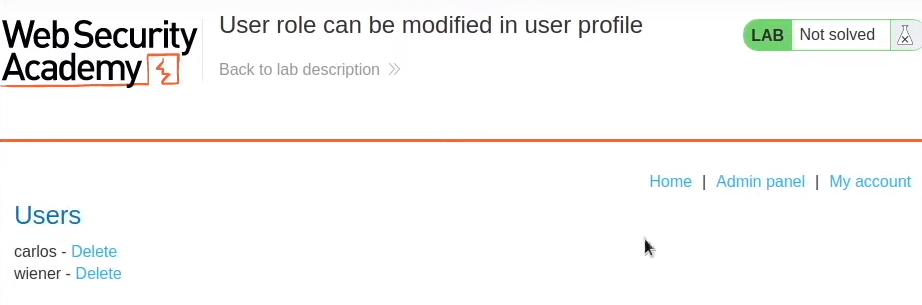
...,

"roleid":2,

...

}

**PROOF OF CONCEPT**

****

**REMEDIATION**

1. **Strict Role Management:** Implement strict checks on the server side for any request modifying user roles. Ensure that users cannot modify their own roles.
2. **Limit Exposure:** Avoid revealing role IDs or any similar sensitive information in client-side responses.
3. **Server-Side Validation:** Always validate and sanitize incoming data on the server side. Ensure that even if data is tampered with on the client side, it does not lead to unintended consequences.
4. **Logging and Monitoring:** Monitor for any suspicious activities or role changes, and notify administrators if an unauthorized change is detected.