**SCENARIO**

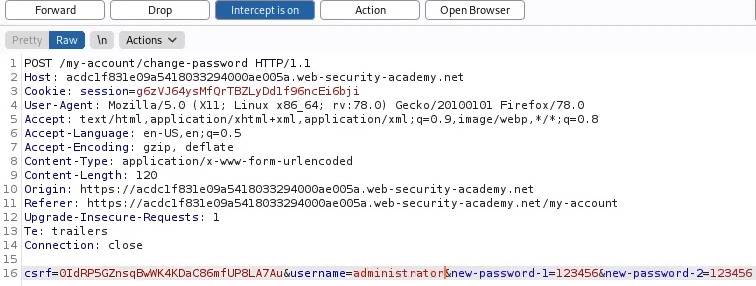
The application assumes that a user's privilege level is determined during the login process. This flawed assumption can be exploited to gain unauthorized administrative access. The goal is to access the admin interface and delete the user 'carlos'.

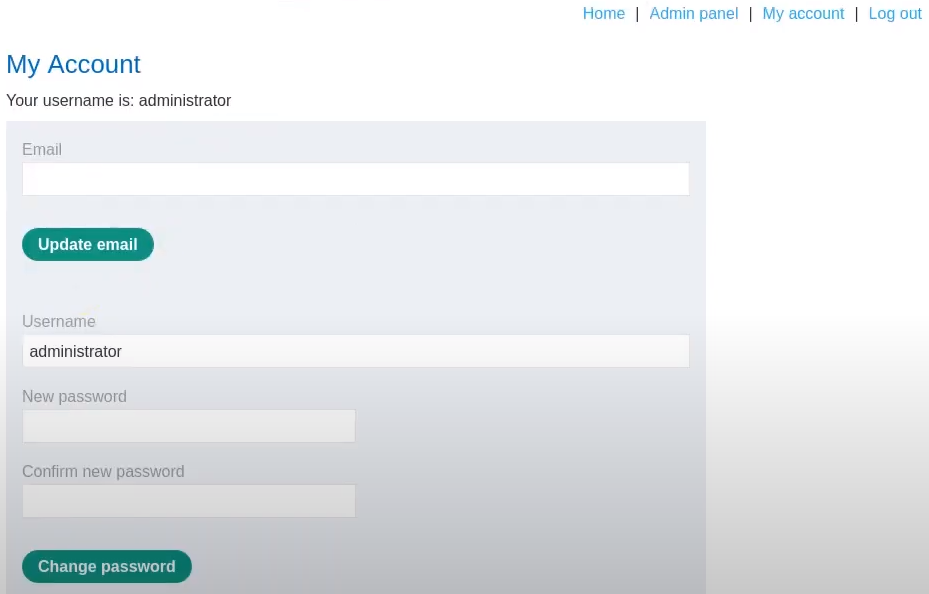
**PROCEDURE**

1. Start Burp Suite and proceed with the login process.
2. Post-login, note the step that requires role selection before landing on the home page.
3. Use the content discovery tool to spot the /admin route.
4. Attempt to navigate directly to /admin from the role selection page, but this fails.
5. Logout, revisit the login page, turn on Burp's proxy interception, and log in again.
6. After intercepting the POST /login request, directly navigate to the lab's home page, where we observe that our role defaults to the administrator role.
7. Use this privilege to access the admin panel and delete the user 'carlos'.

**PAYLOAD**

Intercepted POST /login request to manipulate the navigation sequence.

**  
PROOF OF CONCEPT**

****

**REMEDIATION**

1. **Sequential Flow Verification:** Ensure that the application verifies each step of the user flow for consistency and authenticity.
2. **Strict Role Assignments:** User roles and privileges should be assigned based on verified attributes, not user actions.
3. **Session Verification:** Every session should be verified for consistency at each step to prevent unauthorized deviations.