**SCENARIO**

This lab features an admin panel with a flawed multi-step process for changing a user's role. To understand the workings of the admin panel, log in using the credentials: administrator:admin.

Objective: Using the credentials wiener:peter, exploit the flawed access controls to elevate your permissions and become an administrator.

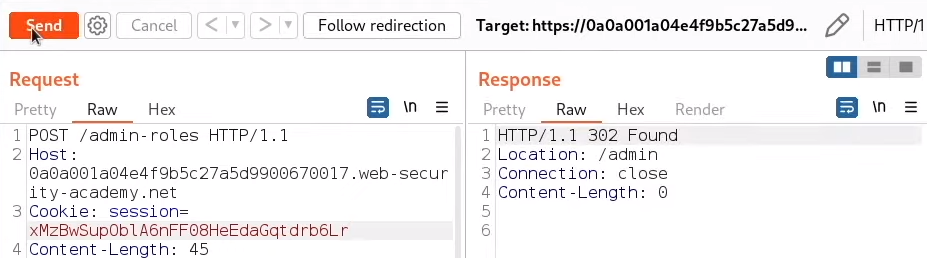
**PROCEDURE**

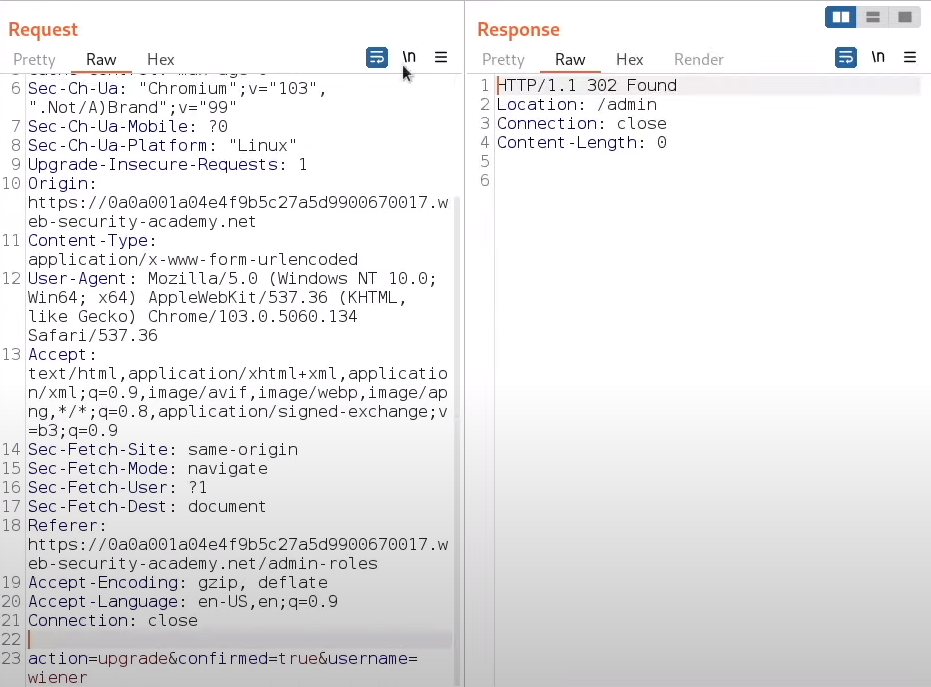
1. Start by logging in with the admin credentials.
2. Navigate to the admin panel and attempt to promote the user 'carlos', then capture the resulting HTTP confirmation request using Burp Suite.
3. Open a private or incognito window in your browser, and sign in with the non-admin credentials (wiener:peter).
4. Extract the session cookie for the non-admin user and replace it in the existing HTTP request captured in Burp Repeater.
5. Modify the username in the request to your non-admin username, then replay the request using Burp Repeater.

**PAYLOAD**

The primary payload involves capturing the HTTP request of an admin promoting a user and replaying it with a non-admin's session cookie, after altering the username.

**PROOF OF CONCEPT**

****

****

**REMEDIATION**

1. **Session Management:** Use secure methods to handle sessions, ensuring they are not easily hijacked or reused.
2. **Implement Secure Access Controls:** Review and strengthen the access control mechanisms, particularly around role-changing functionalities.
3. **Audit and Review:** Periodically review the application's code and functionalities for potential security flaws, and test with tools like Burp Suite.
4. **Multi-Factor Authentication:** Introduce multi-factor authentication, especially for critical actions like role changes.