**SCENARIO**

This lab contains an admin panel located at /admin. The admin panel determines administrator privileges using a forgeable cookie. The objective is to gain access to the admin panel and delete the user 'carlos'. This lab contains an admin panel located at /admin. For testing purposes, we can log into the application using the credentials: wiener:peter.

**PROCEDURE**

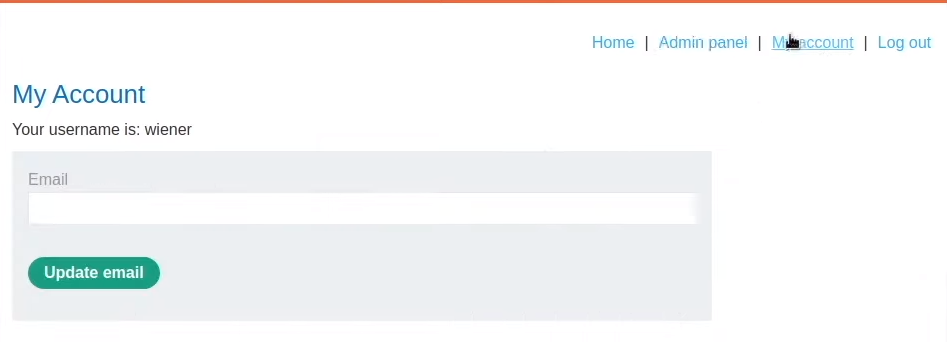
1. Log into the application using the provided credentials: wiener:peter.
2. Navigate to the page or functionality that sends an HTTP request which contains the admin=false cookie.
3. Use BurpSuite's Interceptor to capture the outgoing request.
4. In the intercepted request, modify the cookie value from admin=false to admin=true.
5. Forward the modified request to access the admin panel with elevated privileges.
6. Once in the admin panel, locate and delete the user 'carlos'.

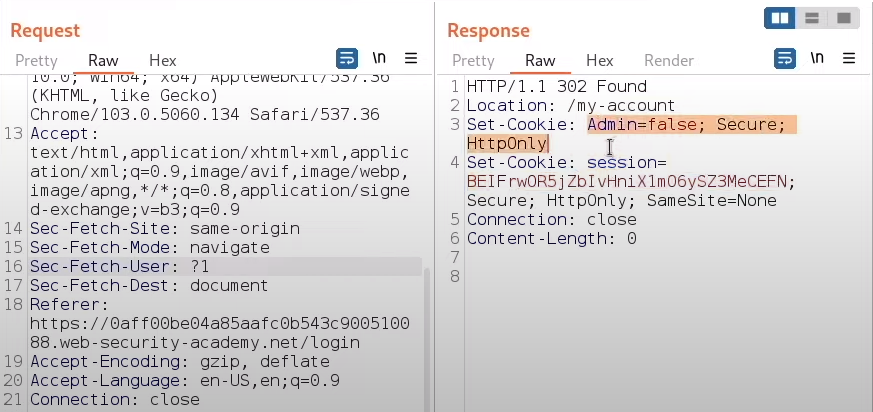
**PAYLOAD**

Modifying the cookie value:

From: admin=false

To: admin=true

**PROOF OF CONCEPT**

****

**REMEDIATION**

1. **Secure Cookie Handling:** Do not rely on client-side cookie values for critical privilege checks. Server-side session management should be used to validate user roles.
2. **Implement Proper Session Management:** Server-side session attributes should be used to determine roles and permissions, rather than relying on client-side data.
3. **Encryption and Signing:** Cookies that store sensitive data or are used for critical operations should be encrypted and signed to prevent tampering.