**SCENARIO**

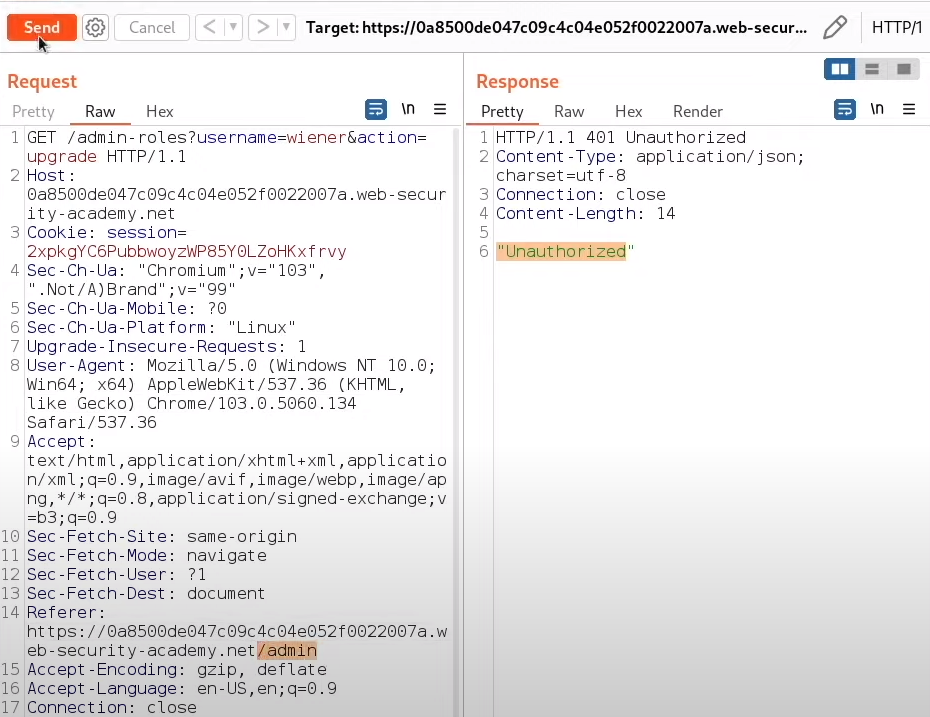
This lab controls access to certain admin functionality based on the Referer header. Users can familiarize themselves with the admin panel by logging in using the credentials administrator:admin. The objective of this lab is to log in using the credentials wiener:peter and exploit the flawed access controls to promote oneself to become an administrator.

**PROCEDURE**

1. Log in using the administrator credentials (administrator:admin).
2. Navigate to the admin panel and choose the option to promote the user 'carlos'. Capture this HTTP request and send it to Burp Repeater.
3. In a separate private/incognito browser window, log in using the non-admin credentials (wiener:peter).
4. Attempt to browse to /admin-roles?username=carlos&action=upgrade. Observe that the request is denied due to the absence of the correct Referer header.
5. In Burp Repeater, replace the session cookie in the previously captured request with the session cookie of the wiener:peter user. Change the 'username' parameter in the request to represent your username, then replay the request.

**PAYLOAD**

**PROOF OF CONCEPT**

****

**REMEDIATION**

1. **Rely on Stronger Access Control Mechanisms:** Do not rely solely on the Referer header for access control as it can be easily manipulated. Implement robust server-side checks.
2. **Session Management:** Ensure each session has proper roles and permissions associated, checked server-side before any sensitive operation.
3. **Audit and Logs:** Regularly audit the access logs for any unauthorized actions and have alarms for suspicious activities.