**SCENARIO**

This website has an unauthenticated admin panel at /admin. A front-end system blocks external access to this path. However, the back-end application is developed on a framework that recognizes the X-Original-URL header. The objective is to solve the lab by accessing the admin panel and deleting the user 'carlos'.

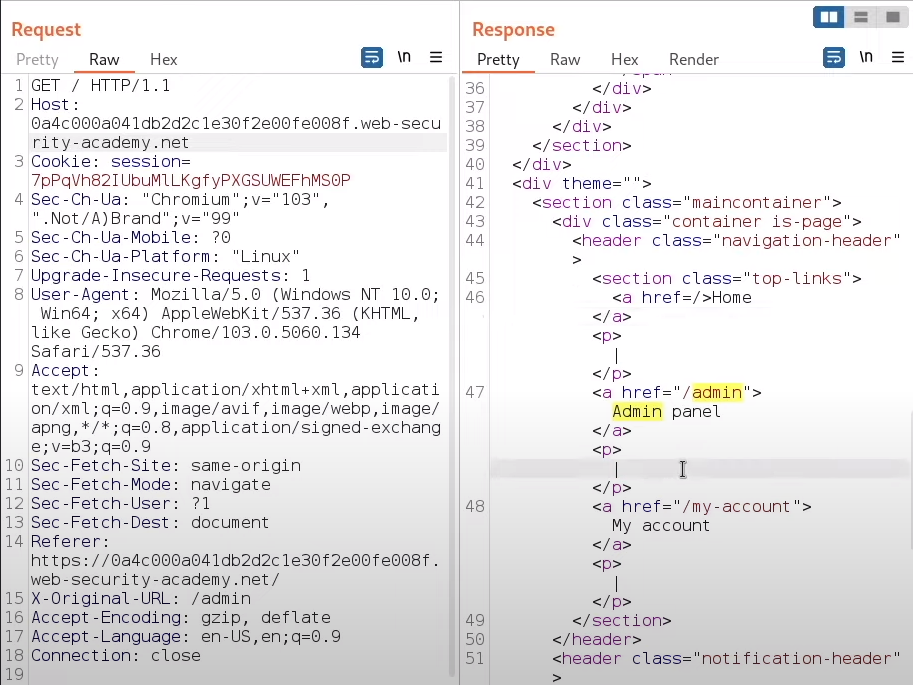
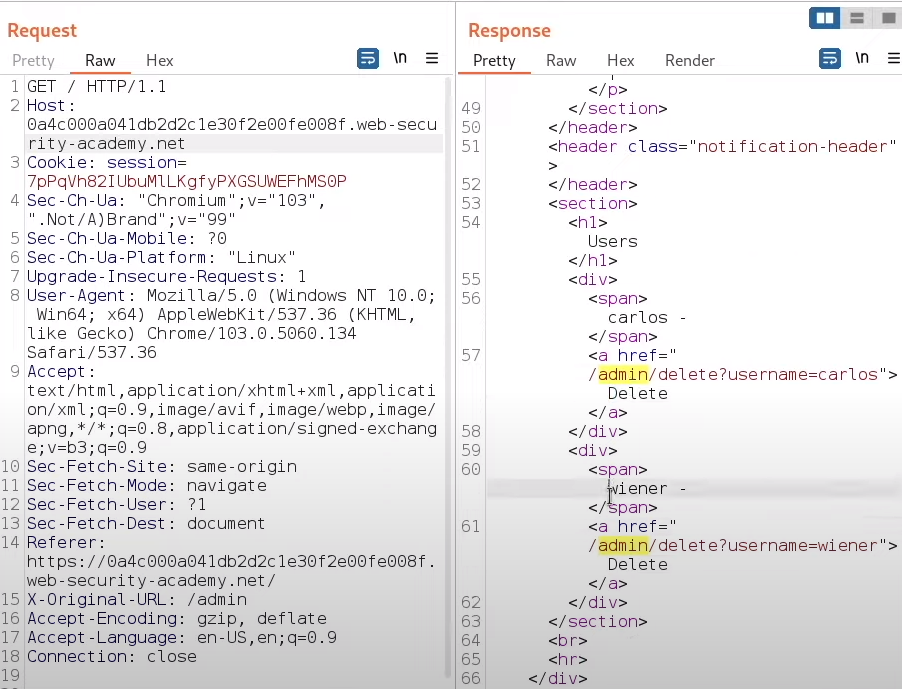
**PROCEDURE**

1. Attempt to load /admin and observe that the access is blocked. The plainness of the response suggests that it may be originating from a front-end system.
2. Forward the request to Burp Repeater. Modify the URL in the request line to / and append the HTTP header X-Original-URL: /invalid. Notice that the application sends back a "not found" response. This hints that the back-end system processes the URL from the X-Original-URL header.
3. Adjust the value of the X-Original-URL header to /admin. You should now be able to access the admin panel.
4. To remove the user 'carlos', append ?username=carlos to the true query string, and modify the X-Original-URL path to /admin/delete.

**PAYLOAD**

1. X-Original-URL: /invalid
2. X-Original-URL: /admin
3. X-Original-URL: /admin/delete?username=carlos

**PROOF OF CONCEPT**

****

**REMEDIATION**

1. **Backend Access Control:** Implement stringent access control on the back-end application to prevent unauthorized access.
2. **Disable Unnecessary Headers:** If not required, disable the support for the X-Original-URL header**.**
3. **Consistent URL Handling:** Ensure both front-end and back-end systems handle URLs consistently and that one can't be manipulated to bypass the other.
4. **Monitoring and Logging:** Keep an eye on unusual patterns and header manipulations in the request logs.