**SCENARIO**

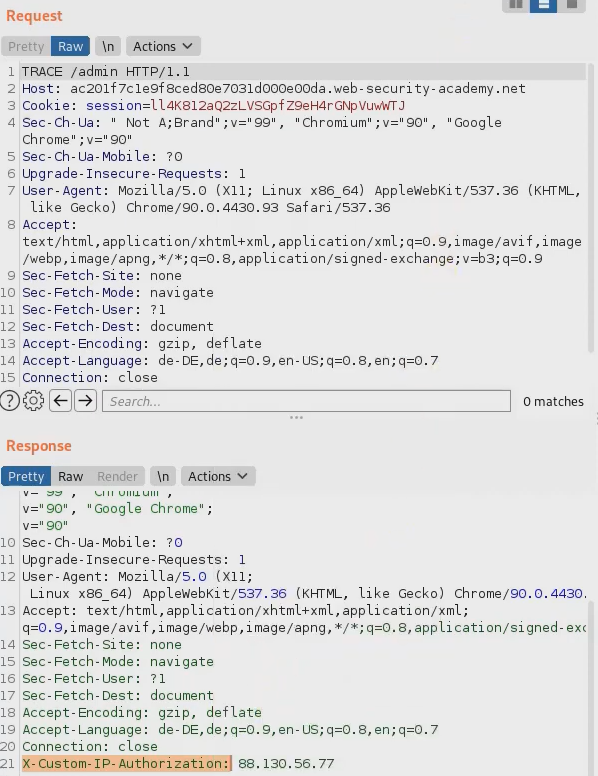
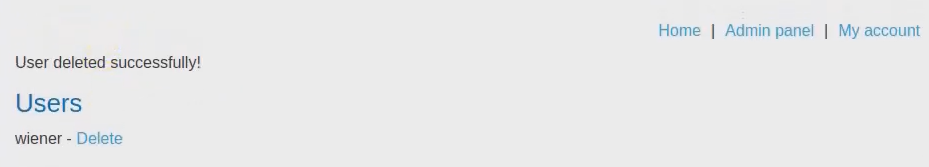
An authentication bypass vulnerability is present in the application's admin panel. It relies on a custom HTTP header, which needs identification.

**PROCEDURE**

1. With Burp's Repeater tool, we attempt to fetch the admin panel through a GET request.
2. Altering the request method to TRACE reveals a custom header, X-Custom-IP-Authorization.
3. Modifying our requests to include this custom header with a localhost IP value allows us unrestricted access to the admin interface.

**PAYLOAD**

Header insertion: X-Custom-IP-Authorization: 127.0.0.1

**PROOF OF CONCEPT  
  
**

**REMEDIATION**

1. **Avoid IP-Based Authentication:** Relying solely on IP addresses for authentication can be insecure.
2. **Validate Custom Headers:** Ensure that custom headers can't be easily manipulated to bypass security measures.
3. **Regularly Review Authentication Mechanisms:** Regularly audit and update authentication mechanisms to fend off bypass vulnerabilities.