**SCENARIO**

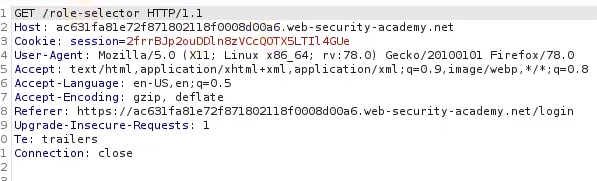
The application’s login procedure has a flaw in its sequence of events. This flaw can be exploited to gain unauthorized administrative access. The aim is to bypass the regular authentication, reach the admin interface, and delete the user 'carlos'.

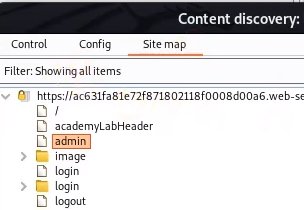
**PROCEDURE**

1. Use Burp Suite, then log in and note the role selection process post-login.
2. Discover the /admin path using the content discovery tool.
3. Log out, revisit the login page, initiate Burp's proxy interception, and log in.
4. Bypass the usual post-login route by dropping the GET /role-selector request and directly navigating to the home page.
5. Observe the default assignment to the administrator role, granting us access to the admin panel.
6. Navigate to the admin panel and proceed to delete the user 'carlos'.

**PAYLOAD**

Dropped GET /role-selector request post-login to manipulate the flow.

**  
PROOF OF CONCEPT**

****

**REMEDIATION**

1. **Role Verification:** Ensure that roles are assigned based on verified attributes and not just the sequence of user actions.
2. **Session Consistency:** Every session should be validated for its consistency at each step, ensuring users can't skip or reorder steps.
3. **Enhanced Logging:** Implement enhanced logging and alert mechanisms for irregular or suspicious behaviours during login and role selection.