**SCENARIO**

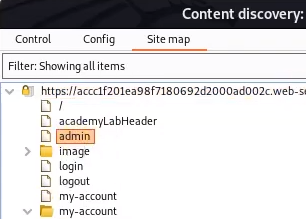
The application's registration process has a logic flaw that doesn't validate email input sufficiently. Exploiting this flaw can grant administrative privileges. The goal is to navigate to the admin panel and delete the user named 'carlos'.

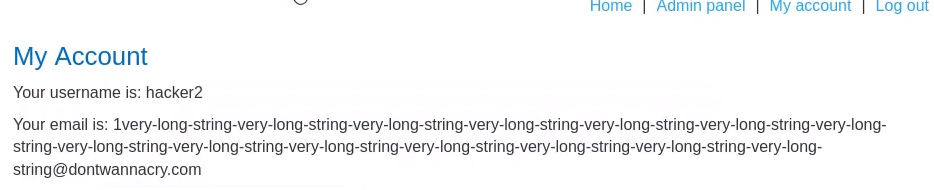
**PROCEDURE**

1. Using Burp, navigate to the lab and discover content to identify hidden routes, spotting the /admin path.
2. Trying to directly access /admin is unsuccessful, but an error message hints that only certain domains have access.
3. Register on the platform, ensuring the email address is exceptionally lengthy and conforms to a particular format.
4. Validate the registration by accessing the linked email client.
5. After logging in with the new account, observe that due to the lengthy email address, the platform truncates the email, which inadvertently grants administrative privileges.
6. Access the admin panel and proceed to delete the user 'carlos'.

**PAYLOAD**

Registration with a specifically formatted elongated email address: extremelylongpattern@desiredsubdomain.domainname

**  
PROOF OF CONCEPT**

****

**REMEDIATION**

1. **Strict Input Validation:** Ensure all registration inputs, especially email addresses, undergo rigorous validation.
2. **Limit Input Length:** Implement character limits to prevent buffer overflows and unintended truncations.
3. **Audit User Privileges:** Regularly review user roles and privileges to detect any anomalies or unauthorized access levels.