**SCENARIO**

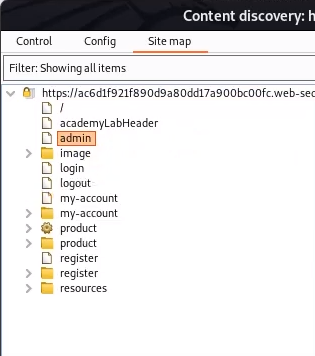
The application inadvertently allows unauthorized users to gain access to administrative functions, revealing sensitive functionalities. The objective is to navigate to the admin panel and delete the user named 'carlos'.

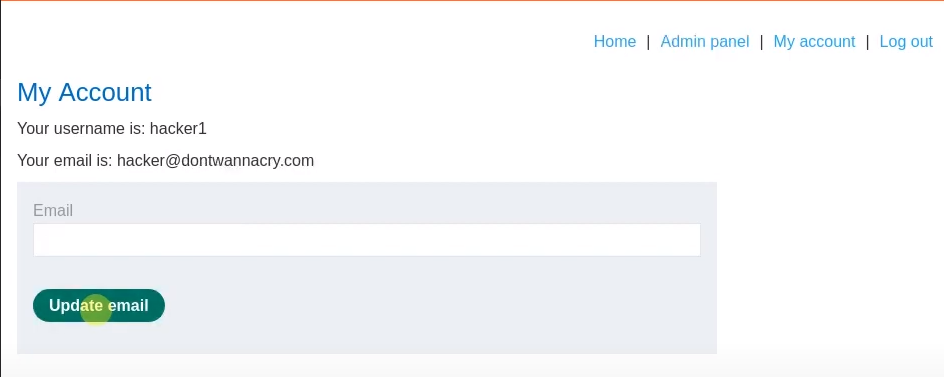
**PROCEDURE**

1. Initialize the lab and navigate to Burp's "Target" > "Site map" tab.
2. Use the content discovery tool to explore hidden paths within the application domain.
3. Identify the /admin route. Attempting direct access yields no results.
4. Register on the application, using a patterned email address, ensuring it resembles an employee email.
5. Validate the email registration by accessing the provided email client.
6. Post-confirmation, log in using the newly registered account. Find that the admin panel is now accessible.
7. Access the admin panel and proceed to delete the user 'carlos'.

**PAYLOAD**

User registration with an email pattern: patternedstring@dontwannacry.com.domainname

**  
PROOF OF CONCEPT**

****

**REMEDIATION**

1. **Role-Based Access Control:** Implement strict role-based access controls ensuring users can only access areas they're authorized for.
2. **Email Validation:** Ensure only valid corporate email addresses have access to sensitive functionalities.
3. **Monitoring & Alerts:** Implement systems to detect and alert on unauthorized access attempts or suspicious behaviours.