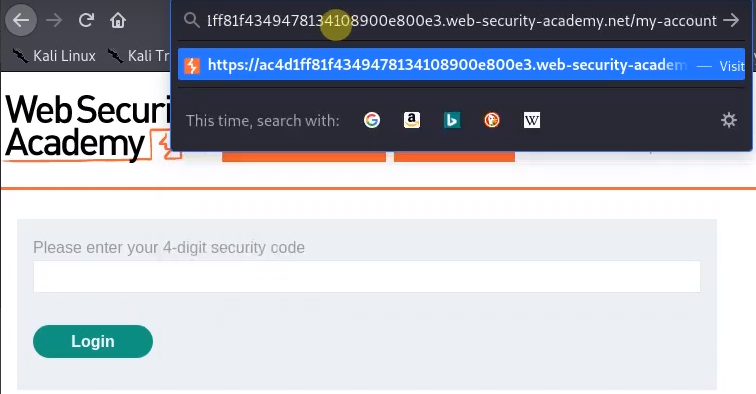
**SCENARIO**

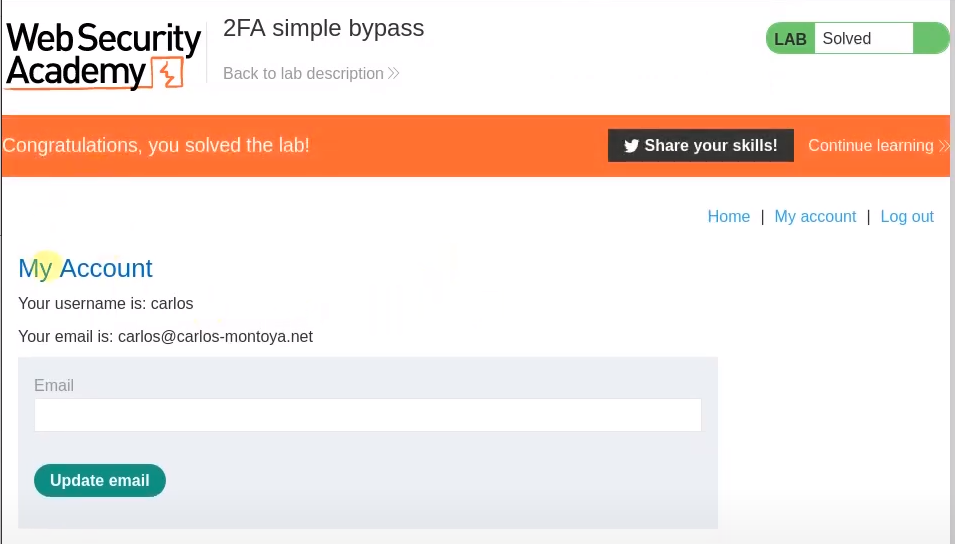
This lab's two-factor authentication mechanism can be bypassed. Although a valid username and password have been obtained, there's no access to the user's 2FA verification code. The goal is to access Carlos's account page without the 2FA code.

**PROCEDURE**

1. Log in to your own account using the credentials: wiener:peter. The 2FA verification code will be sent to your email.
2. Access your emails by clicking the "Email client" button.
3. Navigate to your account page and make note of the URL, particularly the /my-account path.
4. Log out of your account.
5. Log in using the victim's credentials: carlos:montoya.
6. When the system prompts for the 2FA verification code, manually modify the URL to /my-account.
7. Confirm access to the account page; the lab is considered solved when Carlos's account page loads without entering the 2FA code.

**PAYLOAD**

**  
PROOF OF CONCEPT**

****

**REMEDIATION**

1. **Strict 2FA Verification:** Ensure that the 2FA verification process cannot be bypassed by simply changing the URL or path.
2. **Session Handling:** Properly handle user sessions to ensure that users can't access account pages without completing all authentication steps.
3. **Audit and Monitor Logs:** Regularly monitor logs for unusual activities, such as unauthorized account access or suspicious URL changes.