**SCENARIO**

This lab's two-factor authentication (2FA) mechanism has a vulnerability stemming from its flawed logic. The objective is to exploit this flaw to access Carlos's account page without knowing his password. Provided Credentials:

Username: wiener

Password: peter

Victim's Details:

Username: carlos

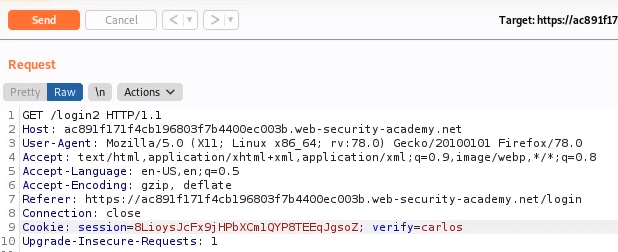
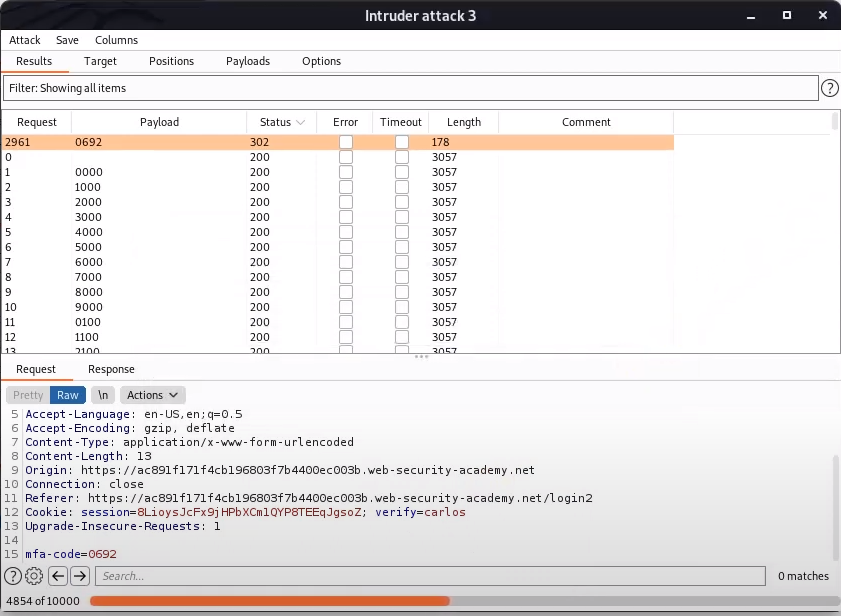
Additional Information: You have access to the email server to receive your 2FA verification code. Carlos will not attempt to log in to the website himself.

**PROCEDURE**

1. With the Burp Suite tool active, log in to your account (wiener:peter) and closely examine the 2FA verification process.
2. Observe that in the POST /login2 request, the "verify" parameter dictates which user account is under access.
3. Log out of your account.
4. Forward the GET /login2 request to Burp's Repeater. Modify the "verify" parameter value to "carlos" and dispatch the request. This action triggers a temporary 2FA code generation for Carlos.
5. Navigate to the login page, provide your username and password (wiener:peter), and input an erroneous 2FA code.
6. Send the POST /login2 request over to Burp Intruder.
7. Within Burp Intruder, adjust the "verify" parameter to "carlos". Next, allocate a payload marker to the "mfa-code" parameter. Use Burp Intruder to brute-force the 2FA code.
8. Once you retrieve the 302 response, load it in your browser.
9. Select the "My account" option to successfully complete the lab.

**PAYLOAD**

Use Burp Intruder to brute-force the 2FA code with potential codes, targeting the "mfa-code" parameter.

**PROOF OF CONCEPT**

**REMEDIATION**

1. **Logic Validation:** Ensure that the 2FA verification logic securely ties a generated code to the user who initiated the request, preventing malicious users from bypassing this security layer.
2. **Rate Limiting:** Implement rate limiting on the 2FA verification endpoint to prevent brute-force attacks.
3. **Monitoring & Alerts:** Monitor for unusual or repeated failed attempts at 2FA verification and alert administrators or temporarily block suspicious users.