**SCENARIO**

This lab is susceptible to exploitation due to a logic flaw in its password brute-force protection. The objective is to brute-force the victim's password, subsequently log in, and then access their account page. While some advanced users might employ a macro or the Turbo Intruder extension, the lab can be solved without these features. Credentials provided:

Username: wiener

Password: peter

Victim's username: carlos

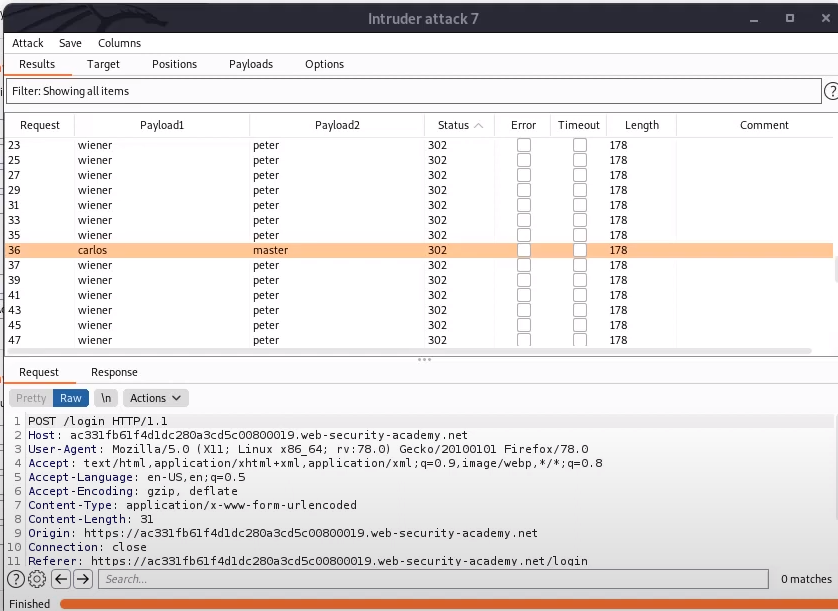
Candidate passwords are provided.

**PROCEDURE**

1. Launch Burp and navigate to the login page. Note that after three consecutive incorrect login attempts, the IP is temporarily blocked. Yet, by logging into your own account prior to this limit, the counter for failed login attempts can be reset.
2. Input an incorrect username and password, and forward the POST /login request to Burp Intruder. Configure a pitchfork attack targeting both the username and password parameters.
3. In the 'Resource pool' tab, include the attack in a resource pool with 'Maximum concurrent requests' capped at 1. This ensures that the login attempts reach the server in the intended sequence.
4. Head to the 'Payloads' tab and pick payload set 1. Add a sequence of payloads alternating between your username and 'carlos'. Ensure your username leads and 'carlos' is listed at least 100 times.
5. Modify the candidate passwords list, integrating your password before each candidate. Confirm that your password corresponds with your username in the opposite list.
6. Integrate this list into payload set 2 and initiate the attack.
7. Once the attack concludes, adjust the results filter to exclude 200 status code responses. Organize the remaining results by username. Only one 302 responses should remain for requests using the username 'carlos'. Document the password located in the 'Payload 2' column.
8. Authenticate into Carlos's account with the discovered password and access his account page to complete the lab.

**PAYLOAD**

**PROOF OF CONCEPT**

****

**REMEDIATION**

1. **Enhanced Brute-Force Protection:** Update the brute-force protection logic to block attempts after a certain number of failures, regardless of successful logins in between.
2. **Rate Limiting:** Implement rate limiting to prevent rapid succession of login attempts.
3. **Multi-Factor Authentication:** Incorporate multi-factor authentication (MFA) to bolster security, making brute-force attempts more challenging.
4. **Monitor and Alert:** Set up monitoring to trigger alerts for unusual login patterns, which can signal brute-force attempts.