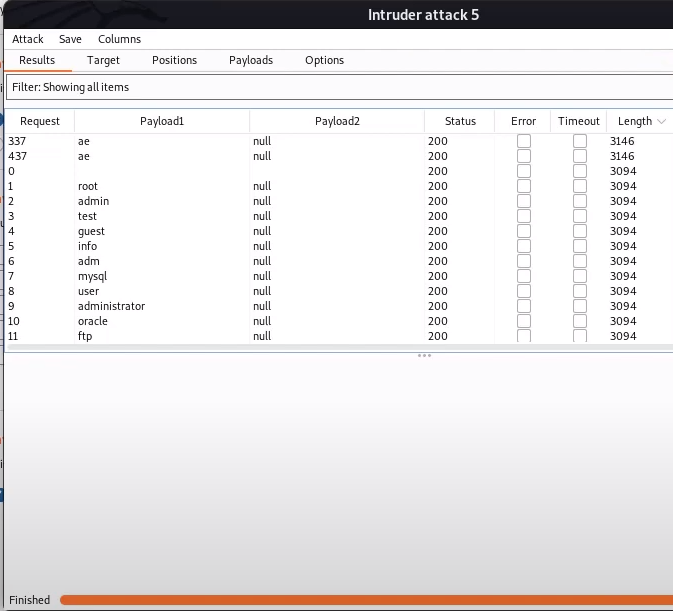
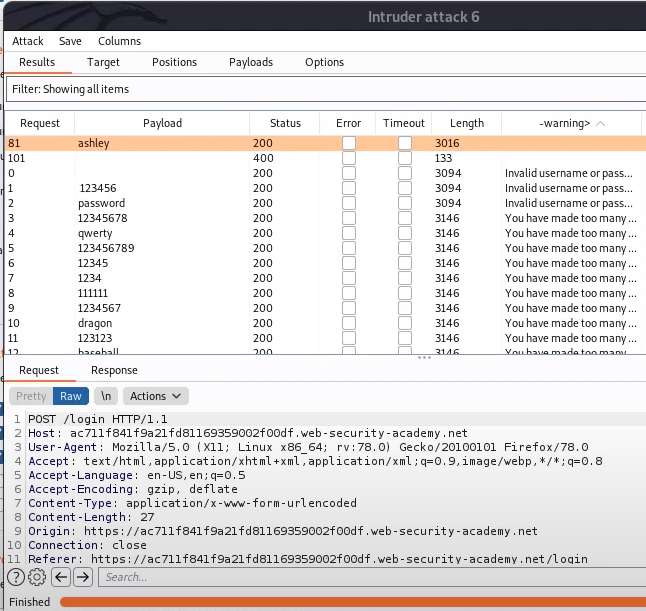
**SCENARIO**

This lab is vulnerable to username enumeration. It uses account locking, but this contains a logic flaw. The objective is to enumerate a valid username, brute-force this user's password, and then access their account page. Candidate usernames and passwords are given.

**PROCEDURE**

1. With Burp Suite running, navigate to the login page and attempt a login using an invalid username and password. Send the POST /login request to Burp Intruder.
2. In Burp Intruder, choose the "Cluster bomb" attack type. Set a payload position for the username parameter. Add a blank payload position at the end of the request body by clicking "Add §" twice. The input should resemble:
3. username=§invalid-username§&password=example§§
4. On the Payloads tab, input the list of candidate usernames for the first payload set. For the second payload set, opt for the "Null payloads" type and generate 5 payloads. This action will effectively repeat each username 5 times. Start the attack.
5. Examine the attack results. Identify a username that has longer responses compared to the others. This particular response should have a unique error message indicating multiple incorrect login attempts. Record this username.
6. Initiate a new Burp Intruder attack on the POST /login request, this time opting for the "Sniper" attack type. Use the previously identified username and set a payload position for the password parameter.
7. Integrate the list of candidate passwords into the payload set. Establish a grep extraction rule aligned with the error message. Begin the attack.
8. Review the results, particularly the grep extract column. Though multiple error messages will be present, identify the response lacking an error message. Record this password.
9. Wait for approximately one minute to allow the account lock to reset.
10. Use the enumerated username and password to log in. Access the user account page to complete the lab objective.

**PAYLOAD**

**PROOF OF CONCEPT**

**REMEDIATION**

1. **Error Message Consistency:** Ensure error messages are consistent regardless of whether it's an incorrect username or password to prevent username enumeration.
2. **Limit Login Attempts:** Introduce an efficient account lockout mechanism that doesn't allow attackers to easily determine valid usernames.
3. **Implement CAPTCHA:** Introduce CAPTCHA on the login page after a set number of failed attempts. This can deter automated brute-force attacks.
4. **Account Lockout Notification:** Notify users via email when their account is locked due to multiple incorrect login attempts.