**SCENARIO**

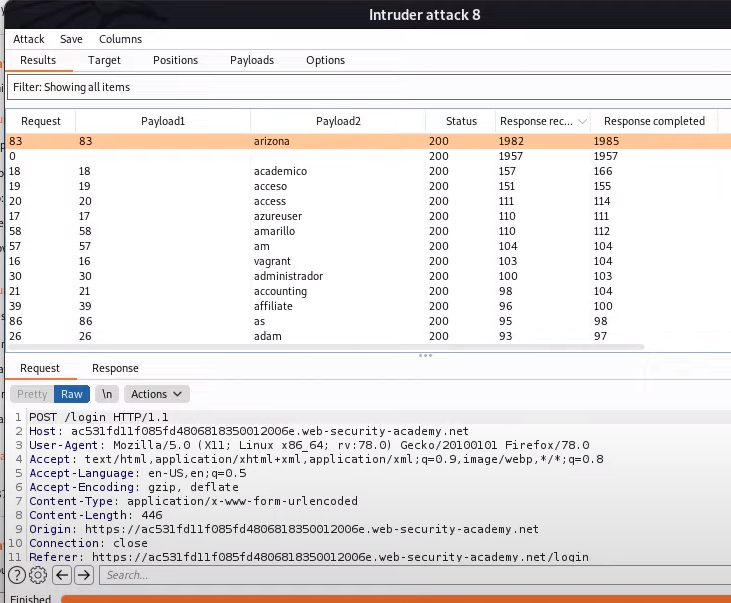
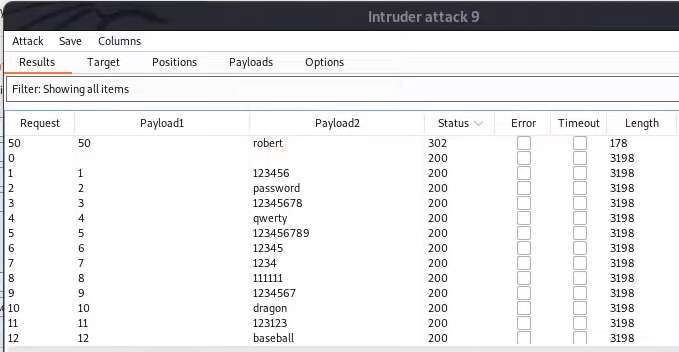
This lab is vulnerable to username enumeration through its response times. To complete the lab, the objective is to enumerate a valid username, brute-force this user's password, and then access their account page. The lab also implements IP-based brute-force protection, but it can be bypassed by manipulating HTTP request headers.

**PROCEDURE**

1. Start Burp and submit an invalid username and password, forwarding the POST /login request to Burp Repeater.
2. Experiment with different usernames and passwords. Be aware that repeated invalid attempts will result in your IP being blocked.
3. Recognize that the lab supports the X-Forwarded-For header, which can be used to spoof the IP and bypass brute-force protection.
4. As you experiment with usernames and passwords, observe the response times. A longer response time with your username indicates its validity.
5. Send the request to Burp Intruder and choose the 'Pitchfork' attack type. Incorporate the X-Forwarded-For header into your requests.
6. Configure payload positions for both the X-Forwarded-For header and the username parameter. Set a long string (around 100 characters) for the password.
7. For payload set 1, choose the 'Numbers' type and range it from 1 to 100 to spoof your IP. In payload set 2, add the list of potential usernames and start the attack.
8. Post-attack, examine response times to identify a valid username by noticing significantly longer times.
9. Launch another Burp Intruder attack for the same request, adding the X-Forwarded-For header. Use the identified username and set the password parameter for brute-forcing.
10. For the new attack, use numbers in payload set 1 and potential passwords in payload set 2. Start the attack.
11. Look for a response with a 302 status to identify the correct password.
12. Use the identified username and password to log in and access the user account page to complete the lab.

**PAYLOAD**

1. List of candidate usernames for enumeration.
2. List of candidate passwords for brute-force attack.

**  
PROOF OF CONCEPT**

**REMEDIATION**

1. **Block X-Forwarded-For Manipulation:** Prevent IP spoofing by rejecting or ignoring X-Forwarded-For headers from untrusted sources.
2. **Add Anti-automation Measures:** Implement CAPTCHAs or other anti-automation mechanisms after repeated failed login attempts.
3. **Consistent Response Times:** Ensure the application response times are consistent, regardless of input, to prevent timing attacks.
4. **Limit Login Attempts:** Implement an account lockout mechanism after a certain number of failed login attempts.
5. **Monitor and Alert:** Set up alerts for multiple failed logins from different IP addresses in a short span of time, which might indicate an attack.