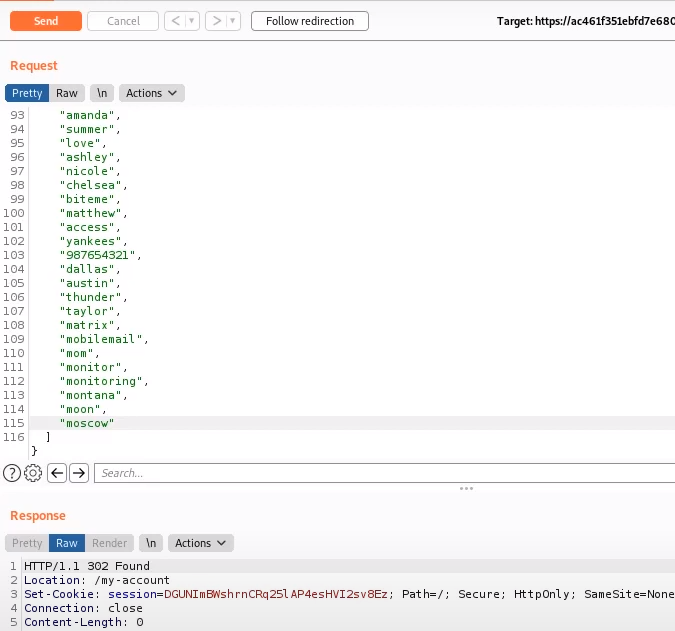
**SCENARIO**

This lab has a vulnerability stemming from a logic flaw in its brute-force protection mechanism. The objective is to exploit this flaw to brute-force Carlos's password and subsequently access his account page.

**PROCEDURE**

1. Navigate to the login page of the lab.
2. Initiate a brute-force attack targeting Carlos's account using various password combinations.
3. Victim's username: carlos
4. Monitor responses to identify when a successful login is achieved.
5. Upon successful brute-forcing, use the correct password to log in as 'carlos'.
6. Access Carlos's account page.

**PAYLOAD**

**PROOF OF CONCEPT**

**REMEDIATION**

1. **Implement Proper Brute-Force Protection:** Ensure mechanisms like account lockouts, CAPTCHAs, or progressive delays after consecutive failed attempts are in place.
2. **Use Multi-Factor Authentication:** Incorporate a secondary method of authentication beyond just a password.
3. **Rate Limiting:** Implement rate limiting on login attempts to slow down and potentially block rapid-fire login attempts.
4. **Monitoring and Alerts:** Set up system alerts for multiple failed login attempts from the same IP or for the same user.