SCENARIO

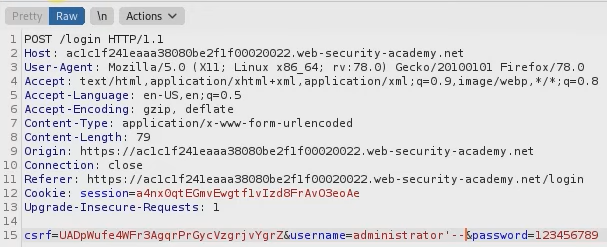
The login function of our application is exposed to SQL injection, potentially allowing unauthorized access.

**PROCEDURE**

1. Start Burp Suite and capture the login request.
2. Modify the username parameter to be administrator'-- and leave the password field blank.
3. Submit the request, aiming to be authenticated as the administrator.

**PAYLOAD**

administrator'--

**PROOF OF CONCEPT**

**REMEDIATION**

1. Utilize parameterized SQL queries to handle user inputs.
2. Establish strong input validation routines.
3. Implement rate limiting and account lockout mechanisms for failed login attempts.
4. Conduct regular security reviews and penetration testing.
5. Use a web application firewall (WAF) to recognize and block common attack patterns.