**SCENARIO**

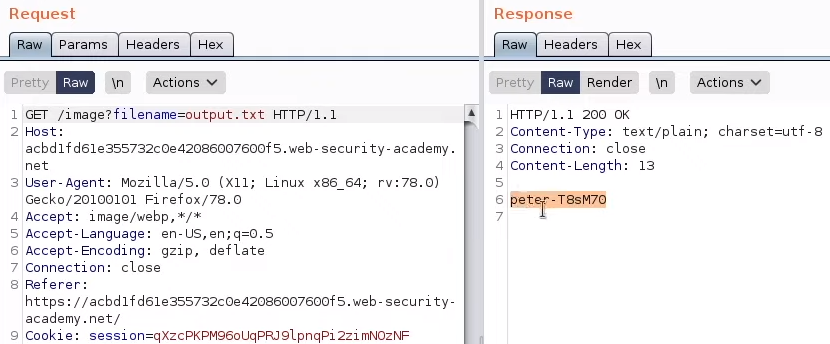
A blind OS command injection vulnerability is present in the feedback mechanism. The output isn't directly visible, but it's possible to redirect it to a location we can access. The objective is to retrieve the output of a command.

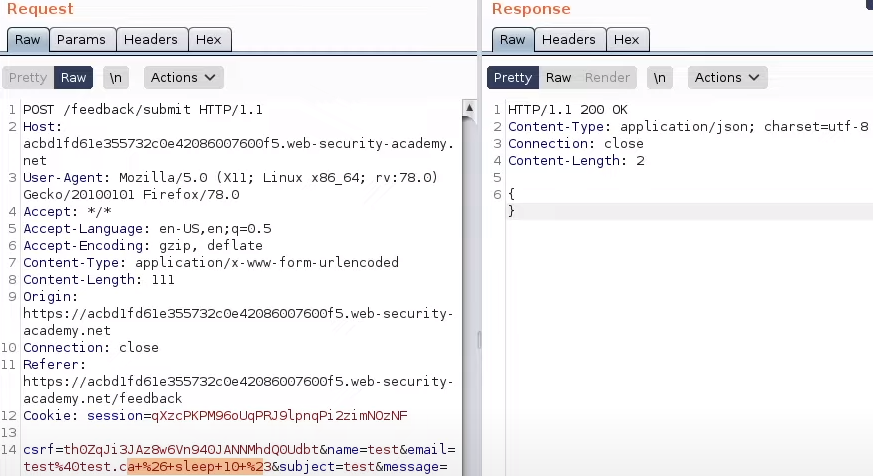
**PROCEDURE**

1. Intercept the request for feedback submission using Burp Suite.
2. Modify the email parameter to inject our desired command.
3. Access the product's image route, trying to retrieve the file into which we redirected our output.

**PAYLOAD**

For the email parameter: ||whoami>/var/www/images/output.txt||

**  
PROOF OF CONCEPT**

****

**REMEDIATION**

1. Validate, sanitize, and parameterize inputs rigorously.
2. Ensure system commands aren't influenced by user inputs.
3. Regularly monitor and audit system commands executed by the application.