**SCENARIO**

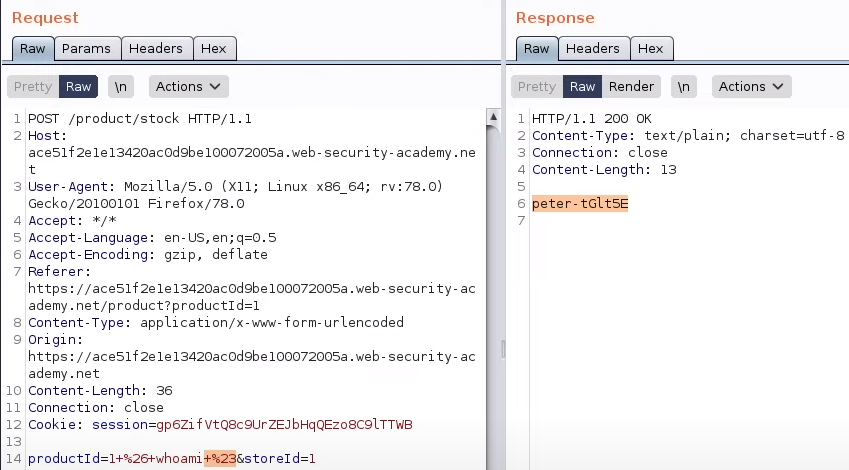
The application seems to have an OS command injection vulnerability within the stock checker feature. By leveraging this vulnerability, commands are executed by manipulating user input. The objective is to find out the name of the current system user.

**PROCEDURE**

1. Capture the stock level check request using Burp Suite.
2. Modify the storeID parameter to integrate the command we aim to execute.
3. Analyze the response to find evidence of the executed command.

**PAYLOAD**

For the storeID parameter: 1|whoami

**  
PROOF OF CONCEPT  
  
REMEDIATION**

1. Always avoid allowing user inputs in system commands.
2. If needed, use safe APIs that can parameterize command inputs.
3. Input validation and sanitization should be applied rigorously.