**SCENARIO**

The current lab setup allows a path traversal vulnerability during the process of displaying product images. This might permit unauthorized access to system files.

**PROCEDURE**

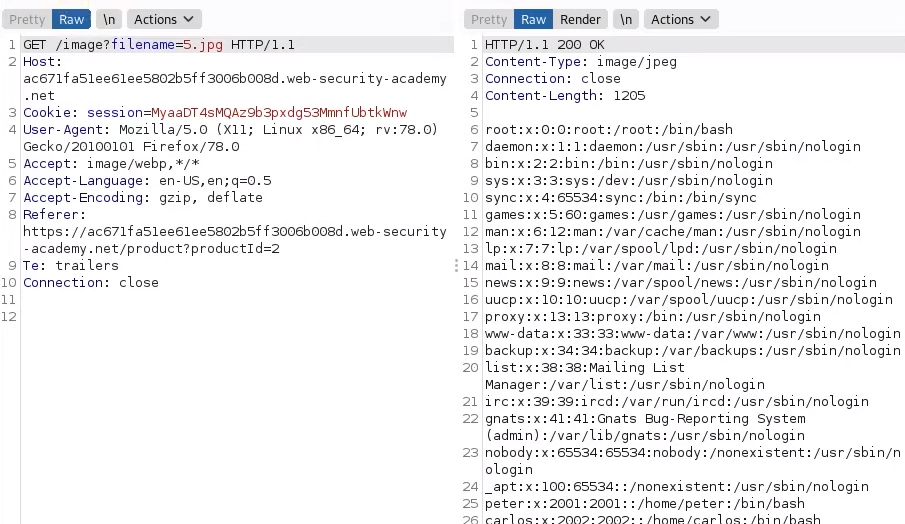
1. Set up Burp Suite and capture a request that's pulling a product image.
2. Alter the filename parameter to:

../../../etc/passwd

1. Evaluate the returned response, ensuring it reveals the /etc/passwd file's contents.

**PAYLOAD**

filename=../../../etc/passwd

**  
PROOF OF CONCEPT**

**REMEDIATION**

1. Implement stringent validation and sanitation measures for all inputs.
2. Define a strict whitelist of permissible file paths.
3. Use a web application firewall to detect and thwart traversal patterns.