**SCENARIO**

The lab's system for displaying product images has a vulnerability. It mandates that user-supplied filenames must end with the correct file extension. However, this check can be bypassed.

**PROCEDURE**

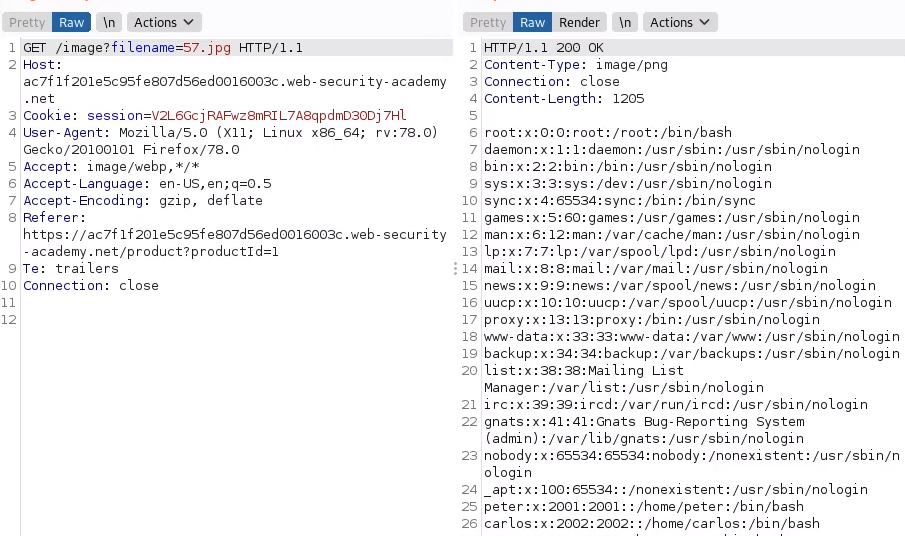
1. Activate Burp Suite and grab a request targeting a product image display.
2. Update the filename parameter to:

../../../etc/passwd%00.png

1. Analyze the output response to see if it outputs the details from the /etc/passwd file.

**PAYLOAD**

Using a previously captured confirmation POST request.

**  
PROOF OF CONCEPT**

**REMEDIATION**

1. Ensure file paths and names are determined by the application, not user input.
2. Implement a whitelist of approved file extensions and reject any that don't match.
3. Educate development staff on null byte injection and its risks.