**SCENARIO**

The lab's method of showing product images is flawed. Although it blocks direct path traversal sequences, there's an oversight in how it processes user-supplied filenames.

**PROCEDURE**

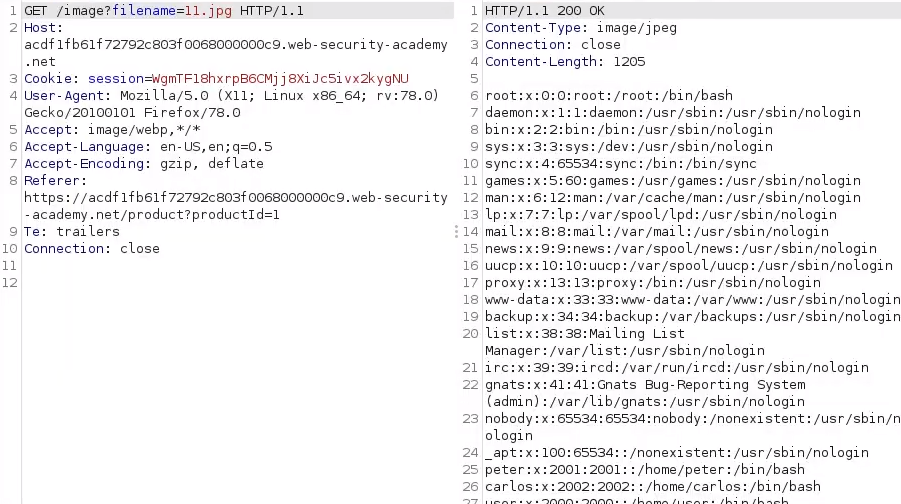
1. With Burp Suite active, intercept a request meant for retrieving a product image.
2. Change the filename parameter to:

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

1. Review the returned response, confirming that it indeed reveals the contents of the /etc/passwd file.

**PAYLOAD**

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

**  
PROOF OF CONCEPT**

**REMEDIATION**

1. Limit the potential paths accessible by the application, ensuring critical system files are unreachable.
2. Adopt a secure coding practice that always processes user inputs as untrusted data.
3. Regularly conduct security audits and vulnerability assessments to detect and patch weaknesses.