**SCENARIO**

The lab demonstrates a vulnerability within its product image display feature. Direct path traversal sequences are blocked, but it considers filenames in relation to a preset directory.

**PROCEDURE**

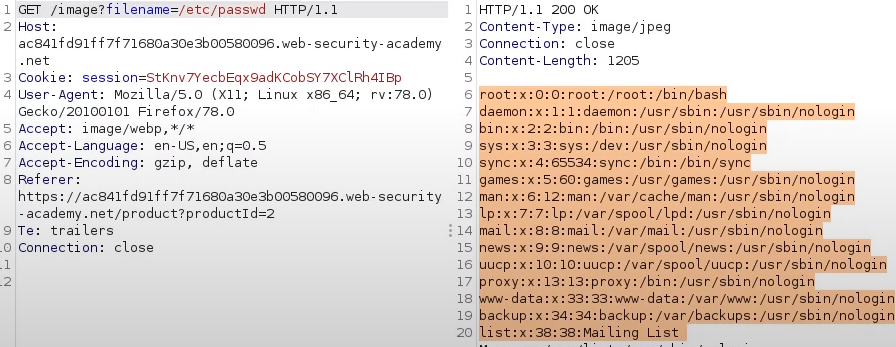
1. Initialize Burp Suite, then intercept a request tasked with displaying a product image.
2. Modify the filename parameter to:

/etc/passwd

1. Check the subsequent response to ascertain it displays the contents of the /etc/passwd file.

**PAYLOAD**

filename=/etc/passwd

**  
PROOF OF CONCEPT**

**REMEDIATION**

1. Ensure all inputs are strictly validated against a known set of safe values.
2. Reject any input containing file paths, ensuring file access is based on permissible criteria, not user inputs.
3. Monitor application logs for unusual file access patterns and block IPs showing malicious intent.