**SCENARIO**

The lab holds a vulnerability when showcasing product images. Path traversal sequences are filtered out from user input, but a subsequent URL-decoding stage reintroduces the risk.

**PROCEDURE**

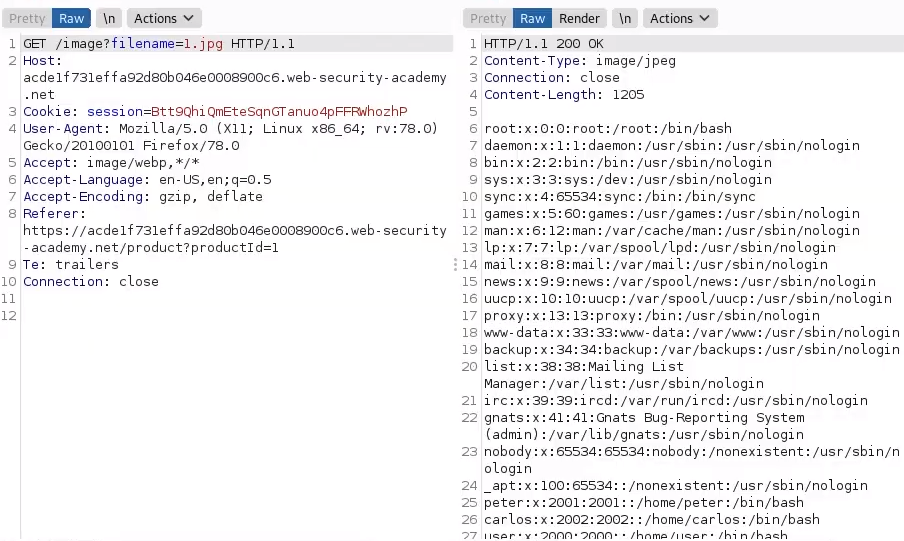
1. Engage Burp Suite and snag a request that fetches a product image.
2. Edit the filename parameter to:

..%252f..%252f..%252fetc/passwd

1. Observe the response, ensuring that it presents the contents of the /etc/passwd file.

**PAYLOAD**

filename=..%252f..%252f..%252fetc/passwd

**  
PROOF OF CONCEPT**

**REMEDIATION**

1. Ensure all sanitization procedures happen post-decoding to prevent manipulation of encoded sequences.
2. Implement logging and monitoring for suspicious requests or anomalous patterns.
3. Educate development teams on secure coding practices, emphasizing the importance of order in input processing.