**SCENARIO**

The lab has a weakness in its product image display mechanism. The full file path is transmitted via a request parameter, with only basic checks to see if the path begins with an expected directory.

**PROCEDURE**

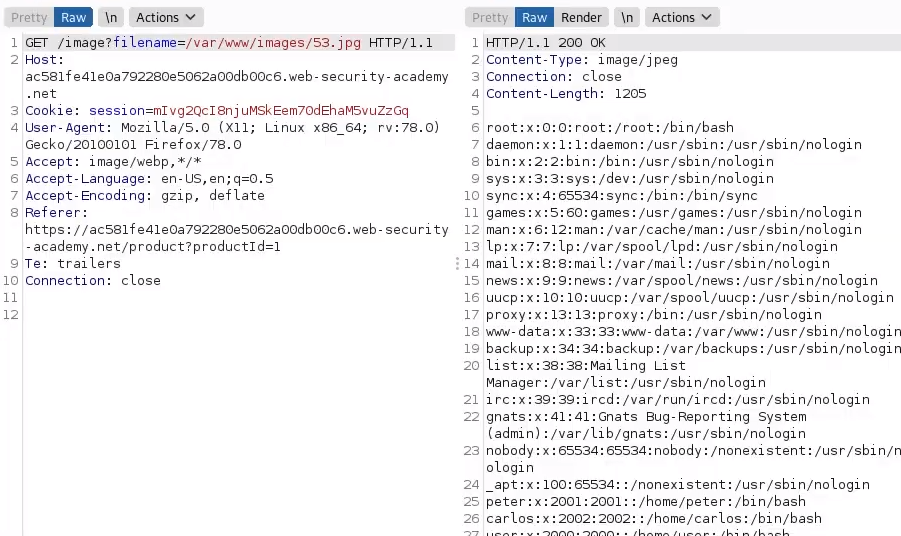
1. Set up Burp Suite and capture a request directed at displaying a product image.
2. Adjust the filename parameter to:

/var/www/images/../../../etc/passwd

1. Inspect the response, checking that it returns the contents of the /etc/passwd file.

**PAYLOAD**

filename=/var/www/images/../../../etc/passwd

**  
PROOF OF CONCEPT**

**REMEDIATION**

1. Instead of relying on relative paths, implement a mapping system that binds user input to specific, pre-defined paths.
2. Monitor for abnormal requests attempting to access directories outside of the defined paths.
3. Employ solutions like chroot jails or containers to isolate applications and limit potential damage.