SCENARIO

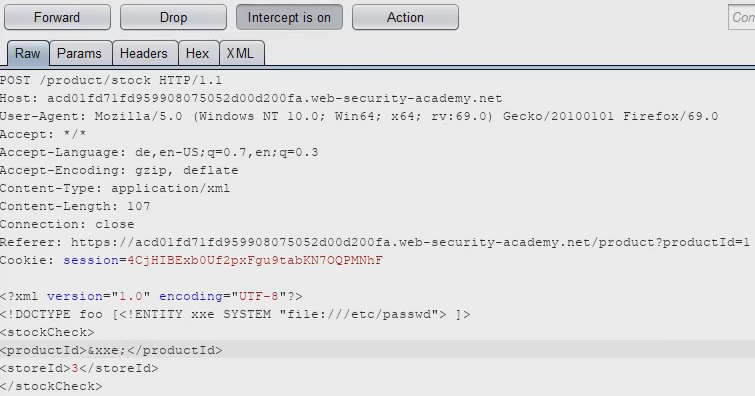
In this lab, the "Check stock" functionality utilizes XML parsing. Unexpectedly, it echoes unusual values from the XML input within its response.

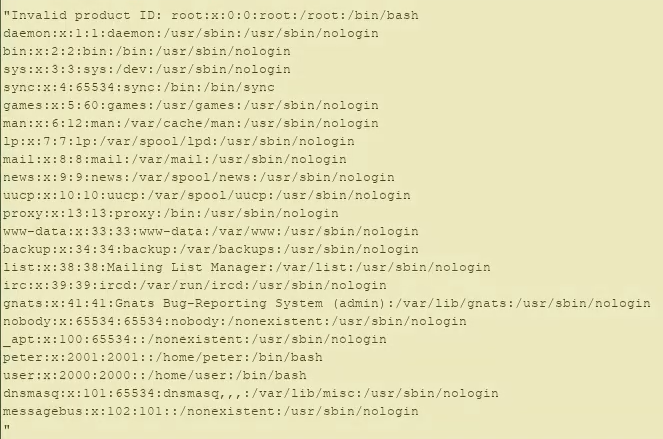
**PROCEDURE**

1. Navigate to the product page and click on "Check stock". While doing so, use Burp Suite to capture the outgoing POST request.
2. Between the XML declaration and the stockCheck element, embed this external entity definition: <!DOCTYPE test [ <!ENTITY xxe SYSTEM "file:///etc/passwd"> ]>
3. Then, update the productId value by referencing this external entity using &xxe;. If successful, the server's response should prefix the contents of the /etc/passwd file with "Invalid product ID:".

**PAYLOAD**

<!DOCTYPE test [ <!ENTITY xxe SYSTEM "file:///etc/passwd"> ]>

**PROOF OF CONCEPT**



**REMEDIATION**

1. **Disable DTDs:** XML external entity parsing should be disabled within the XML parser's configuration.
2. **Whitelist Approach:** Only allow specific, known entities. As an added precaution, consider transitioning to a simpler, less error-prone data format.