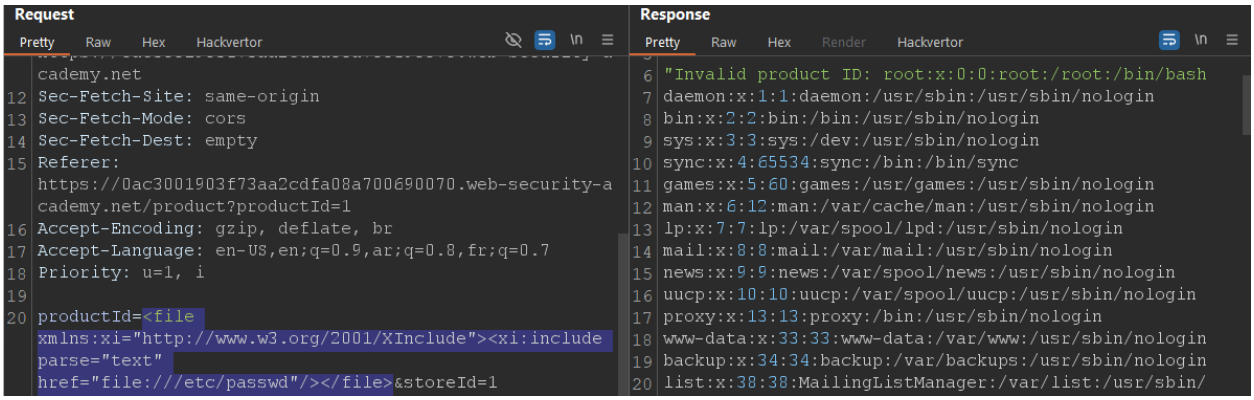
Exploiting XInclude to retrieve files

1. This lab has a "Check stock" feature that embeds the user input inside a server-side XML document that is subsequently parsed. Because you don't control the entire XML document you can't define a DTD to launch a classic XXE attack. To solve the lab, inject an XInclude statement to retrieve the contents of the /etc/passwd file.

2. After a few searches, I found document from XML that explains XInclude.

3. I prepared a basic xinclude payload then passed it via productId variable in check stock request.



Reference: XML Document