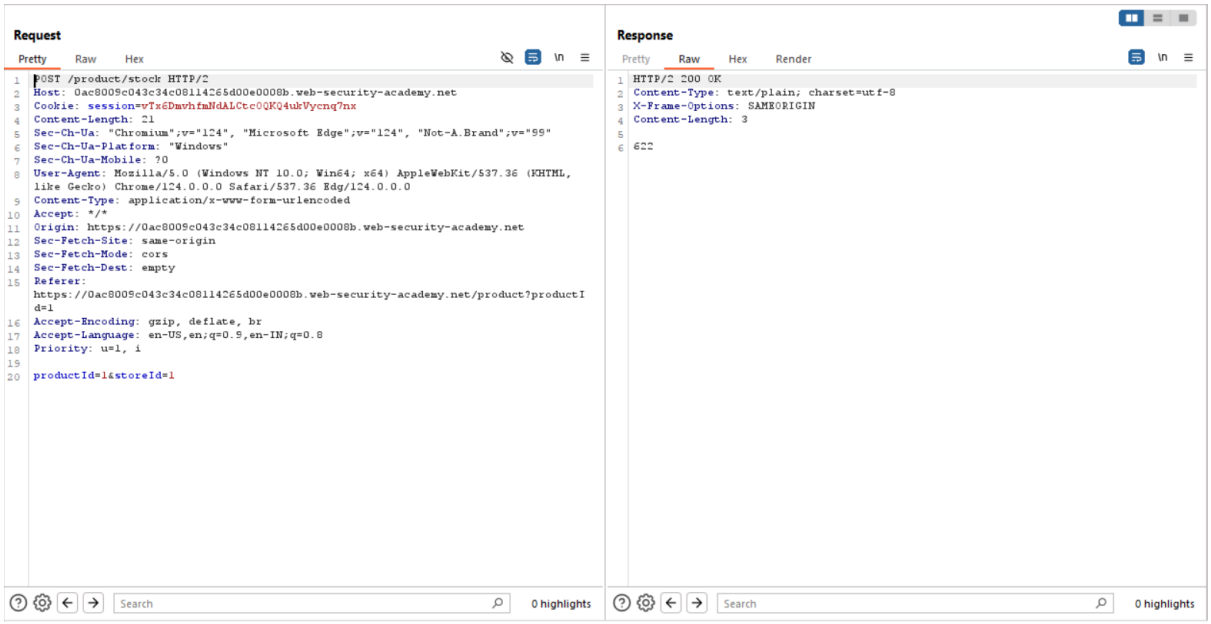
S. Giridharan
CB.SC.P2CYS23006

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.

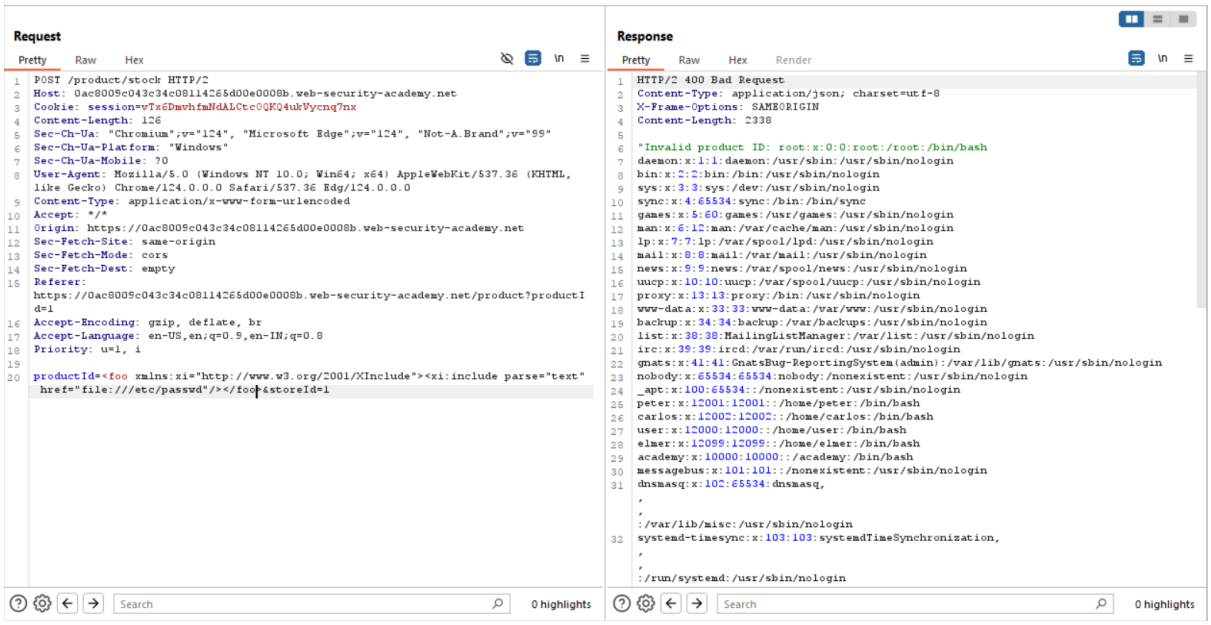
To solve the lab, inject an `XInclude` statement to retrieve the contents of the `/etc/passwd` file.

As Stated in the lab description, intercept the Check Stock POST Request in the Burpsuite.



Set the value of the productId parameter to:

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



We can able to retrieve the /etc/passwd file contents.