20th January 2023

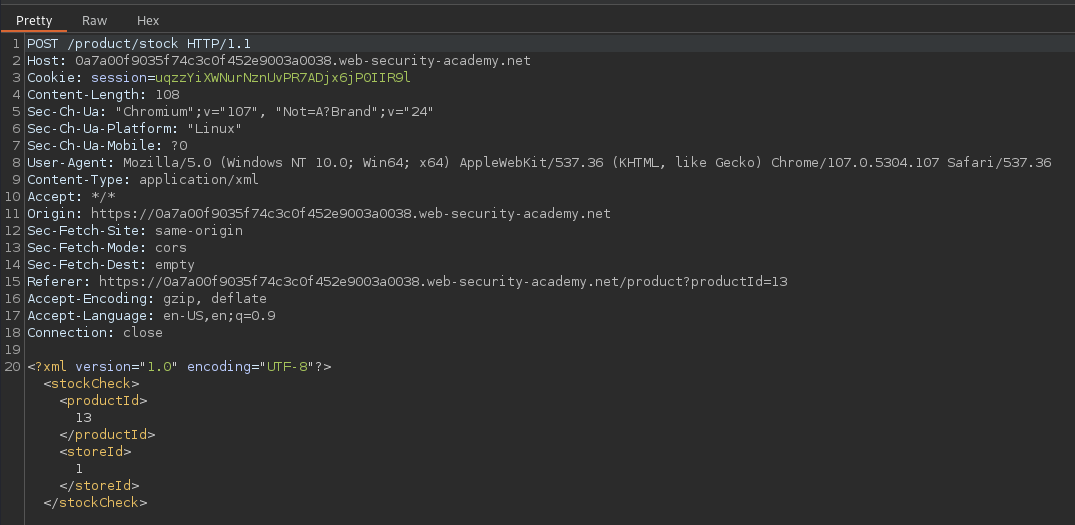
**XML External Entity Attack Lab 1**

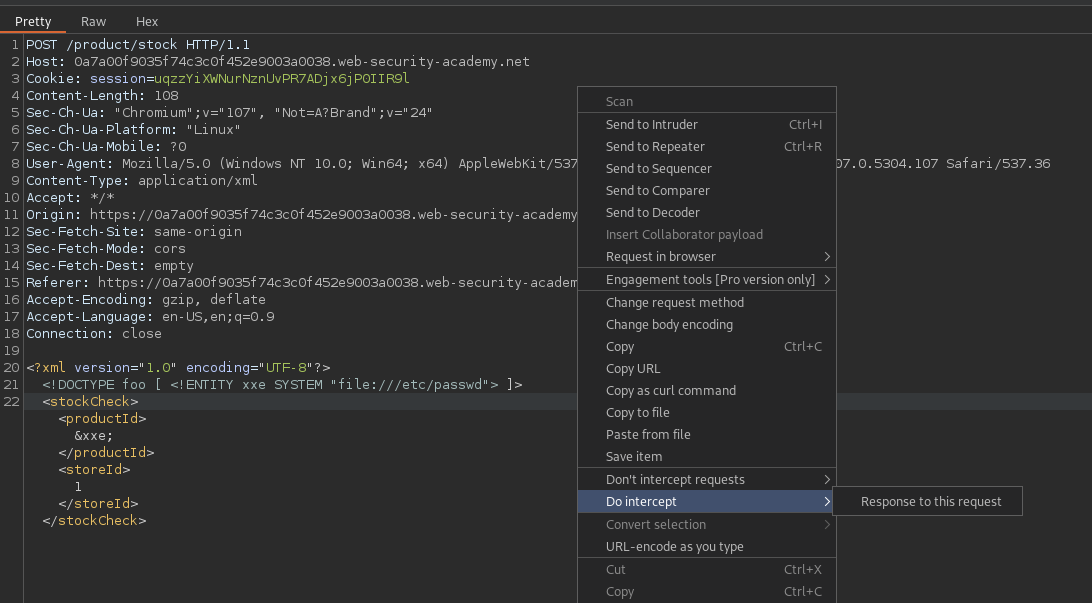
**Summary of Results**

This lab is vulnerable to file retrieval through an XXE injection attack. To perform the attack, a request to the ‘Check stock’ feature, that parses XML input is abused. By intercepting the request to this feature, an external entity definition containing an OS command to retrieve the file ‘/etc/passwd’ is used. This request was then forwarded to the server, which returned the contents of the file.

**Attack Narrative**

In an attempt to analyse the response from the application, the request to the element ‘Check stock’is intercepted in Burp suite’s proxy.



The request is edited by introducing a DOCTYPE element that defines an external entity containing the path to the file. 

The response from the server returned the contents of the file ‘/etc/passwd’. This confirms that the file retrieval vulnerability through an XXE payload is present.