20th January 2023

**XML External Entity Attack Lab 2**

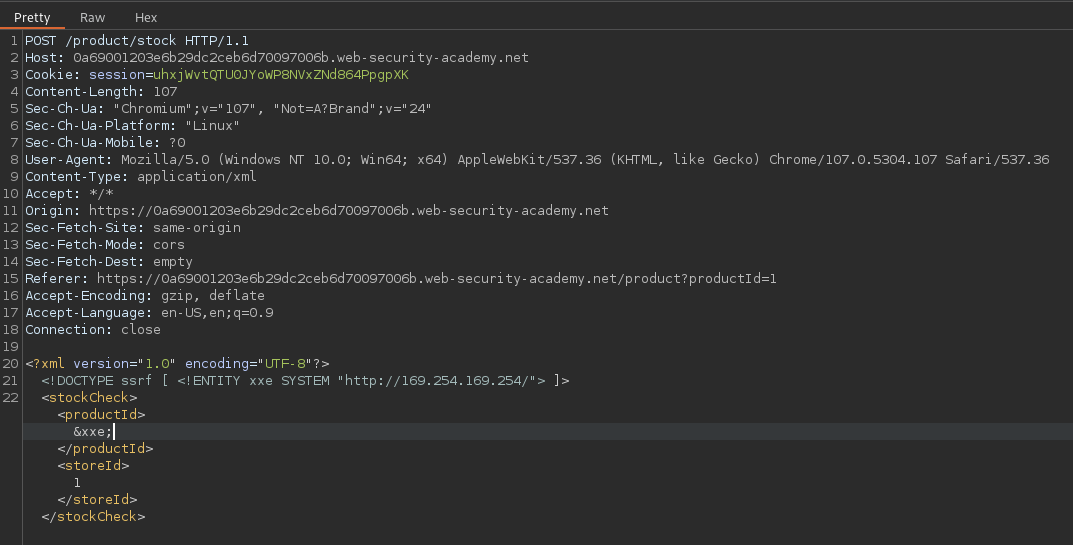
**Summary of Results**

This lab is vulnerable to Server-Side Request Forgery (SSRF) through an XXE attack. By intercepting the request to ‘Check stock’ feature in the lab, an XML entity targeting the URL <http://169.254.169.254/> was used. This belongs to a simulated EC2 metadata endpoint, and can be used to retrieve data about the instance, some of which might be sensitive.

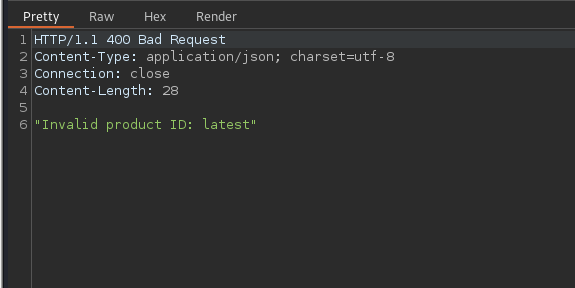
An external entity definition containing the URL is inserted, and the payload is forwarded to the server. The response returns an error stating ‘Invalid product ID: latest’, which essentially is a folder name. Further, a couple more requests to the ‘Check stock’ feature is intercepted, and the external entity definition is changed to the consecutive folder names obtained from the response. The final ‘admin’ folder in the API returns a JSON file containing the ‘SecretAccessKey’.

**Attack Narrative**

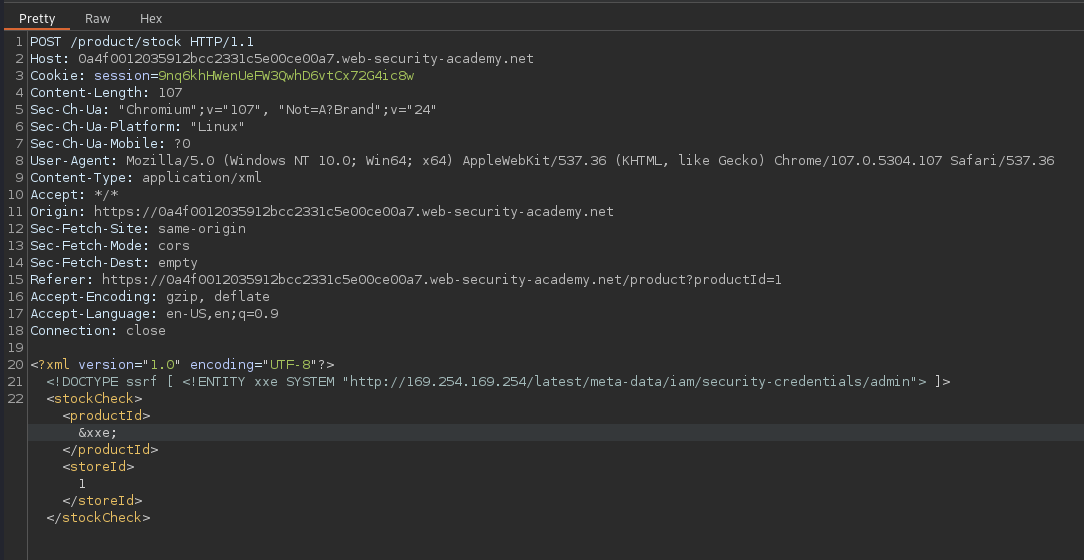
The first request to the ‘Check stock’ feature is intercepted, and the XML entity targeting the URL <http://169.254.169.254/> was sent.



The response returned the first folder ‘latest’, present in the chain of folders leading up to the final directory ‘admin’.



The final request with the external entity definition containing the chain of folders is sent.



The response returned the EC2 metadata containing the ‘SecretAccessKey’.

