Exploiting XXE to perform SSRF attacks

1. This lab has a "Check stock" feature that parses XML input and returns any unexpected values in the response.

2. The lab server is running a (simulated) EC2 metadata endpoint at the default URL, which is **http://169.254.169.254/**. This endpoint can be used to retrieve data about the instance, some of which might be sensitive.

3. The check stock is done via XML code. I intercepted the request and injected my custom entity that visit that endpoint.

4. When I sent the request, the response was another endpoint. I added it to the URL like this: http://169.254.169.254/latest and so on till I get the full URL.

5. And finally, I get the metadata.