Lab name: [Exploiting XXE to perform SSRF attacks](https://portswigger.net/web-security/xxe/lab-exploiting-xxe-to-perform-ssrf)

Severity: High

Lab description:

* This lab shows how an XXE (XML External Entity) vulnerability can be used to perform a Server-Side Request Forgery (SSRF).
* The server processes user-supplied XML and allows external entity definitions.
* An attacker can define an entity that makes the server send a request to internal systems (e.g., http://169.254.169.254) using SSRF.

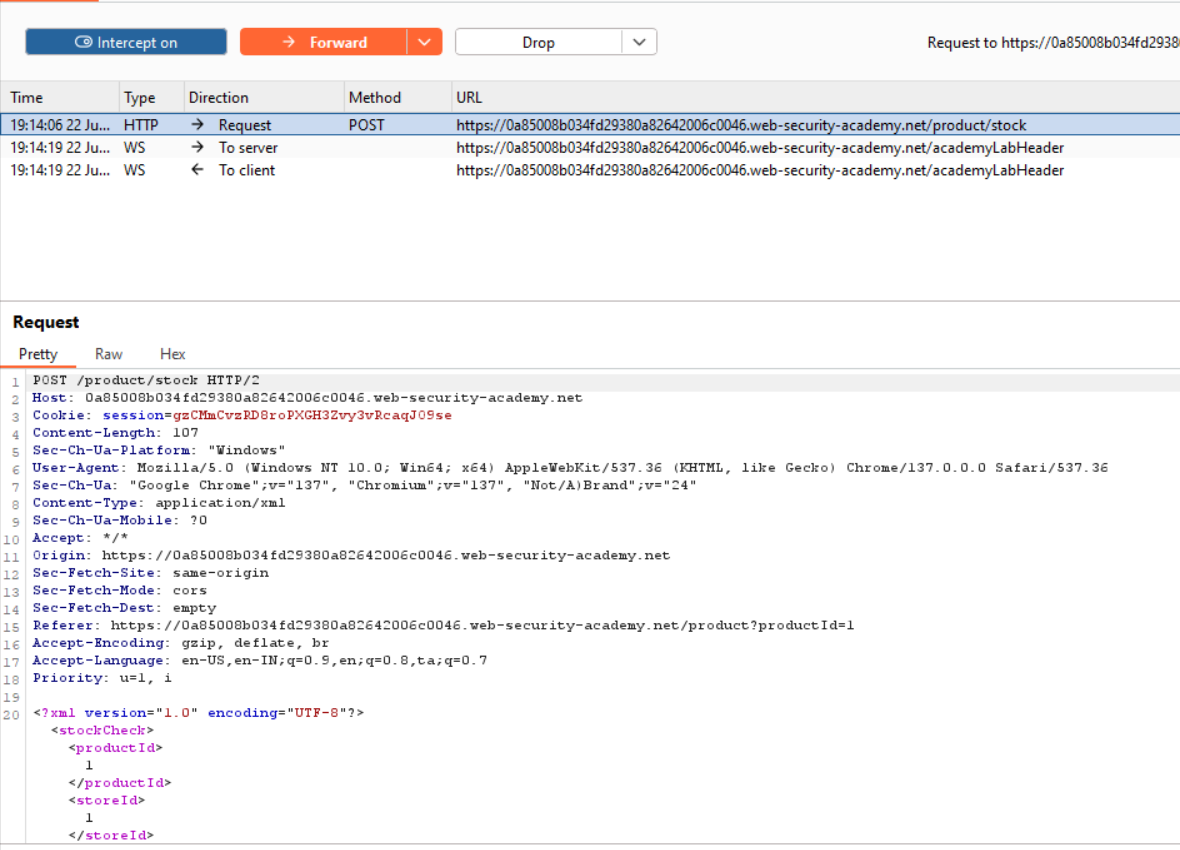
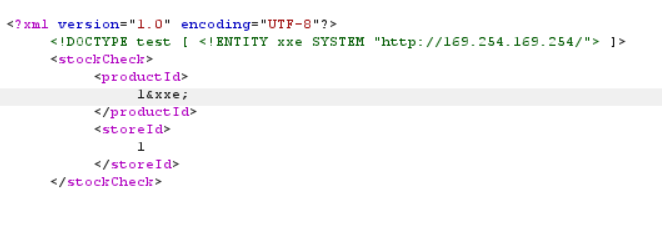
Impact:

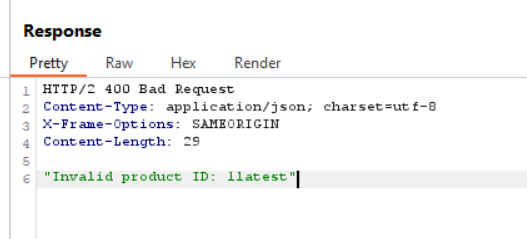
* Attackers can make the server access internal or protected resources that are not exposed publicly.
* For example, accessing the AWS metadata service at 169.254.169.254 can leak cloud credentials.
* This can lead to cloud account takeover, data theft, or privilege escalation.
* It may expose internal APIs, admin portals, or other sensitive services.
* The request comes from the server, so it bypasses firewalls or IP-based access controls.
* Users have no idea such background attacks are happening.

Recommendations:

* Disable external entity processing (XXE) in XML parsers by default.
* Use safe data formats like JSON instead of XML when possible.
* Validate all user input and avoid parsing user-controlled XML.
* Block server access to internal IP ranges (e.g., 127.0.0.1, 169.254.169.254) through firewall rules.
* Monitor outgoing server traffic and alert for unusual requests.
* Use IAM roles with limited permissions in cloud services to minimize damage if credentials are exposed.

Steps to reproduce:

1. Open the lab and go to the "Check stock" feature on a product page.
2. Intercept the POST request using Burp Suite; it contains XML data.
3. Enter the following in between the XML declaration and stock check element  
   *<!DOCTYPE test [ <!ENTITY xxe SYSTEM "http://169.254.169.254/"> ]>* and also change the productid value to ‘*&xxe*;’.
4. this will reveal the folders that are present in this domain. Iteratively check for furher folders.



1. At last we get admin’s URL which has the secret key to solve the lab.

