Lab name: [Basic SSRF against the local server](https://portswigger.net/web-security/ssrf/lab-basic-ssrf-against-localhost)

Severity: High

Lab description:

* This lab shows a Server-Side Request Forgery (SSRF) vulnerability.
* The application loads product images from a URL, which can be controlled by the user.
* The server does not block access to localhost (127.0.0.1), allowing attackers to target services running on the same server.

Impact:

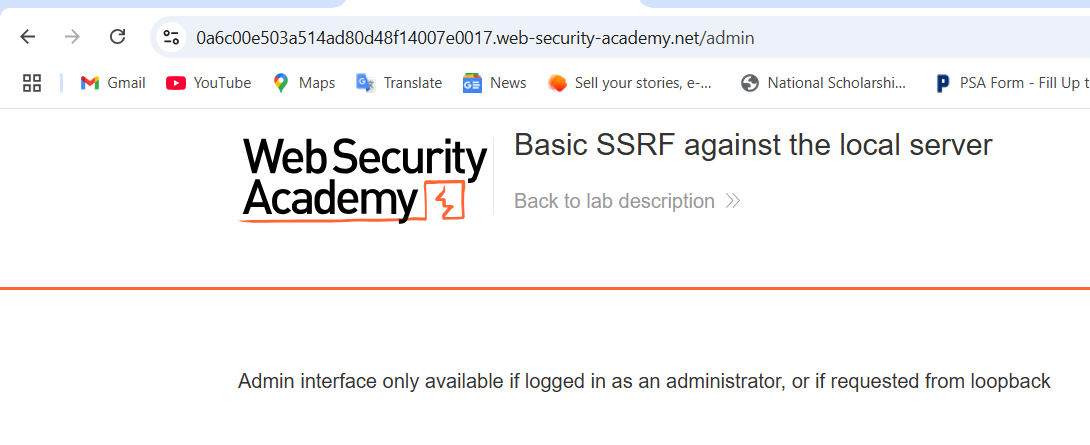
* The attacker can send requests to internal services running on localhost, like admin panels or APIs.
* This may reveal sensitive information or lead to unauthorized access.
* Since the server is making the request, it bypasses firewall rules meant for external users.
* Internal-only services (meant to be private) become exposed to attackers.
* SSRF can lead to further attacks like scanning open ports, accessing internal metadata, or RCE.
* Users won’t notice the attack since it happens in the background on the server.

Recommendations:

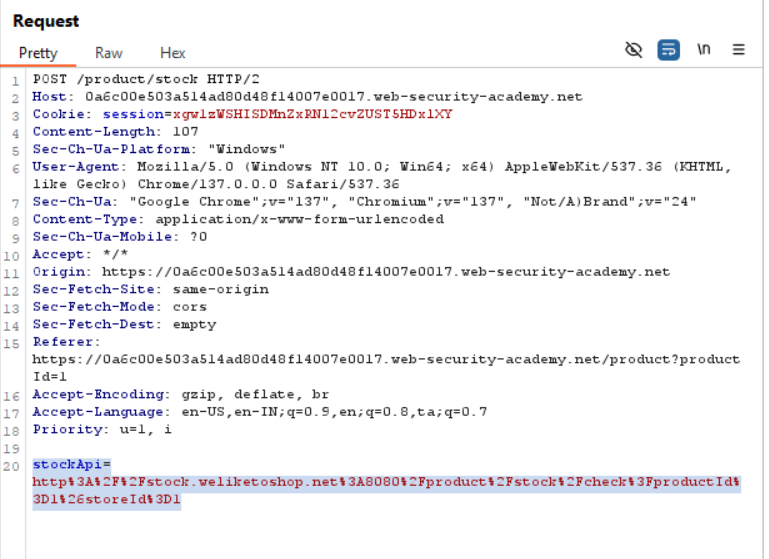
* Never trust URLs from user input without validation.
* Block requests to **localhost (127.0.0.1)** and other internal IP ranges (e.g., 192.168.x.x, 10.x.x.x).
* Use a URL whitelist and allow only trusted domains (like your own image server).
* Implement metadata filters or firewall rules that restrict outbound access from the server.
* If loading external content is required, use a **proxy server with strict rules**.
* Log all outgoing requests and set alerts for access to internal IPs or services.

Steps to reproduce:

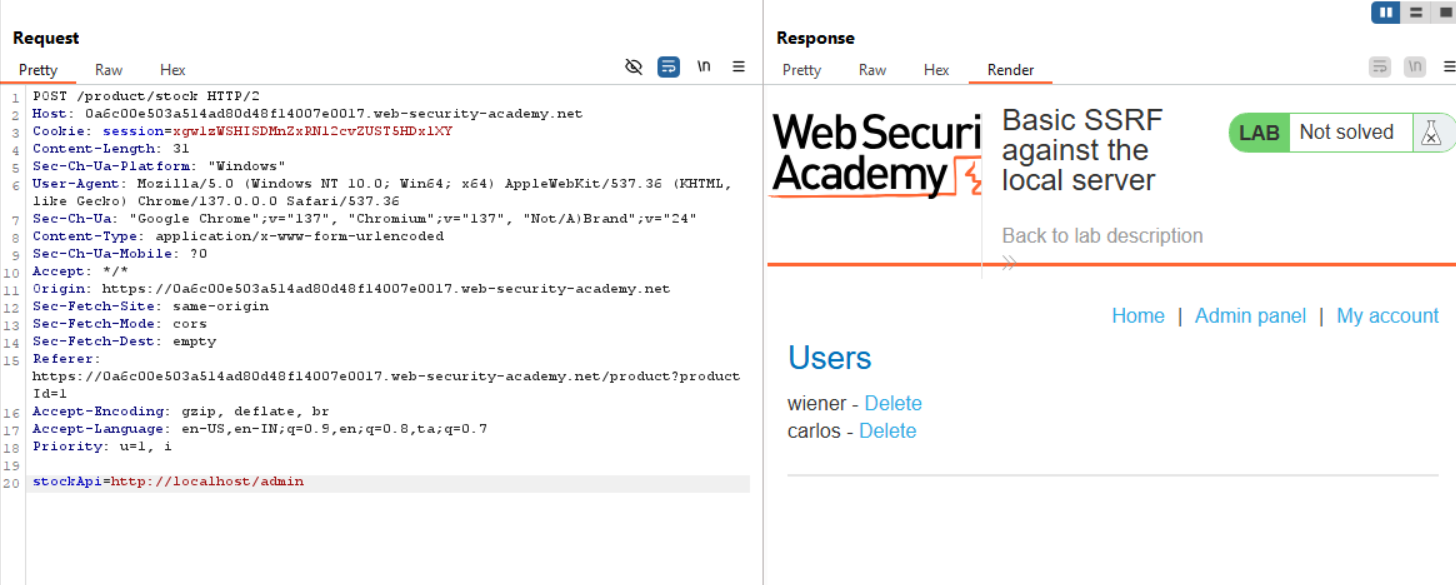
* 1. Access the lab and try accessing /admin through URL, it is not accessible.

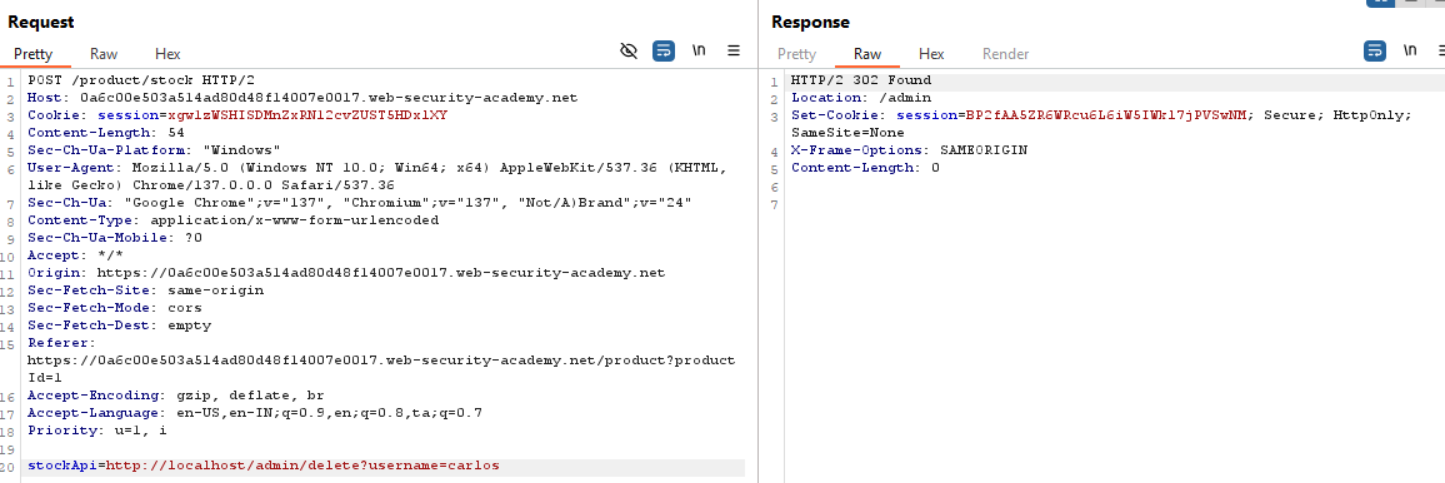


* 1. Move to a product and use intercept while clicking the checkStore button. It can be seen that there is stockApi parameter in it. Change it to localhost/admin.



* 1. Now the admin page is visible, then give this payload to delete carlos user:  
     *http://localhost/admin/delete?username=carlos*





* 1. Send this request then the user carlos profile is deleted.