SSRF with filter bypass via open redirection vulnerability

1. This lab has a stock check feature which fetches data from an internal system.

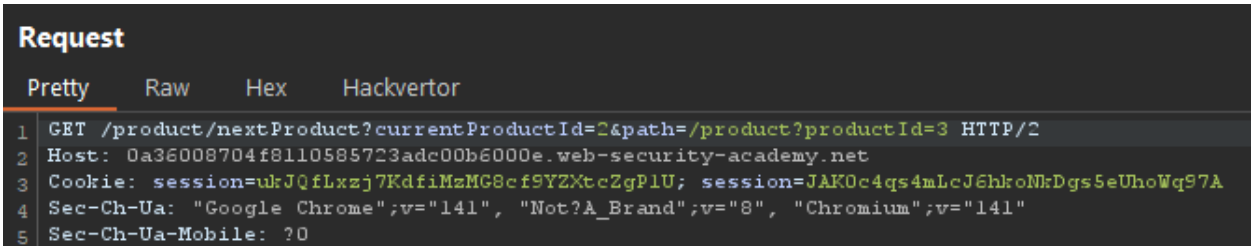
2. The stock checker has been restricted to only access the local application, so you will need to find an open redirect affecting the application first.

3. After intercepting the stock check request, I find that there is no way to modify the URL in stockApi. This time it takes only the endpoint not the full URL. So, we need to find another way to access the admin panel.

```
stockApi=/product/stock/check?productId=2&storeId=1
```

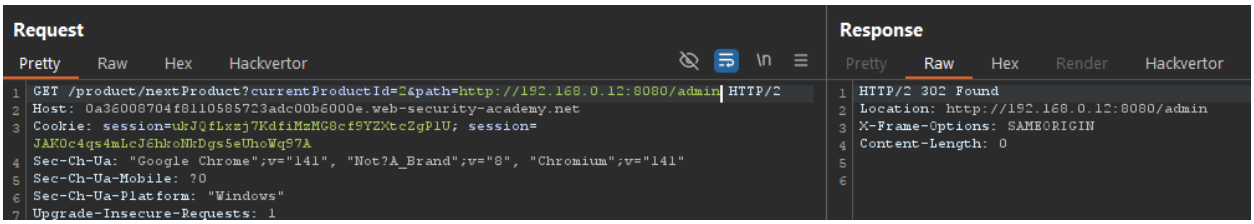
4. The lab description tells us that this lab is vulnerable to open redirect vulnerability.
   NOTE: An open redirect vulnerability occurs when an application allows a user to control a redirect or forward to another URL. If the app does not validate untrusted user input, an attacker could supply a URL that redirects an unsuspecting victim from a legitimate domain to an attacker's phishing site.

5. While browsing the application. I found a button on the product page that redirected me to the next product page. I clicked it and intercepted the request. This is the request:



   The request takes the next page path in the path parameter under the **product** endpoint.

6. When I modify it to http://192.168.0.12:8080/admin, the response is **302** and redirect me to admin panel. But when I followed redirection, the lab took a long time and didn't redirect me to admin panel. Actually, I don't know why but let's think in another way.



7. What happened if I copy this path and paste it in stockApi ?? Let's try it.

It works!! I already have access to the admin panel. Let's delete the user carlos.