Portswigger: SSRF vuln via open redirect

Sam Newman

April 2025

1 Website in Question

This section of the website contains a vulnerability with an unsecured API endpoint that can be manipulated into executing unsafe commands on the company servers. In the lab, you must exploit these weaknesses to delete a user from the system

2 Business Impact

This vulnerability could allow user execution of admin-only API endpoints, allowing everything from dumping of data to user data manipulation and remote code execution. This is an extremely dangerous vulnerability and could lead to disastrous outcomes were a website author not careful, as in this case.

3 How It Works

First, I explored the website using Portswigger, checking out what different buttons did and seeing where their request went. I then found an open redirect through the next product button, and this could be used to force the stock checker to access the admin panel on local machine and delete the user with admin permissions. All you have to do is alter the stock check URL, and my payload looked like this:

/product/nextProduct?currentProductId=15&
path=http://192.168.0.12:8080/admin/delete?user=carlos

It forces the stock checker server to access the admin API endpoint deleting the user carlos.

4 Why It Works + Mitigation

The website has a vulnerability in their servers, where user input is not thoroughly sanitized in the stock checker URL, and too much is fed through. It should be hardcoded to contain /stock/product or whatever inside of it, and the only variable should be a number for the product ID. This should then be sanitized to make sure it contains only numbers, and reject the input if not.

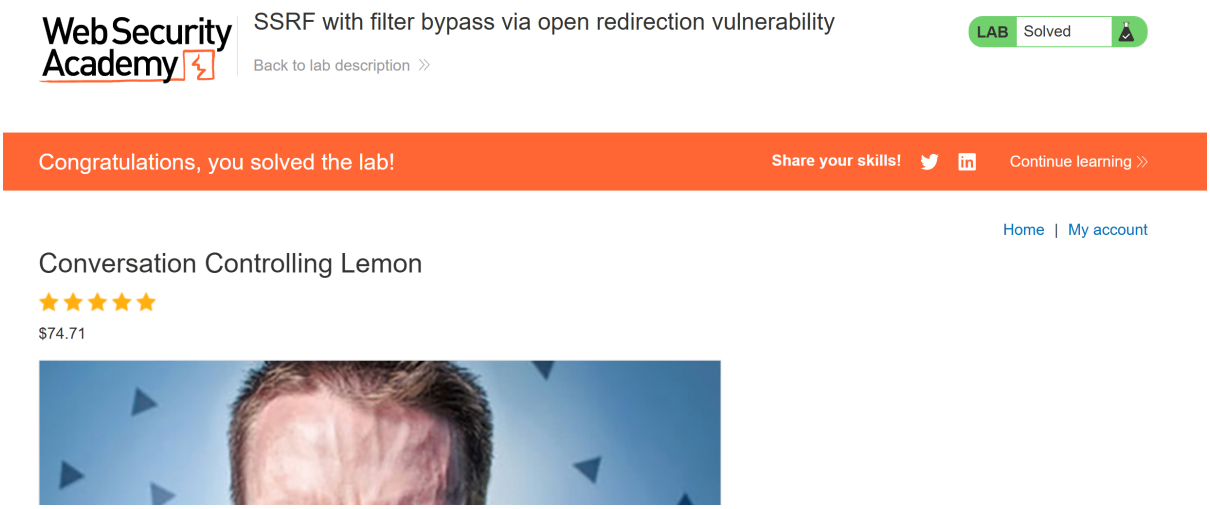

Figure 1: Lab Solved