



Daniel Carrillo  
Omar Villalobos

## Lab: Method-based access control can be circumvented

---

Iniciamos sesión con las credenciales de administrador para ver que tiene.

 Method-based access control can be circumvented

LAB Solved 

Back to lab description >>

Congratulations, you solved the lab!

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

Login

Username


administrator


Password

•••••

Log in

Interceptamos el Admin panel para ver que tiene.

 Method-based access control can be circumvented

LAB Solved 

Back to lab description >>

Congratulations, you solved the lab!

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

User

carlos (NORMAL)

carlos (NORMAL)

administrator (ADMIN)

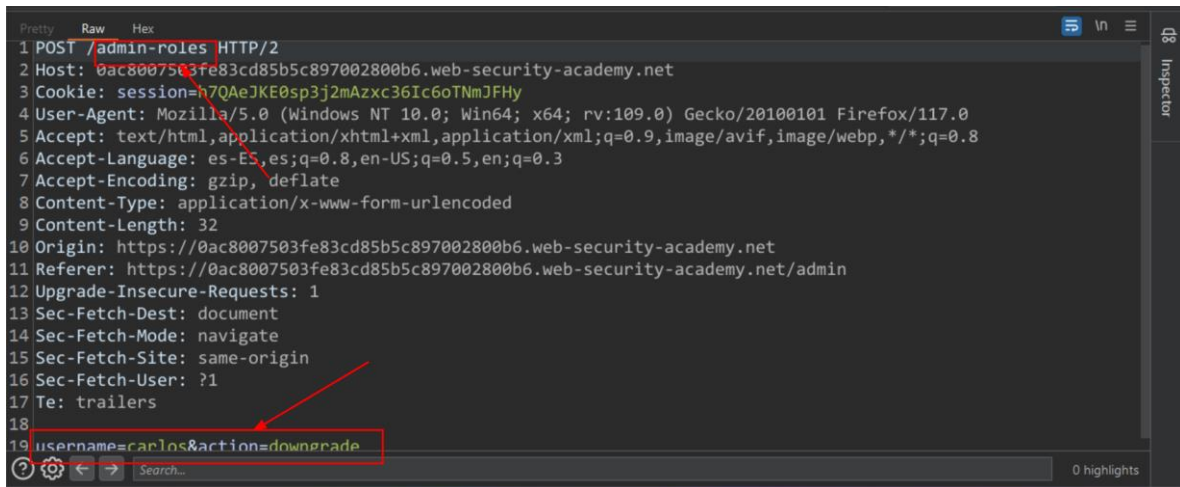
wiener (ADMIN)

Upgrade user

Downgrade user

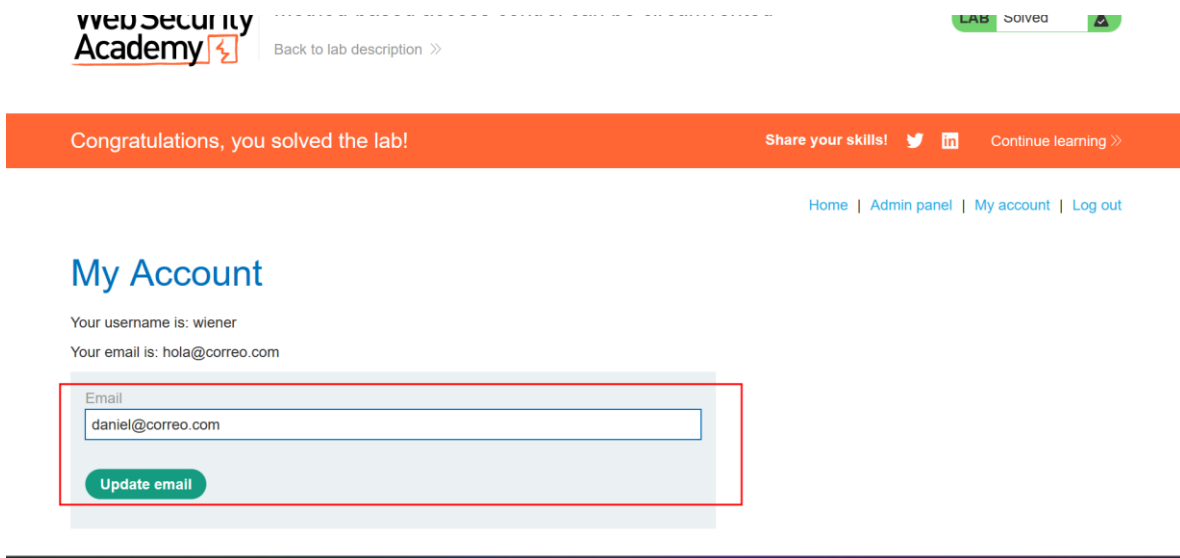
Daniel Carrillo  
Omar Villalobos

Observamos que tiene por método POST “admin-roles” y el cuerpo que es username=carlos&action=downgrade



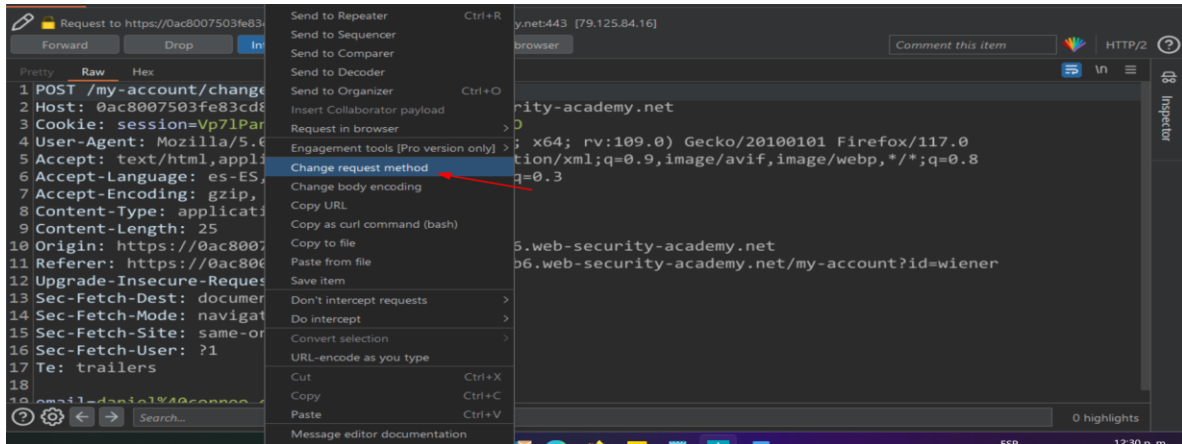
```
1 POST /admin-roles HTTP/2
2 Host: 0ac8007503fe83cd85b5c897002800b6.web-security-academy.net
3 Cookie: session=h7QAeJKE0sp3j2mAzc36Ic6oTNmJFHy
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/117.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: es-ES;q=0.8,en-US;q=0.5,en;q=0.3
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 32
10 Origin: https://0ac8007503fe83cd85b5c897002800b6.web-security-academy.net
11 Referer: https://0ac8007503fe83cd85b5c897002800b6.web-security-academy.net/admin
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 Te: trailers
18
19 username=carlos&action=downgrade
```

Cambiamos con Wiener e iniciamos sesión y subimos un correo para interceptar.

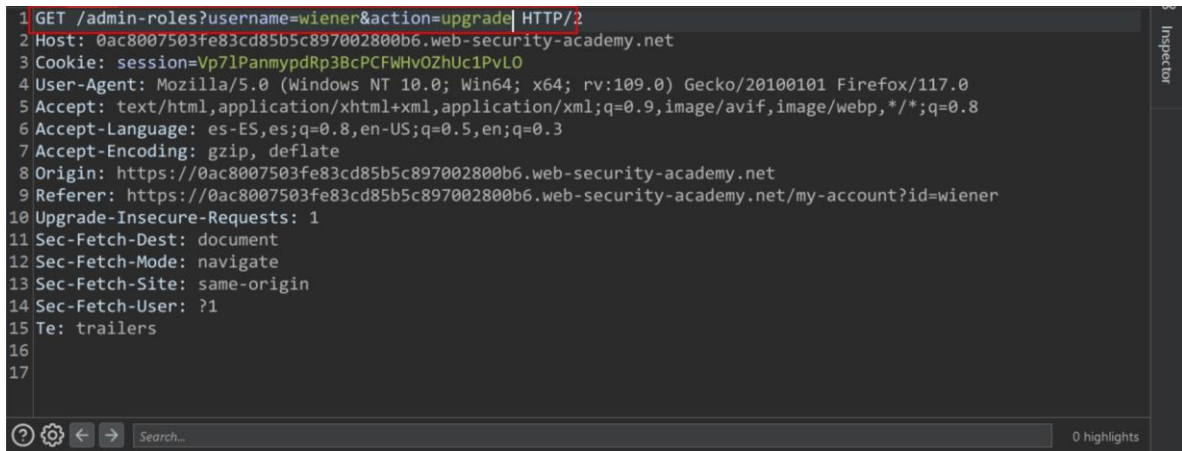


Daniel Carrillo  
Omar Villalobos

Cambiamos el método de entrada a GET



Cambiamos la petición.



Vemos que se logró cambiar Wiener a admin



Congratulations, you solved the lab!

Share your skills!



[Continue learning >>](#)

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

User

carlos (NORMAL) ▾  
carlos (NORMAL)  
administrator (ADMIN)  
wiener (ADMIN)

Upgrade user

Downgrade user

## Lab: Multi-step process with no access control on one step

Se inicio sesión con las credenciales de admin

Congratulations, you solved the lab!

Share your skills!



[Continue learning >>](#)

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

### Login

Username

administrator


Password

•••••


Log in

Daniel Carrillo  
Omar Villalobos

Checamos que se hace con el panel de administrados y vemos con burp.



**WebSecurity Academy** 

Multi-step process with no access control on one step

LAB Solved 

Back to lab description >>

Congratulations, you solved the lab!

Share your skills!   Continue learning >>

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

User

carlos (ADMIN) ▾

carlos (ADMIN)

administrator (ADMIN)

wiener (ADMIN)

Upgrade user

Downgrade user

Are you sure?

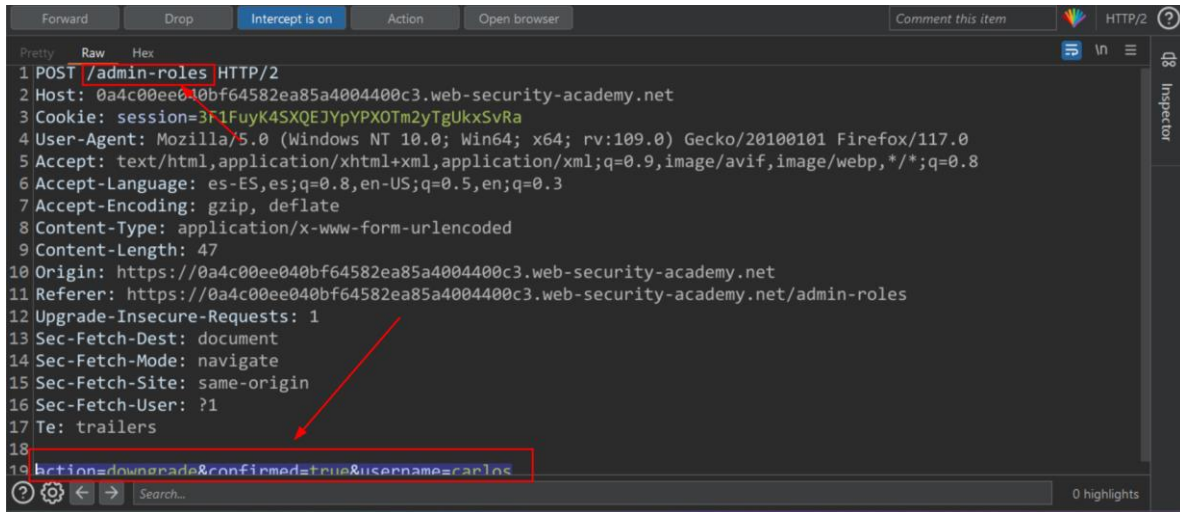
No, take me back

Yes

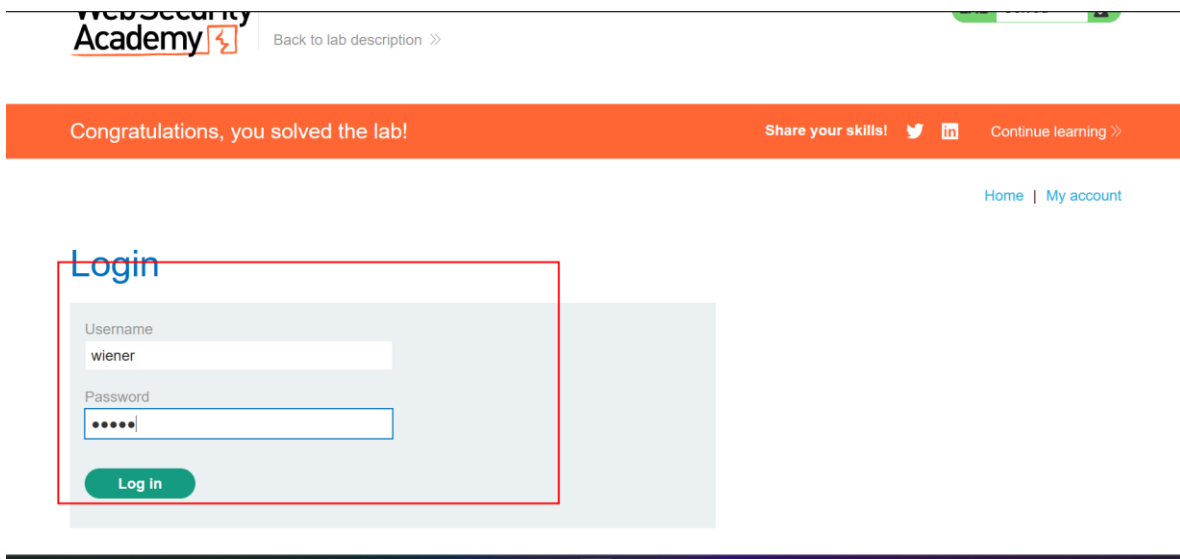
---

Daniel Carrillo  
Omar Villalobos

Observamos que manda en recurso /admin-roles y en el cuerpo  
action=downgrade&confirmed=true&username=carlos



Cambiamos a el usuario Wiener



Daniel Carrillo  
Omar Villalobos

Ingresamos un correo y capturamos la petición.

webSecurity Academy

Back to lab description >>

LAB Solved

Congratulations, you solved the lab!

Share your skills! [Twitter](#) [LinkedIn](#) Continue learning >>

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

## My Account

Your username is: wiener

Your email is: carlos@correo.com

Email

daniel@correo.com

daniel@correo.com

Update email

Cambiamos los parámetros seleccionados por los vistos en admin.

Forward Drop Intercept is on Action Open browser Comment this item HTTP/2

1 POST /my-account/change-email HTTP/2

2 Host: 0a4c00ee040bf64582ea85a4004400c3.web-security-academy.net

3 Cookie: session=psM2xWZ20s2ET09yRc9qnI029fR3YXWQ

4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/117.0

5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8

6 Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3

7 Accept-Encoding: gzip, deflate

8 Content-Type: application/x-www-form-urlencoded

9 Content-Length: 25

10 Origin: https://0a4c00ee040bf64582ea85a4004400c3.web-security-academy.net

11 Referer: https://0a4c00ee040bf64582ea85a4004400c3.web-security-academy.net/my-account

12 Upgrade-Insecure-Requests: 1

13 Sec-Fetch-Dest: document

14 Sec-Fetch-Mode: navigate

15 Sec-Fetch-Site: same-origin

16 Sec-Fetch-User: ?1

17 Te: trailers


18

19 email=daniel@correo.com


action=upgrade&confirmed=true&username=wiener

Daniel Carrillo  
Omar Villalobos

Se subió privilegios a Wiener



**WebSecurity Academy** 

Multi-step process with no access control on one step

LAB Solved 


Back to lab description >>

Congratulations, you solved the lab!

Share your skills!   Continue learning >>

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

User


wiener (ADMIN) 

Upgrade user


Downgrade user


## Lab: File path traversal, traversal sequences blocked with absolute path bypass

Se arrastra cualquier imagen al path.




Home


WE LIKE TO SHOP 




AbZorba Ball  
★★★★★ \$82.49  
View details



The Lazy Dog  
★★★★★ \$43.93  
View details



Couple's Umbrella  
★★★★★ \$48.03  
View details

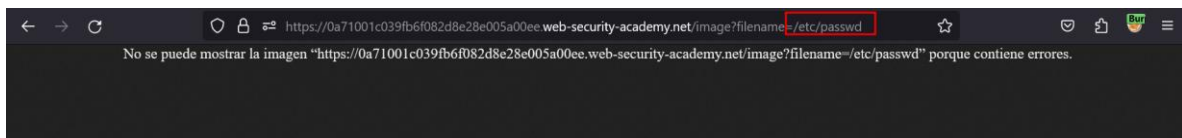
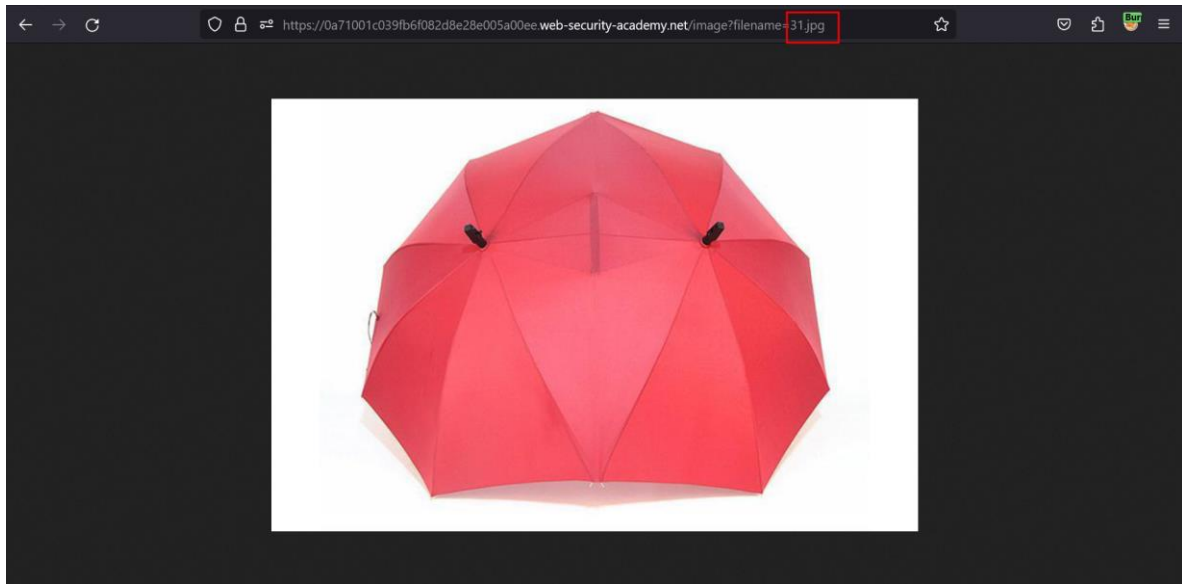


Mood Enhancer  
★★★★★ \$68.08  
View details



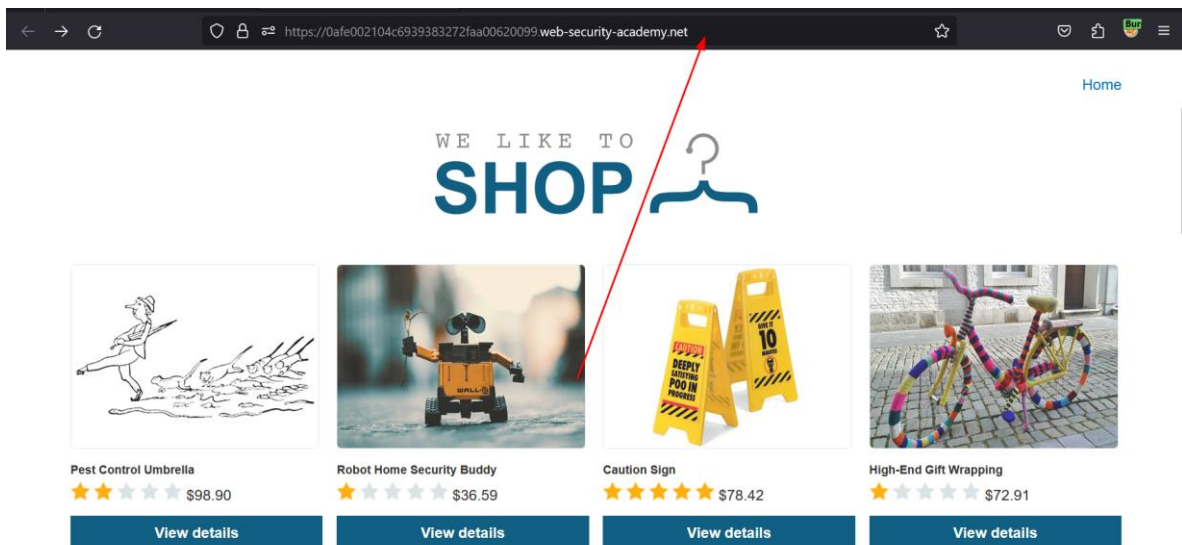
Daniel Carrillo  
Omar Villalobos

Cambiaremos el nombre la imagen por: /etc/passwd



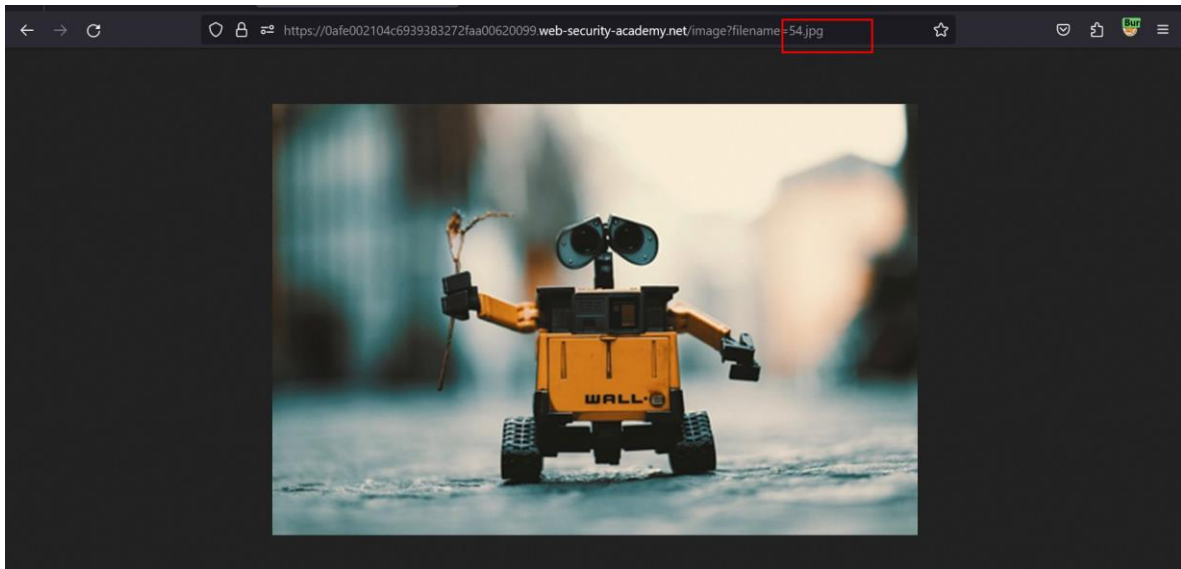
## Lab: File path traversal, traversal sequences stripped non-recursively

Ponemos la imagen en el path.

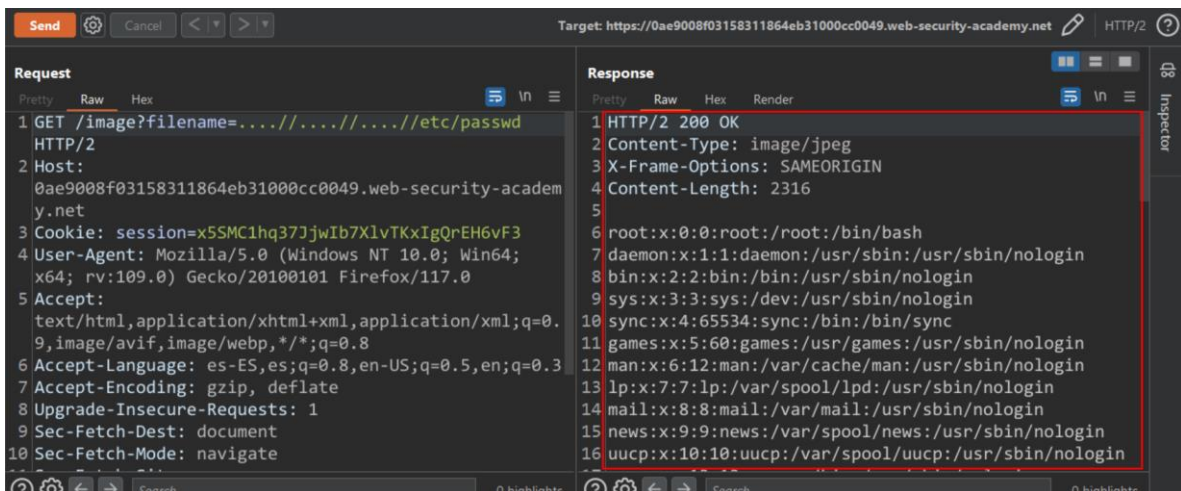


Daniel Carrillo  
Omar Villalobos

Cambiamos el nombre de la imagen y luego ocupamos el método de sanitización.

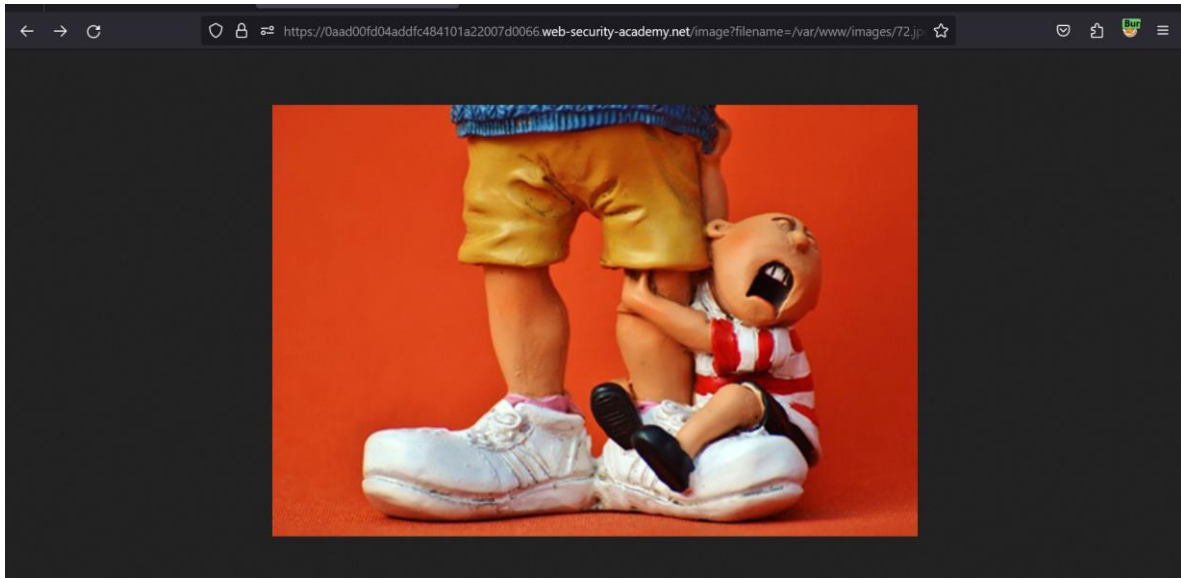


Con Burp podemos ver el contenido.



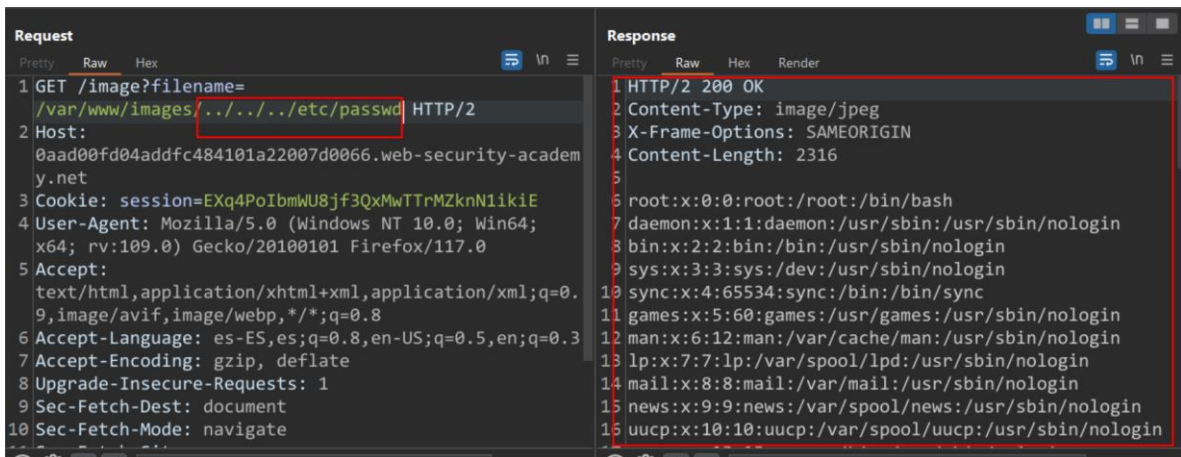
## Lab: File path traversal, validation of start of path

La imagen abierta la abrimos en burp para ver mejor la respuesta.

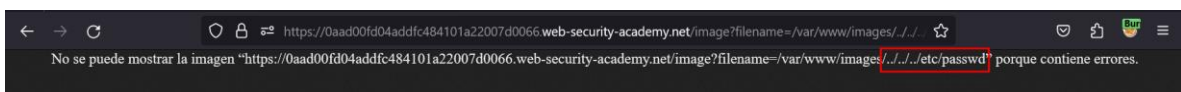


Cambiamos el nombre por ../../../../passwd/etc

Para poder regresar.

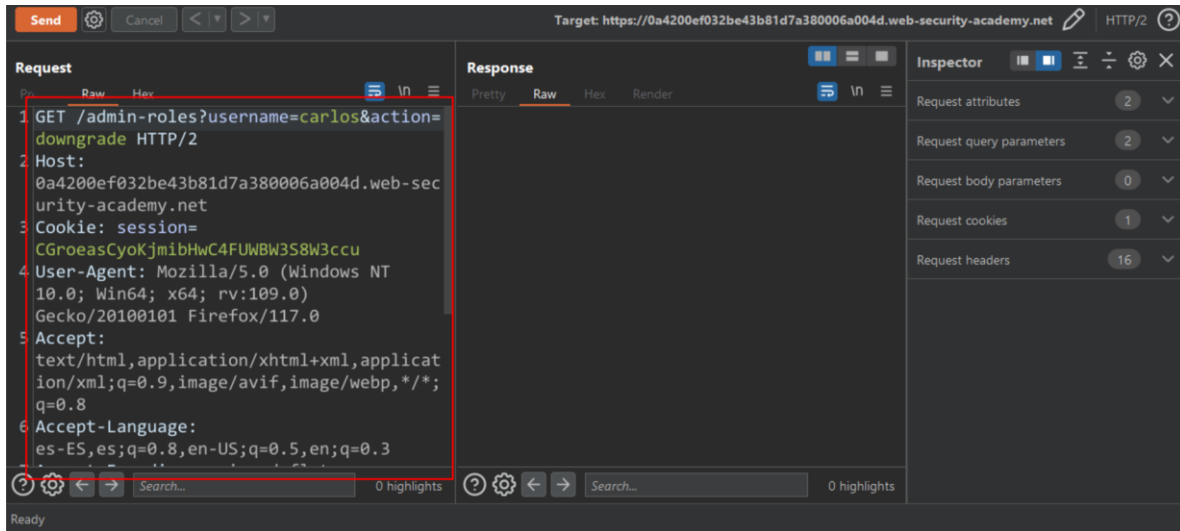


Y queda resuelto.

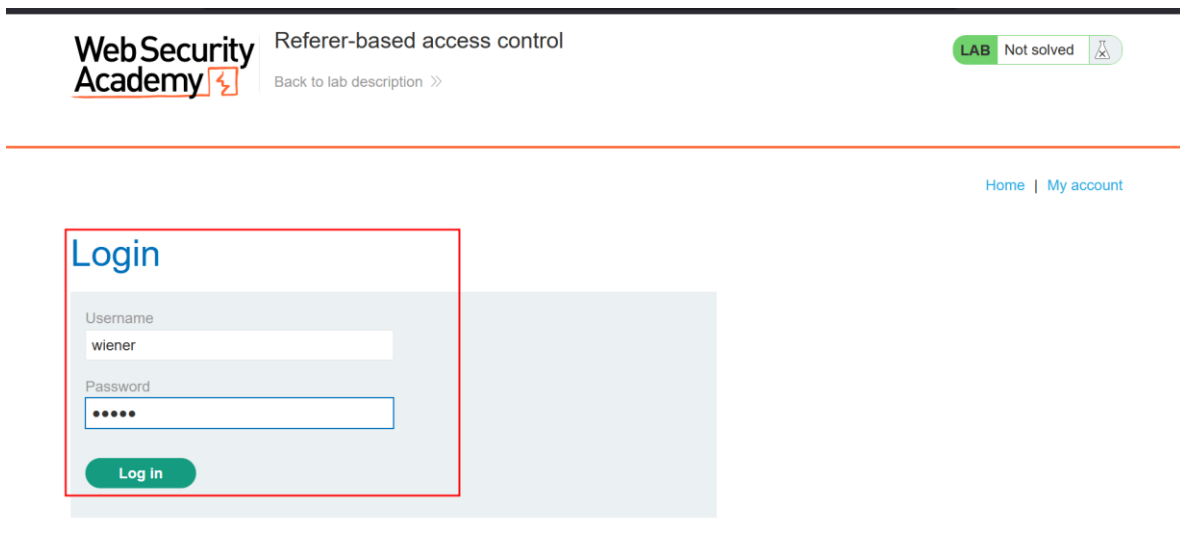


## Lab: Referer-based access control


Ingresamos con las credenciales de administrador y capturamos la vista de adminpanel en el Burp.




Luego cambiamos a las credenciales de Wiener.



## Mandamos un correo para capturar la petición en Burp

 Referer-based access control

LAB Not solved 

[Back to lab description >>](#)

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

### My Account

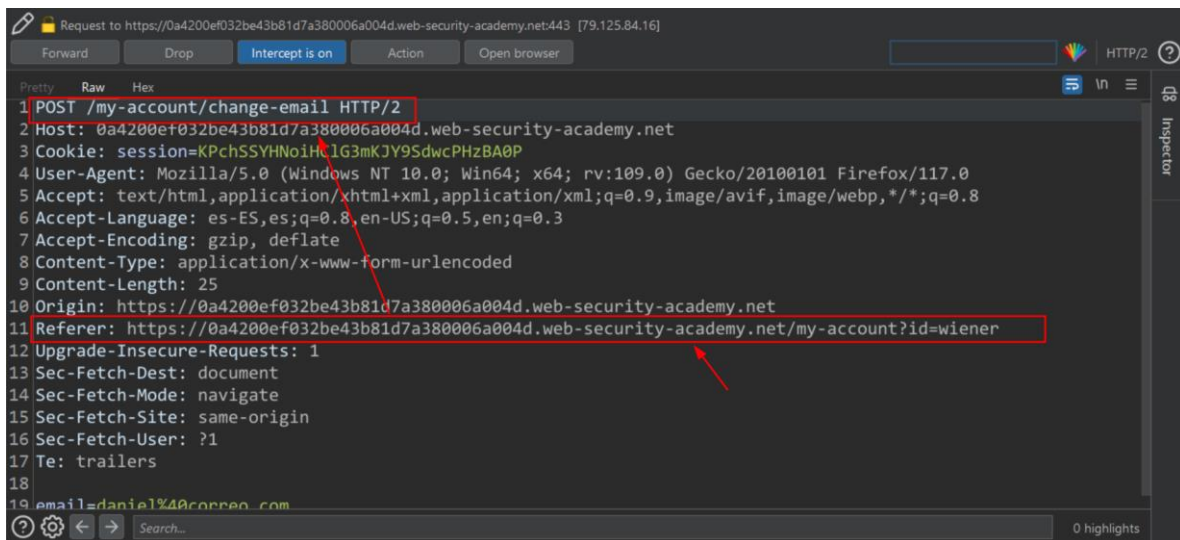
Your username is: wiener

Your email is: daniel@correo.com

Email

Update email

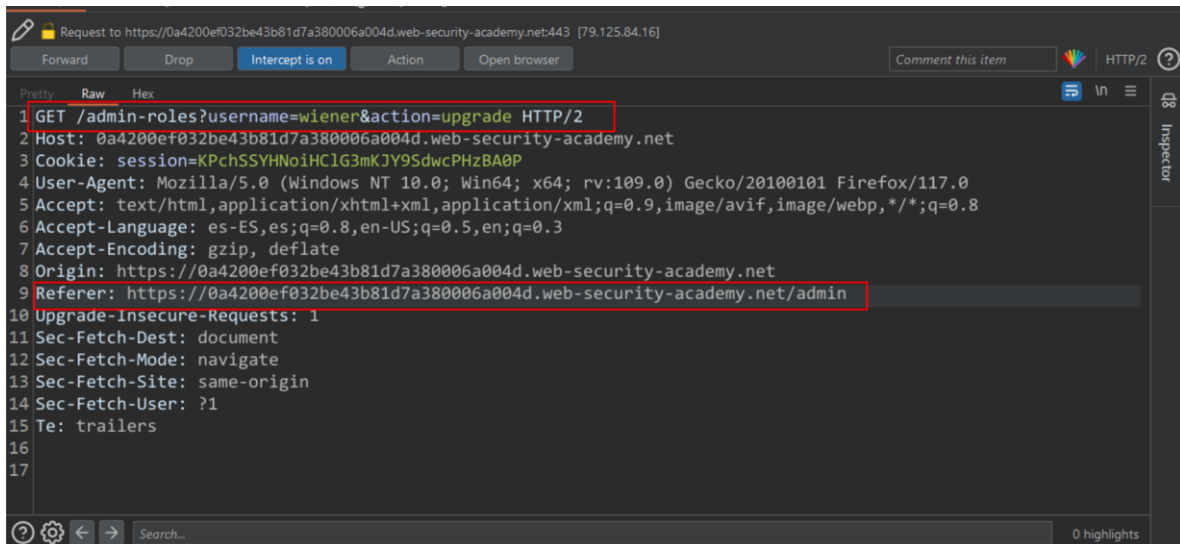
## Cambiamos el metodo a GET y cambiaremos el Referer



```
1 POST /my-account/change-email HTTP/2
2 Host: 0a4200ef032be43b81d7a380006a004d.web-security-academy.net
3 Cookie: session=KPchSSYHNoiHc1G3mKJY9SdwcPHzBA0P
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/117.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 25
10 Origin: https://0a4200ef032be43b81d7a380006a004d.web-security-academy.net
11 Referer: https://0a4200ef032be43b81d7a380006a004d.web-security-academy.net/my-account?id=wiener
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 Te: trailers
18
19 email=daniel%40correo.com
```

Daniel Carrillo  
Omar Villalobos

Se cambio el referer del admin y el username y la action, para subir privilegios a Wiener



Completando el laboratorio una vez que se le sube privilegios a Wiener desde Wiener

Usando el referer y el metodo GET.

