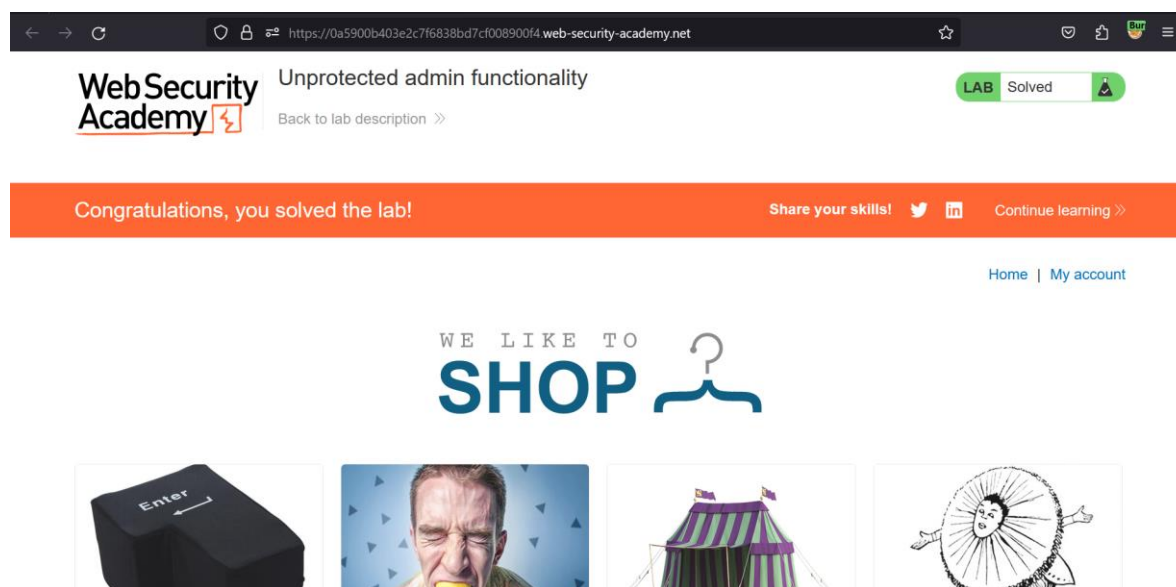
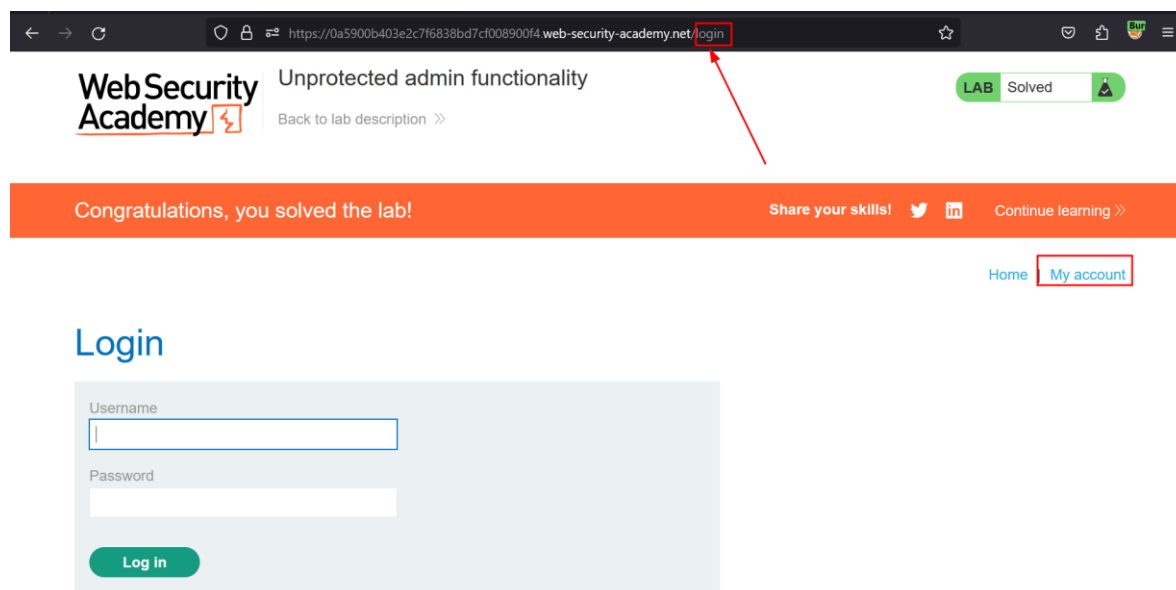


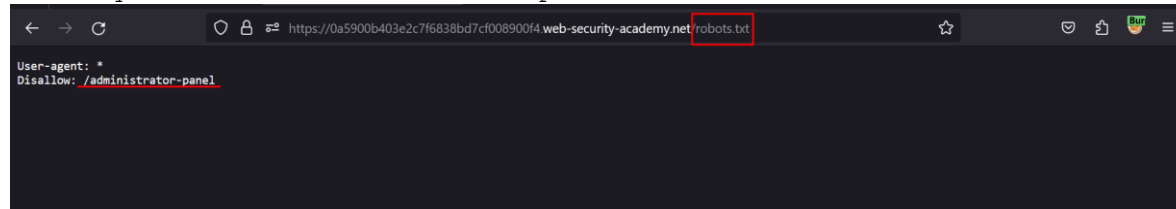
Lab: Unprotected admin functionality



Ingresamos a “My account” y en la URL cambiamos “/login” por /robots.txt



Vemos que tenemos /administrator-panel



Daniel Carrillo
Omar Villalobos

Ingresamos a la url y borramos Carlos.

The screenshot shows a web browser at the URL `https://0a5900b403e2c7f6838bd7cf008900f4.web-security-academy.net/administrator-panel`. The page title is "Unprotected admin functionality". A green "LAB Solved" badge is visible. Below the header, an orange banner says "Congratulations, you solved the lab!". The main content area is titled "Users" and shows a list of users. The first user is "wiener" with a "Delete" link next to it. A red arrow points to the "Delete" link.

Lab: User role controlled by request parameter

Ingresamos al laboratorio

The screenshot shows the Web Security Academy lab page for "User role controlled by request parameter". The URL is `https://0ae100dd03e6d4f180ea211500cb001d.web-security-academy.net`. The page shows a "LAB Not solved" badge. Below the header, there is a large image with the text "WE LIKE TO SHOP" and a shopping cart icon. Below this image are four smaller images: a smartphone showing a castle, a dog jumping with colorful balloons, a person in a blue dress, and a red balloon with a face.

Daniel Carrillo
Omar Villalobos

Ingresamos credenciales.

WebSecurity Academy User role controlled by request parameter LAB Not solved

Back to lab description >>

Home | My account

Login

Log in

WebSecurity Academy User role controlled by request parameter LAB Not solved

Back to lab description >>

Home | Admin panel | My account

Users

wiener - Delete
carlos - Delete

WebSecurity Academy User role controlled by request parameter LAB Solved

Back to lab description >>

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

Home | Admin panel | My account

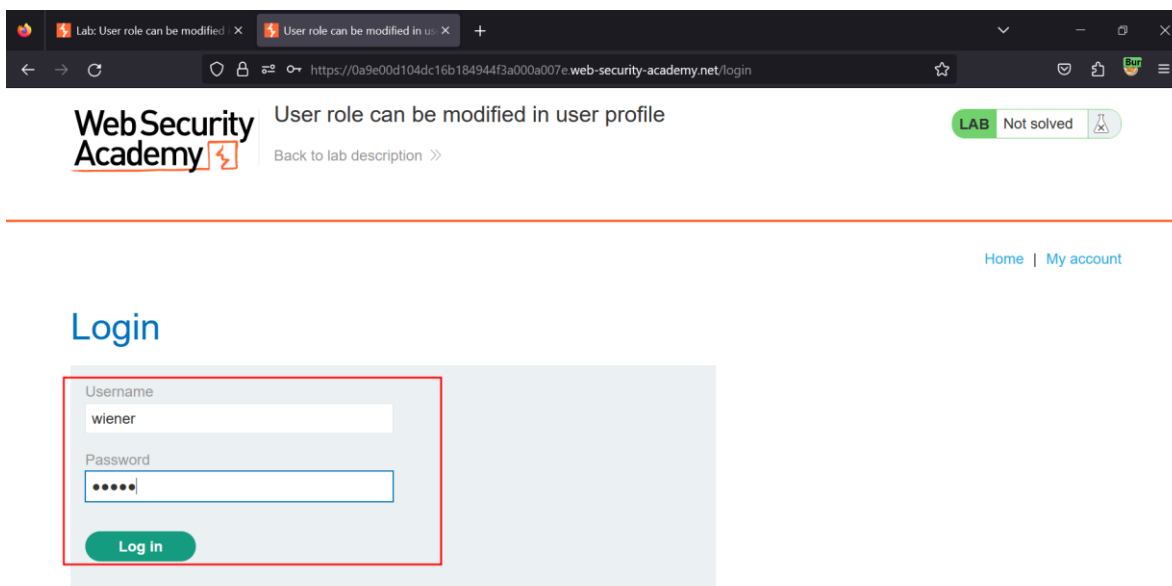
User deleted successfully!

Users

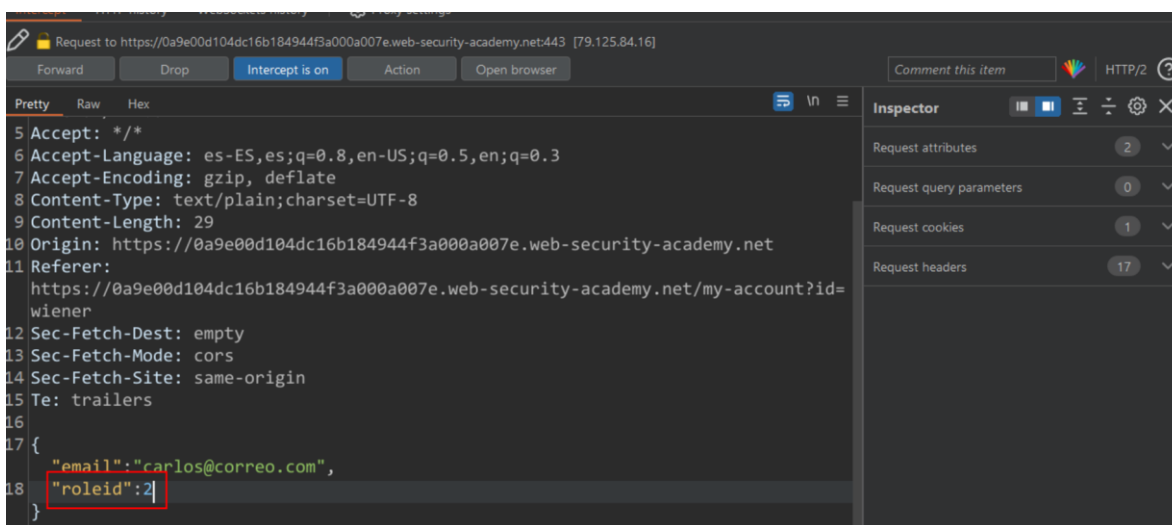
wiener - Delete

Daniel Carrillo
Omar Villalobos

Ingresamos credenciales y capturamos con burp

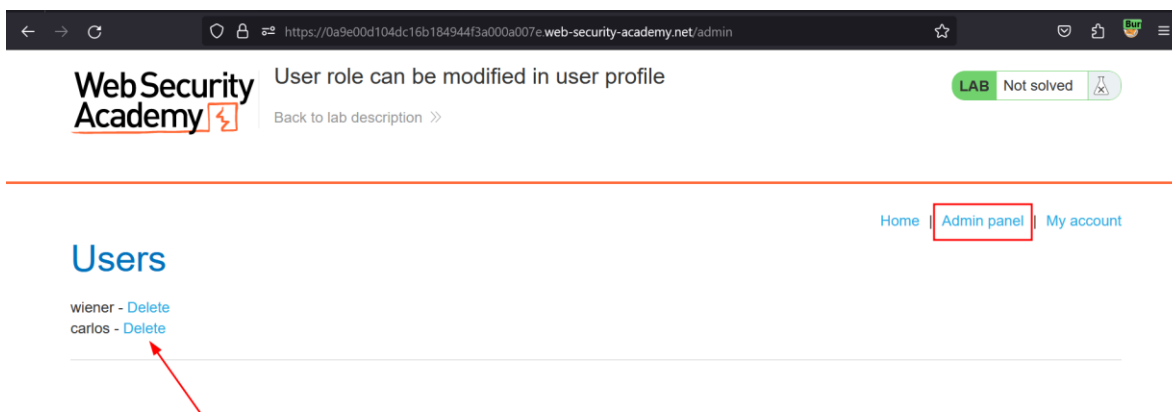


Elevamos privilegios cambiando el roleid:2



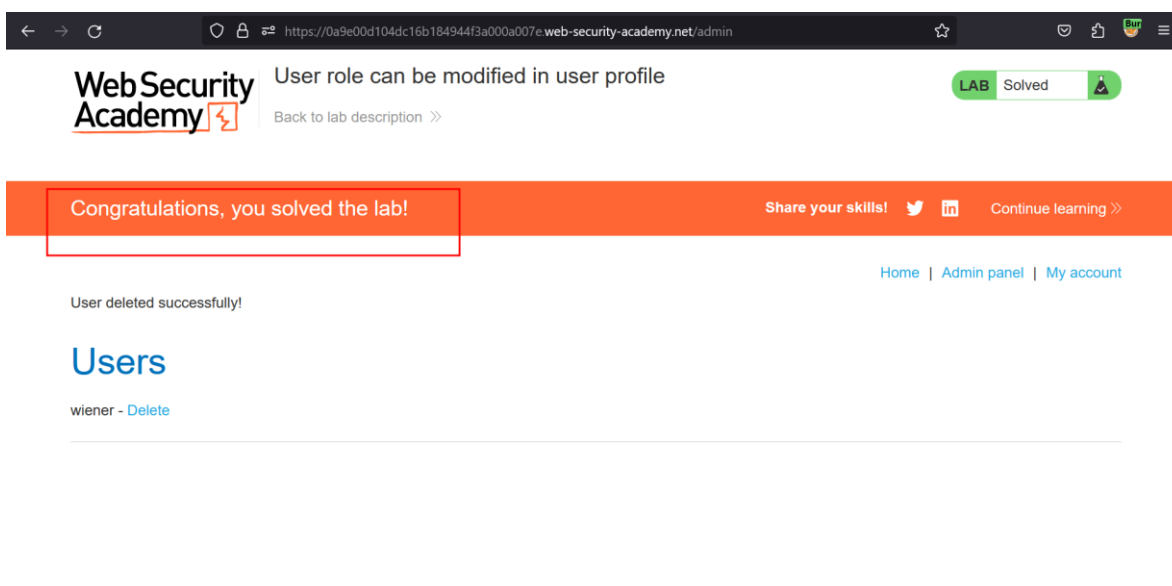
Daniel Carrillo
Omar Villalobos

Entramos a Admin panel y borramos a Carlos



The screenshot shows the Web Security Academy admin interface. At the top, there's a navigation bar with the logo, a title 'User role can be modified in user profile', and a 'LAB Not solved' status. Below this is a breadcrumb trail: Home | Admin panel | My account. The main section is titled 'Users' and contains a list of users: 'wiener' and 'carlos'. Each user has a 'Delete' link next to their name. A red arrow points to the 'Delete' link for 'carlos'.

Al eliminar Carlos se resuelve el laboratorio.

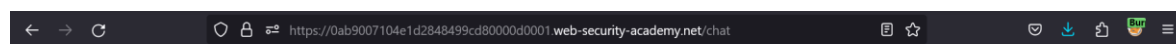


The screenshot shows the Web Security Academy admin interface after deleting the user 'carlos'. The top navigation bar now shows 'LAB Solved'. A large orange banner at the top says 'Congratulations, you solved the lab!'. Below this, a message states 'User deleted successfully!'. The 'Users' list now only contains 'wiener' with a 'Delete' link. The breadcrumb trail remains: Home | Admin panel | My account.

Daniel Carrillo
Omar Villalobos

Lab: Insecure direct object references

Ingresamos al live chat y empezamos a capturar



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

Live chat

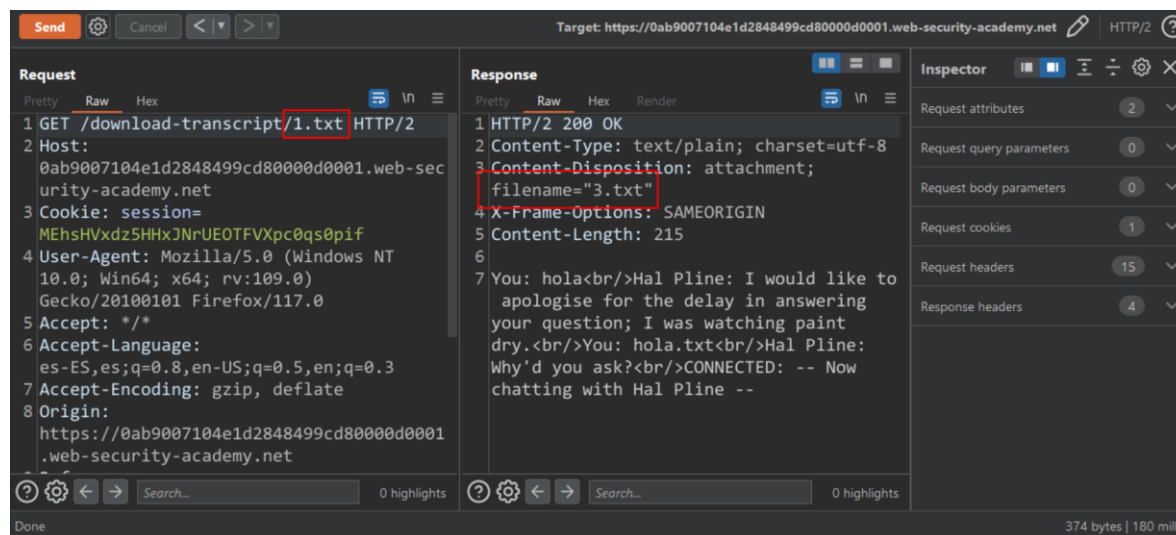
You: hola
Hal Pline: I would like to apologise for the delay in answering your question; I was watching paint dry.
You: hola.txt
Hal Pline: Why'd you ask?
CONNECTED: -- Now chatting with Hal Pline --

Your message:

Send

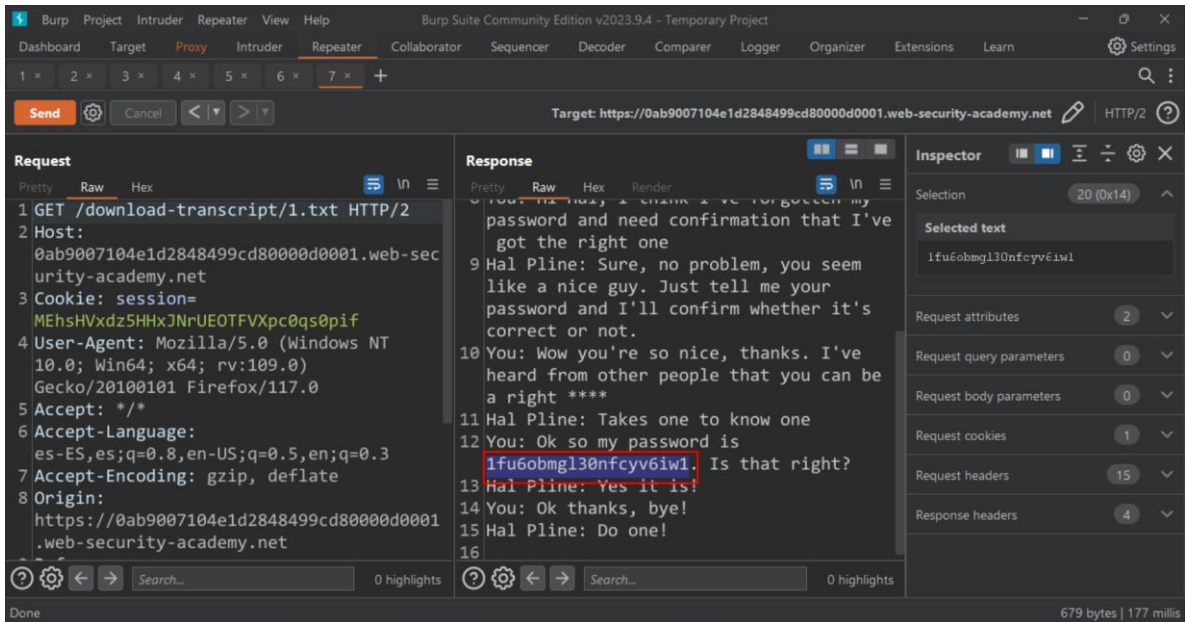
View transcript

Le damos en Repeater y enviamos, después vemos que se crean archivos .txt, cambiamos el numero 3 por 1.

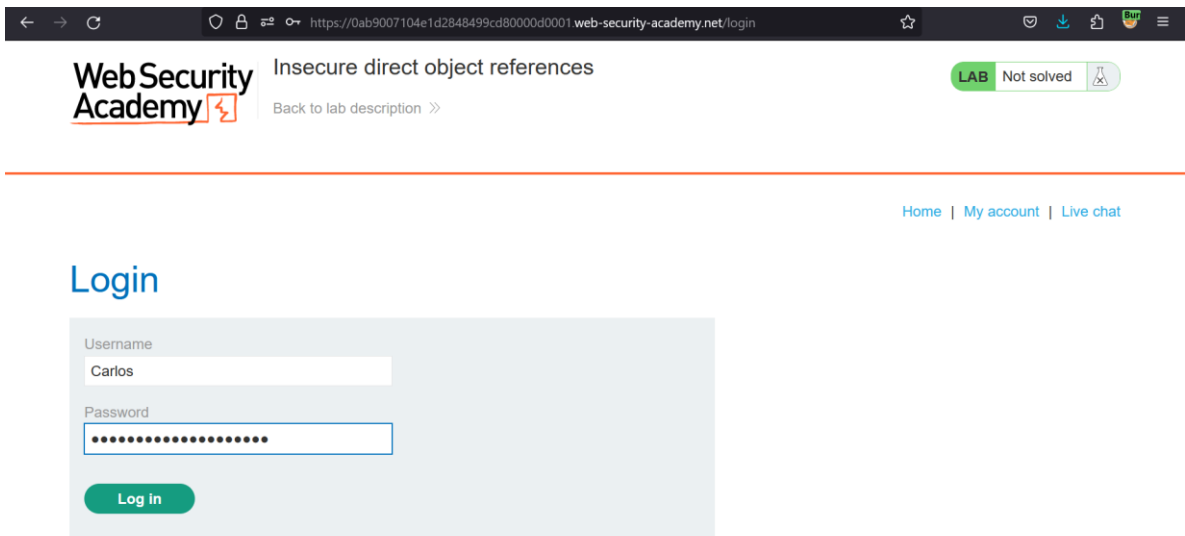


Daniel Carrillo
Omar Villalobos

Vemos en el chat de Carlos la contraseña.



La usamos para poder iniciar sesión.



Daniel Carrillo
Omar Villalobos

← → ↻ 🔒 📄 🔍 https://0ab9007104e1d2848499cd80000d0001.web-security-academy.net/my-account?id=carlos ☆ 📧 ⬇️ 📄 🌟 ☰

Web Security Academy ⚡

Insecure direct object references

LAB Solved 🔒

Back to lab description >>

Congratulations, you solved the lab!

Share your skills! 🐦 🌐 Continue learning >>

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

My Account

Your username is: carlos

Email

Update email

Lab: User ID controlled by request parameter with data leakage in redirect

Iniciamos sesión con las credenciales

← → ↻ 🔒 📄 🔍 https://0a4d00960320304c88d8dd210011004f.web-security-academy.net/login ☆ 📧 ⬇️ 📄 🌟 ☰

Web Security Academy ⚡

User ID controlled by request parameter with data leakage in redirect

LAB Not solved 🔒

Submit solution

Back to lab description >>

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

Login

Username

wiener

Password

•••••

Log in