

## **Ingeniería en Desarrollo de Software.**

### **Nombre de la Actividad.**

Actividad 3. Cross Site Scripting (XSS).

### **Actividad [#3]**

Etapa #3 – Cross Site Scripting (XSS).

### **Nombre del Curso.**

Auditoría Informática

**Tutor:** Jessica Hernández Romero.

**Alumno:** José Luis Martin Martínez.

**Fecha:** 10/10/2023.

## Índice.

<b>Contextualización y Actividades.....</b>	<b>4</b>
<b>Introducción.....</b>	<b>6</b>
<b>Descripción.....</b>	<b>8</b>
<b>Justificación.....</b>	<b>12</b>
<b>Etapa 1:</b>	
➤ Descripción del sitio web	
➤ Ataque al sitio	
<b>Etapa 2:</b>	
➤ Ataque al sitio	
<b>Etapa: 3</b>	
➤ Ataque al sitio	
<b>Conclusión.....</b>	<b>16</b>
<b>Referencias.....</b>	<b>18</b>

## Contextualización y Actividades.

Una empresa de software solicita realizar varias pruebas de seguridad en páginas web que no cuentan con los candados de seguridad.

Para esta tercera etapa se solicita realizar una prueba de **vulnerabilidad de Cross Site Scripting (XSS)**. En ella se debe obtener las credenciales que se ingresen para iniciar sesión. Después, desde *Burp Suite*, modificar la información para comprobar si se puede iniciar sesión o no.

### Actividad:

Utilizando el sitio web que se subió a Internet en la primera actividad, y el programa utilizado en la *Actividad 2*, trabajar con la vulnerabilidad *Cross Site Scripting (XSS)*. Así, con la ayuda de *Burp Suite*, captar las credenciales que se ingresen cuando se inicie sesión, y comprobar si se puede modificar.

## Introducción.

En esta tercera actividad, se nos pide realizar una prueba de **vulnerabilidad de Cross Site Scripting (XSS)**. En ella se debe obtener las credenciales que se ingresen para iniciar sesión. Después, desde *Burp Suite*, modificar la información para comprobar si se puede iniciar sesión o no. El Cross Site Scripting (XSS) es uno de los ataques más populares y vulnerables que se conoce. Está considerado como uno de los ataques más arriesgados para las aplicaciones web y también puede traer consecuencias muy graves. El XSS se compara a menudo con otros ataques similares en el lado del cliente, ya que durante este ataque se utilizan principalmente lenguajes del lado del cliente. Sin embargo, el ataque XSS se considera más arriesgado, debido a su capacidad para dañar incluso tecnologías, en teoría menos vulnerables. El ataque Cross Site Scripting es una inyección de código malicioso, que se ejecutará en el navegador de la víctima. El script malicioso puede guardarse en el servidor web y ejecutarse cada vez que el usuario llame a la funcionalidad correspondiente. También se puede realizar sin ningún script guardado en el servidor web. El objetivo principal de este ataque es robar los datos de identidad de un usuario, como cookies, tokens de sesión y otra información. En la mayoría de los casos, este ataque se utiliza para robar las cookies del usuario. Como sabemos, las cookies nos ayudan a iniciar la sesión automáticamente. Por lo tanto, con las cookies robadas, podemos iniciar sesión con otras identidades. Y esta es una de las razones por las que este ataque se considera uno de los más arriesgados. El ataque XSS se realiza en el lado del cliente. Se puede realizar con diferentes lenguajes de programación en el lado del cliente. Sin embargo, la mayoría de las veces este ataque se realiza con Javascript y HTML.

### **Descripción.**

Como mencionamos en la introducción, nos pide realizar una prueba de **vulnerabilidad de Cross Site Scripting (XSS)**. En ella se debe obtener las credenciales que se ingresen para iniciar sesión. La vulnerabilidad de Cross-Site Scripting (XSS) es un tipo de vulnerabilidad de seguridad en aplicaciones web que permite a un atacante injectar código malicioso, generalmente JavaScript, en una página web o aplicación web que luego se ejecuta en el navegador de un usuario. Esta vulnerabilidad puede permitir que el atacante:

1.- Robe información confidencial: El atacante puede utilizar el código malicioso para robar cookies de sesión, credenciales de usuario, datos personales u otra información sensible almacenada en el navegador del usuario.

2.- Suplante la identidad del usuario: Al robar cookies de sesión, un atacante puede hacerse pasar por un usuario legítimo y acceder a sus cuentas y datos.

3.- Realice acciones maliciosas en nombre del usuario: Una vez que el atacante tiene acceso a la sesión de un usuario, puede llevar a cabo acciones en su nombre, como realizar transacciones no autorizadas o cambiar la configuración de la cuenta.

#### **Existen varios tipos de XSS, incluyendo:**

1.- XSS Reflejado (Reflected XSS): En este caso, el código malicioso se inyecta en una URL o en los parámetros de una solicitud HTTP y se refleja en la respuesta del servidor. El usuario debe hacer clic en un enlace manipulado o visitar una URL específica para activar el ataque.

2.- XSS Almacenado (Stored XSS): En este tipo de XSS, el código malicioso se almacena en la base de datos de la aplicación web y se entrega a múltiples usuarios cuando acceden a

una página específica. Esto lo hace especialmente peligroso ya que puede afectar a un gran número de usuarios.

3.- XSS DOM-based (DOM XSS): Este tipo de XSS se produce cuando el código malicioso modifica el Document Object Model (DOM) de una página web, lo que puede llevar a cambios en la funcionalidad de la página sin necesidad de interacción con el servidor.

Para prevenir y remediar las vulnerabilidades de XSS, es necesario realizar una entrada de datos adecuada (sanitización) y la salida de datos (codificación) en la aplicación web, además de implementar políticas de seguridad, como encabezados HTTP de seguridad y utilizar bibliotecas y marcos de trabajo seguros. La detección y mitigación temprana de las vulnerabilidades de XSS son esenciales para proteger la integridad de las aplicaciones web y la privacidad de los usuarios.

### **Justificación.**

Es momento de poder justificar el por qué debemos de conocer a detalle la implementación. La vulnerabilidad de Cross-Site Scripting (XSS) es una amenaza de seguridad significativa y se justifica debido a varias razones clave: Explotación de información confidencial: La explotación exitosa de una vulnerabilidad de XSS permite a un atacante acceder a información confidencial almacenada en el navegador de un usuario, como cookies de sesión, credenciales de inicio de sesión y datos personales. Esto podría comprometer la privacidad y la seguridad de los usuarios. Suplantación de identidad (phishing): Al robar cookies de sesión o credenciales de usuario, un atacante podría hacerse pasar por un usuario legítimo, lo que puede llevar a la realización de acciones maliciosas en nombre del usuario, como el robo de cuentas o la propagación de mensajes de phishing.

Impacto en la integridad de los datos: XSS puede llevar a la manipulación no autorizada de datos en aplicaciones web. Un atacante puede realizar cambios en la información almacenada en la aplicación, lo que puede tener un impacto significativo en la integridad de los datos. Riesgos para la seguridad de la aplicación: Una vulnerabilidad de XSS podría permitir a un atacante tomar control de una aplicación web, lo que podría llevar a la ejecución de comandos maliciosos, la instalación de malware o la divulgación de información sensible.

Propagación de ataques: Los ataques de XSS a menudo se propagan rápidamente, ya que pueden afectar a múltiples usuarios a través de un solo punto de entrada malicioso. Esto puede tener un efecto dominó y dañar a un gran número de usuarios y sistemas. Cumplimiento legal y reputación: Las empresas y organizaciones pueden enfrentar repercusiones legales y daños en su reputación si se descubre que sus aplicaciones web son vulnerables a ataques de XSS. Los reguladores pueden imponer multas y sanciones, y los clientes pueden perder la confianza en la seguridad de sus servicios. Dada la amplia gama de riesgos y consecuencias asociados con la vulnerabilidad de XSS, es esencial que las organizaciones tomen medidas proactivas para identificar y remediar estas vulnerabilidades en sus aplicaciones web. Esto incluye la implementación de mejores prácticas de seguridad de desarrollo de aplicaciones, pruebas de seguridad regulares y la educación de los equipos de desarrollo y operaciones sobre cómo prevenir y mitigar las amenazas de XSS.

Burp Suite, es una plataforma capaz de llevar a cabo las auditorías de seguridad, de una organización con el objetivo de evitar ataques de software maliciosos.

Ahora bien, en este apartado analizaremos con mayor profundidad que se puede hacer con Burp Suite, qué herramientas ofrece esta plataforma para el cuidado de la ciber seguridad de una empresa. Burp Suite es una herramienta de pruebas de seguridad diseñada para evaluar

la seguridad de aplicaciones web y sistemas. Funciona como un proxy web que intercepta las solicitudes y respuestas HTTP entre un cliente web (como un navegador) y el servidor web.

### **Etapa 1:**

#### **➤ Descripción del sitio web**

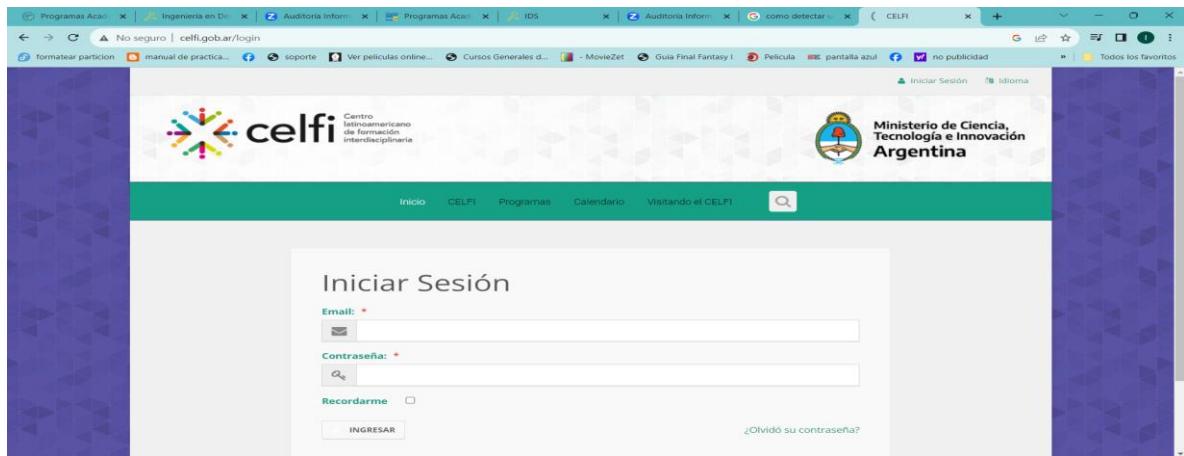
A continuación daremos detalle cómo se realizó el hacker, el protocolo de transferencia de hipertexto es muy vulnerable, hoy en día las páginas que lo llegan a usar son vulnerable ataque y robo de datos, para comprobar que se utilizó un analizador de paquetes llamado Wireshark , vamos a introducirnos en una página de http, para poder observar lo fácil que es extraer los datos del usuario, cabe recalcar que esto funciona solo si el usuario al cual extraeremos sus datos, debe estar conectado a la misma red que nosotros, es decir que para poder extraer datos del usuario con un analizador de paquetes. Ambos, tanto el como yo debemos de estar conectado a la misma red.

Entramos a la página y cómo podemos observar el navegador ya nos indica que no es seguro, ahora abrimos el wireshark que nos permite analizar paquetes de la red ya sea con cableado, bluetooth o inalámbrico. En este caso utilizaremos el inalámbrico y daremos doble clic en wifi y podemos observar como ya estamos analizando los paquetes que circulan por la red. Ahora vamos a ser la víctima de la vulnerabilidad. Ponemos el correo “[jm23270107@bachilleresdesonora.edu.mx](mailto:jm23270107@bachilleresdesonora.edu.mx)” y de contraseña **12345678**, este caso también nosotros estamos jugando el papel de víctima y vemos que logramos ingresar a la página, aunque nuestro correo no este dado de alta, abrimos el analizador de paquetes y pondremos un filtro en la parte de arriba, es para que nos muestre los paquetes con el protocolo de http. Al aplicar el filtro podemos observar que ya solo nos muestra que circularon por la red con el protocolo http y lo que nos importa es el “application login” le daremos doble clic y nos

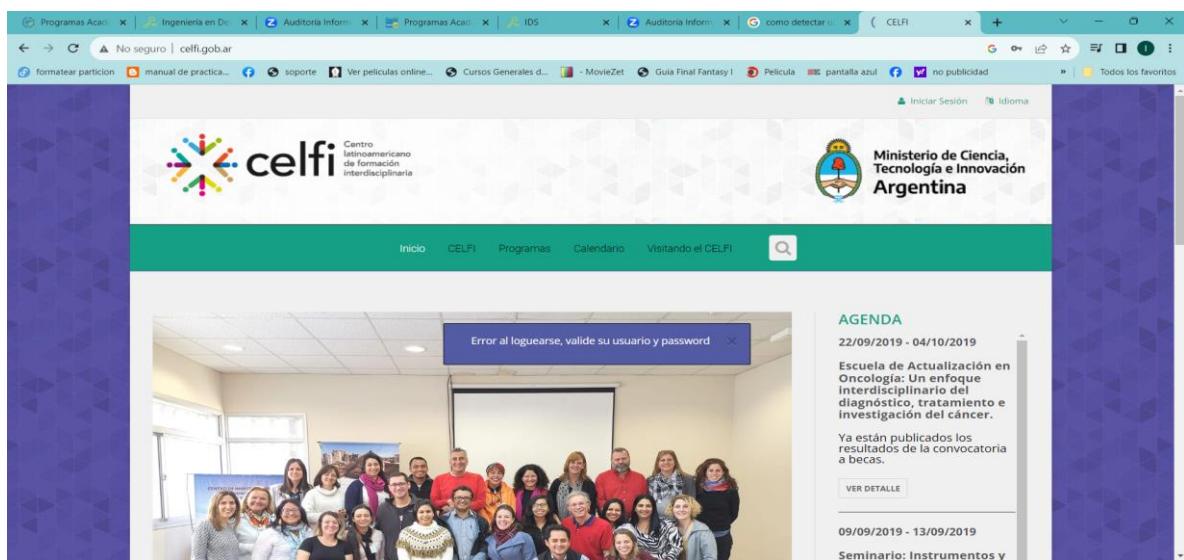
muestra todo lo que paso en ese momento el protocolo, internet, la transmisión y lo mas importante es (encoded) es donde nos va a mostrar el usuario y la contraseña que se introdujo en la página http.

### Página principal: <http://www.celfi.gob.ar/>

Inicio de sesión y contraseña. En el navegador nos indica que es una página insegura.



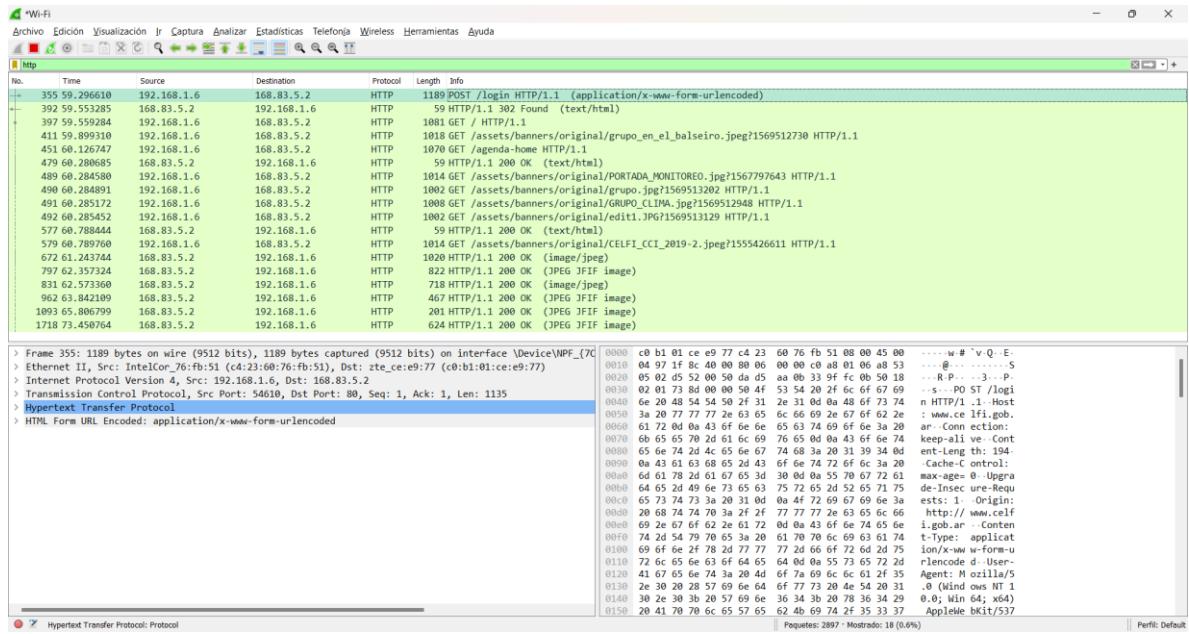
Ingresar página y automáticamente nos da el acceso a la conexión de base de datos aunque no estemos dado de alta.



## ➤ Ataque al sitio.

- Abrimos el analizador de paquetes y pondremos un filtro en la parte de arriba, es para que nos muestre los paquetes con el protocolo de http. Al aplicar el filtro podemos observar que ya solo nos muestra que circularon por la red con el protocolo http y lo que nos importa es el “application login” le daremos doble clic y nos muestra todo lo que paso en ese momento el protocolo, internet, la transmisión y lo más importante es (encoded) es donde nos va a mostrar el usuario y la contraseña que se introdujo en la página http.

Al aplicar el filtro podemos observar que ya solo nos muestra que circularon por la red con el protocolo http y lo que nos importa es el “application login”



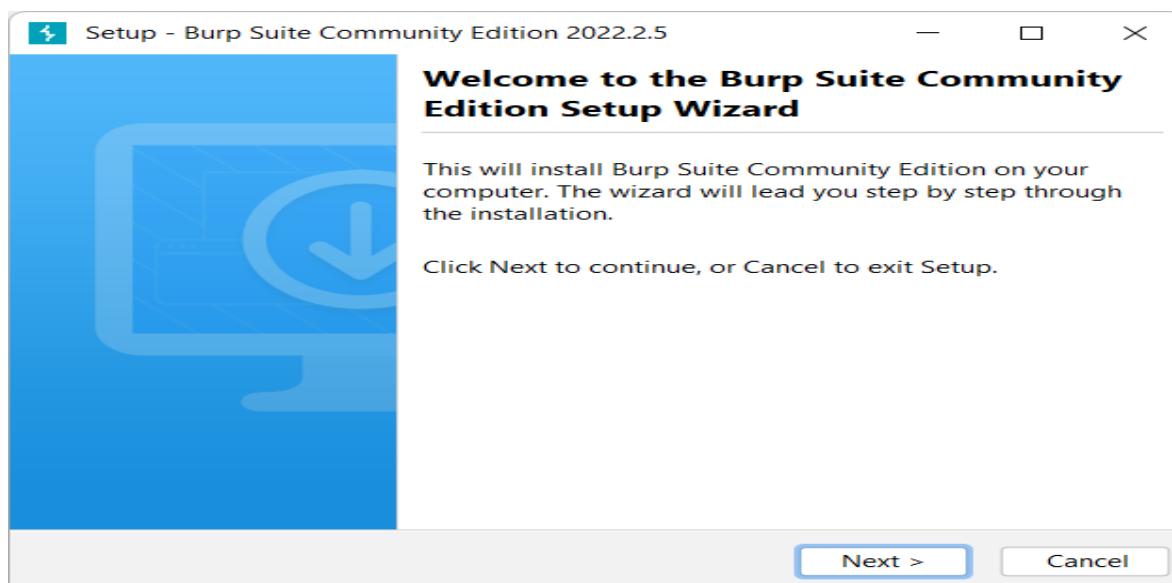
Encoded, es donde nos va a mostrar el usuario y la contraseña que se introdujo en la página

http.

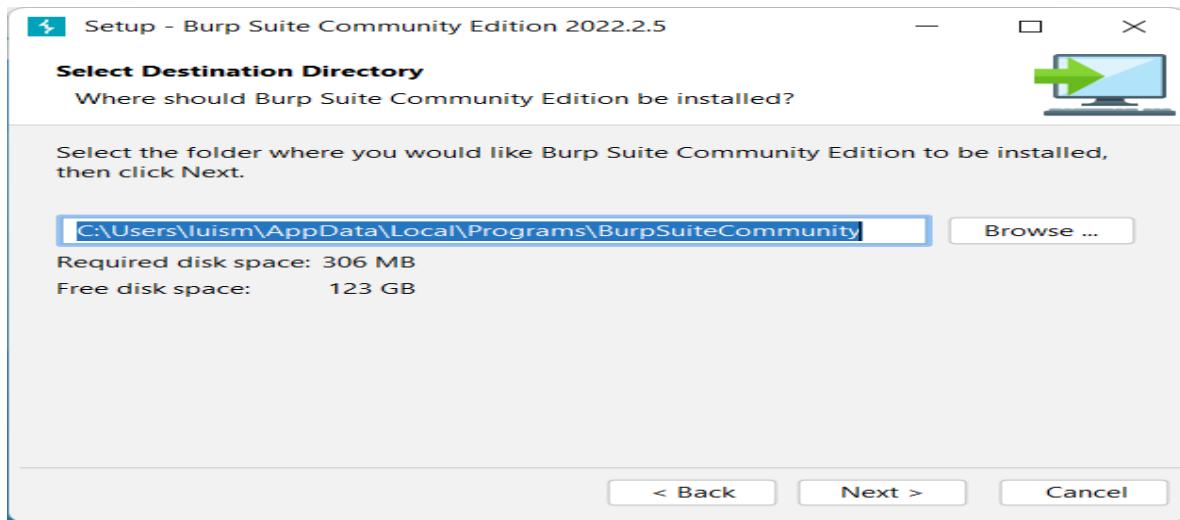
## **Etapa 2:**

## ➤ Ataque al sitio.

## Instalar Burp Suite Community Edition



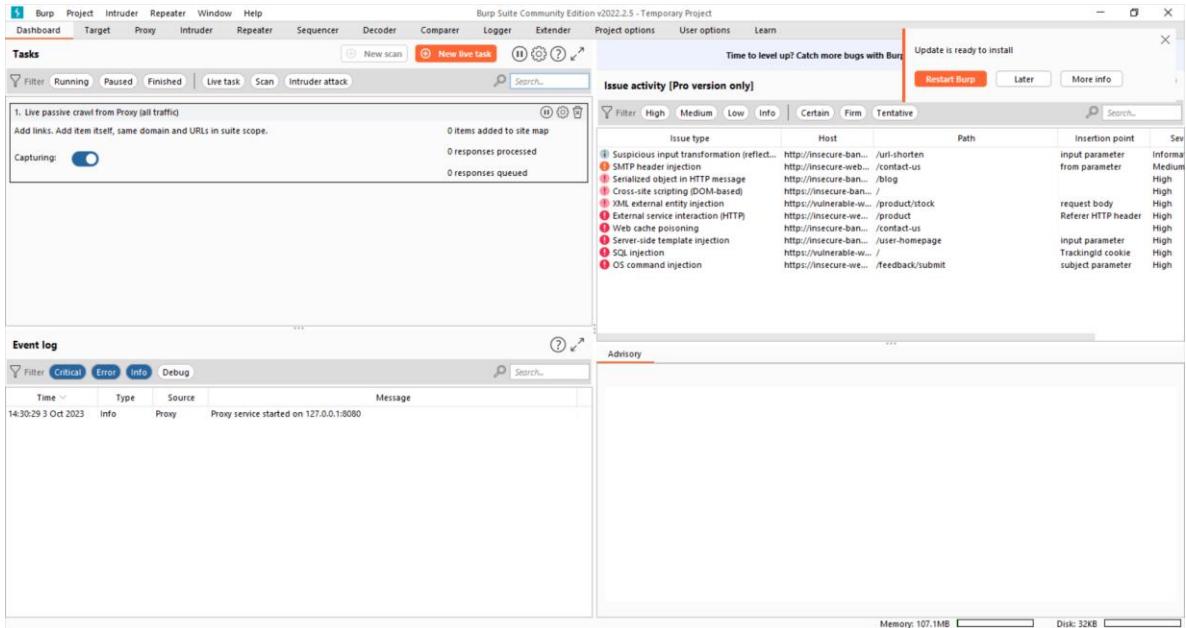
## Seleccionar directorio de destino



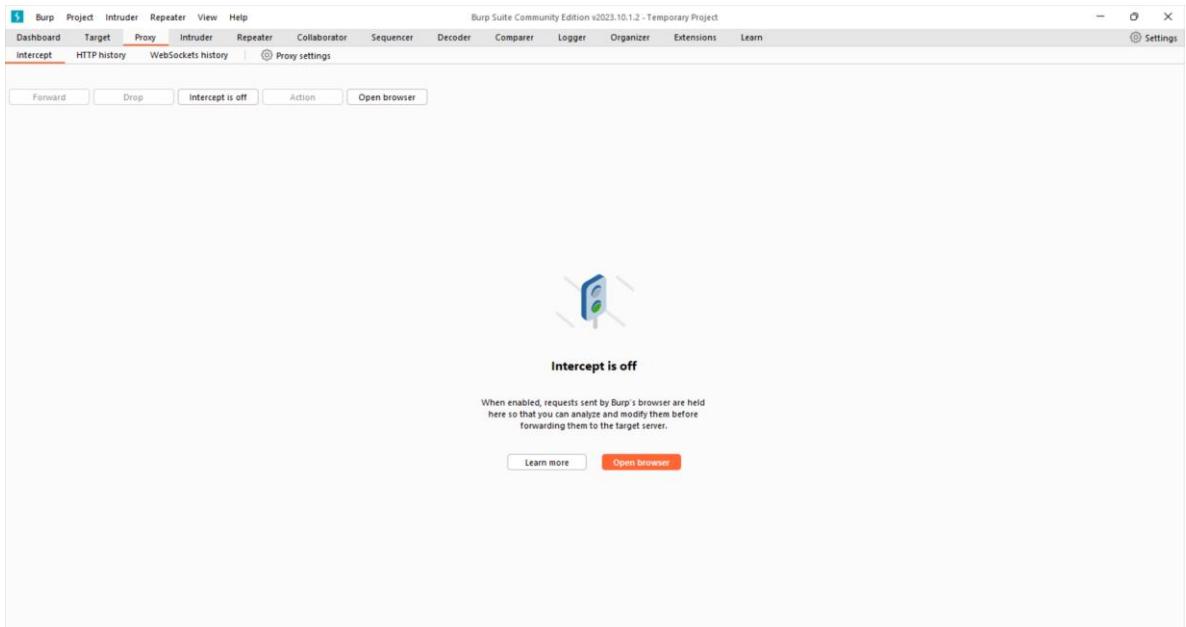
## Inicio de pantalla principal.



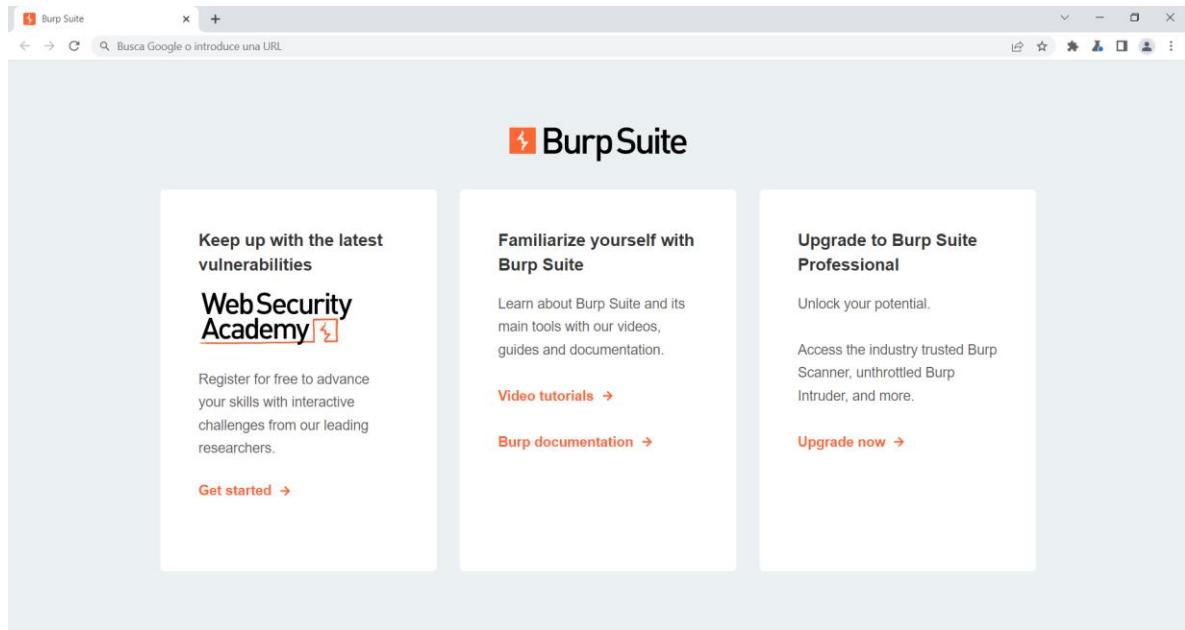
## Interfaz principal.



## Accediendo al Proxy dentro de Burp Suite



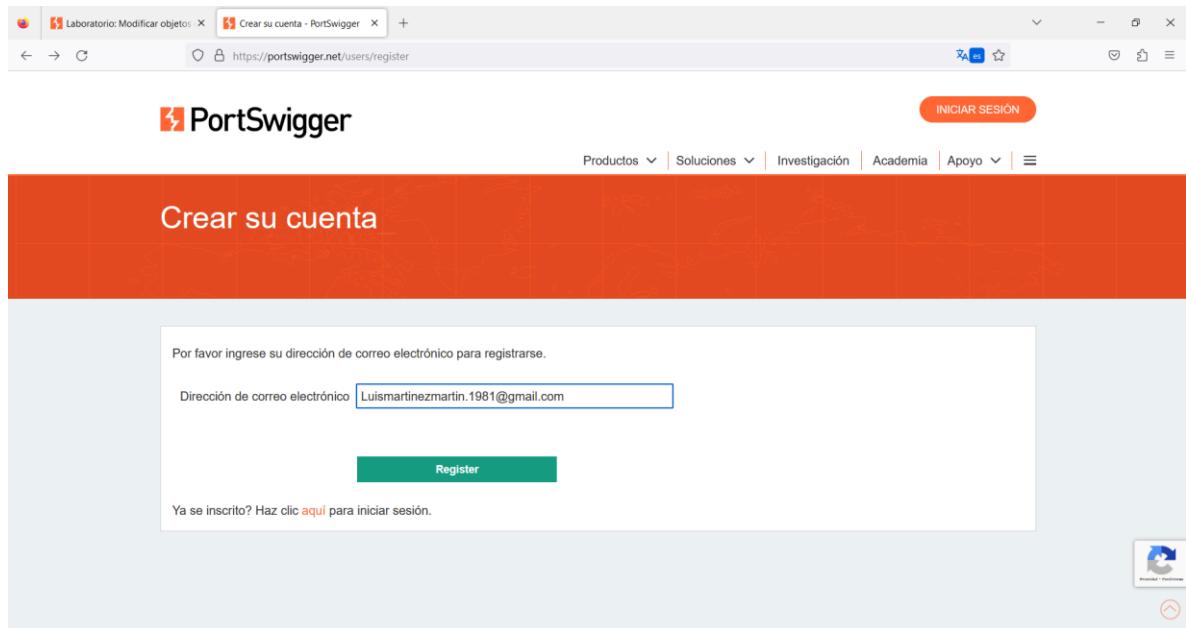
## Navegador del Burp Suite.



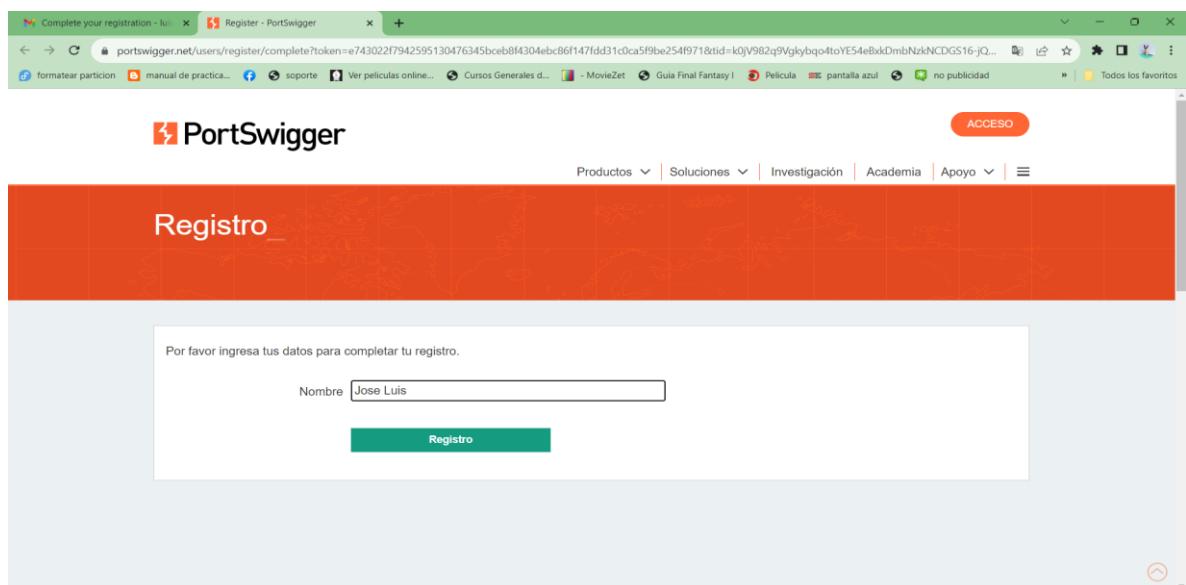
Se obtuvo información en cookie sesión de usuario en post /login

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener po
84	https://0a6700f6040684ad80b562f00b200e4.web-security-academy.net	POST	/login		✓	200	3140	HTML		Modifying serialized...		✓	79.125.84.16		22:27:27 3 ...	8080
85	https://0a6700f6040684ad...	GET	/academyLabHeader		✓	101	147					✓	79.125.84.16		22:27:27 3 ...	8080
86	https://0a6700f6040684ad...	GET	/my-account		✓	302	86					✓	79.125.84.16		22:27:32 3 ...	8080
87	https://0a6700f6040684ad...	GET	/login		✓	200	3148	HTML				✓	79.125.84.16		22:27:33 3 ...	8080
88	https://0a6700f6040684ad...	POST	/login		✓	101	147					✓	34.246.129.62		22:38:01 3 ...	8080
89	https://0a6700f6040684ad...	GET	/academyLabHeader		✓	200	3226	HTML				✓	34.246.129.62		22:38:03 3 ...	8080
90	https://0a6700f6040684ad...	POST	/login		✓	302	238					✓	34.246.129.62	session=Tzo0Ij...	22:38:44 3 ...	8080
91	https://0a6700f6040684ad...	GET	/my-account?tid=wiener		✓	200	3243	HTML				✓	34.246.129.62		22:38:45 3 ...	8080
92	https://0a6700f6040684ad...	GET	/academyLabHeader		✓	101	147					✓	34.246.129.62		22:38:45 3 ...	8080
93	https://0a6700f6040684ad...	GET	/my-account?tid=wiener		✓	200	3243	HTML				✓	34.246.129.62		22:50:47 3 ...	8080

## Crear cuenta de PortSwigger.



## Ingresar datos personales.



## Acceso.

The screenshot shows a web browser window with the PortSwigger logo at the top. Below it, a large orange header bar displays the word 'Acceso'. The main content area contains a form for logging in. It includes fields for 'Dirección de correo electrónico' (luismartinezmartin.1981@gmail.com) and 'Contraseña' (redacted). There is also a link 'Olvidaste tu contraseña?' and a checkbox for 'Recuérdame en esta computadora'. At the bottom of the form are two buttons: a green 'Acceso' button and a grey 'Crear una cuenta' button.

## Mi cuenta.

The screenshot shows a web browser window with the PortSwigger logo at the top. Below it, a dark blue header bar displays the word 'Mi cuenta'. The main content area is divided into several sections. On the left, there is a sidebar with links: 'Detalles personales' (selected), 'Certificaciones', 'Suscripciones', and 'Historial de pedidos'. The main content area has two main boxes: 'Detalles personales' (showing a profile picture of José Luis, his name, email luismartinezmartin.1981@gmail.com, and a 'Cambiar la contraseña' link) and 'Dirección de cuenta' (which says 'No hay dirección asociada con esta cuenta'). At the bottom, there is a section titled 'Tarjetas guardadas' with a placeholder box containing a plus sign and the text 'Agregar nueva tarjeta'.

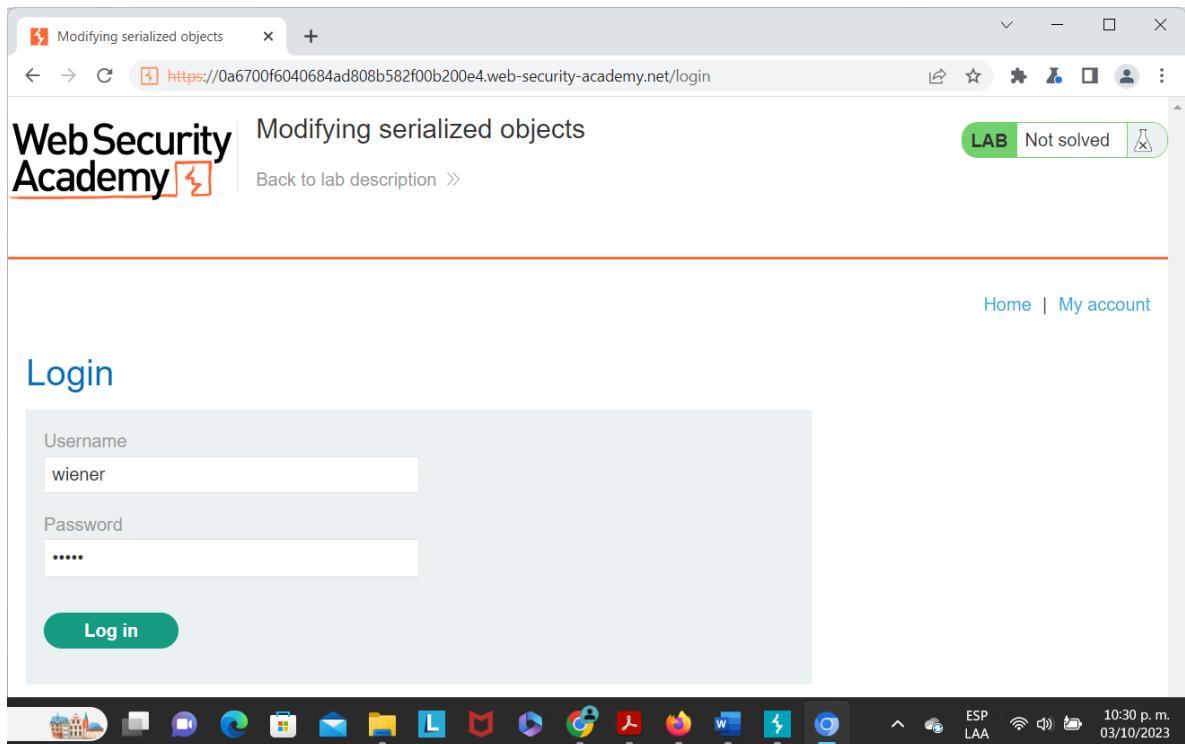
## Acceso al laboratorio.

The screenshot shows a browser window with the PortSwigger logo at the top. The main content area is titled "Laboratorio: Modificar objetos en serie". Below the title, there's a green button labeled "APPRENTICE". The page contains descriptive text about the lab, mentioning session serialization and privilege escalation, along with credentials: "wiener:peter". There's also a red button labeled "ACCESO EL LAB". A sidebar on the left provides navigation links related to serialization and deserialization.

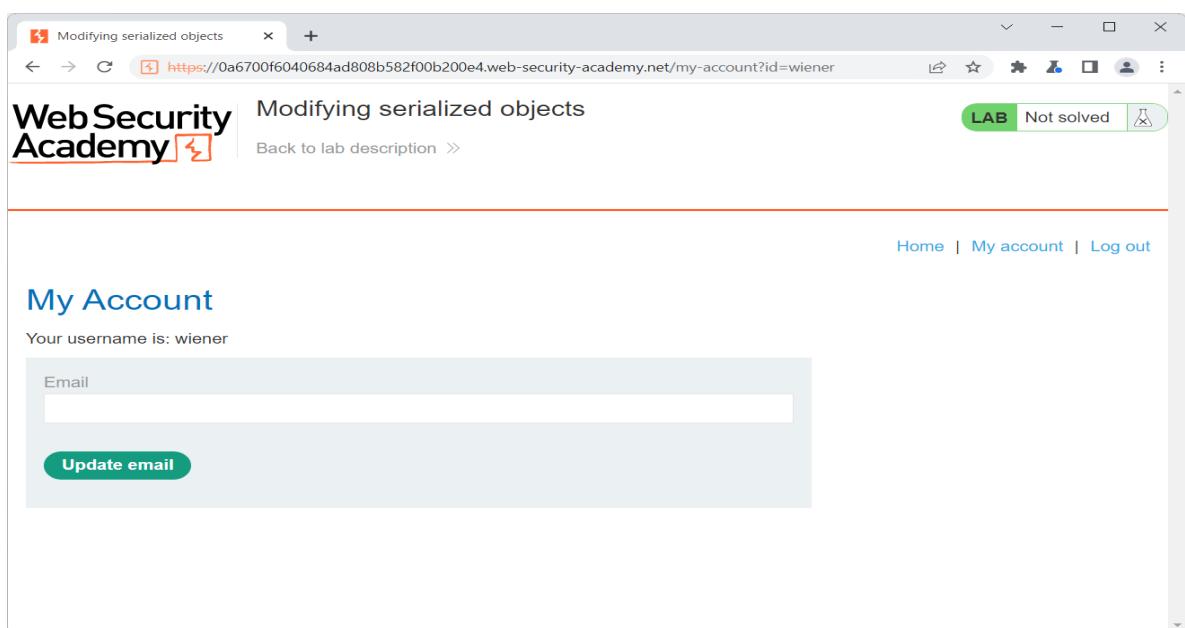
## Navegador

The screenshot shows a browser window with the Web Security Academy logo at the top. The main content area is titled "Modificar objetos serializados". It features a green button labeled "LAB No resuelto". Below the title, there's a "WE LIKE TO SHOP" section with four product cards: "Bebés de piel" (two babies in bunny hats), "Cosas de almohada gigante" (a person sitting on a large blue beanbag), "Adult Space Hopper" (an orange ball-like device), and "Gadgets plegados" (a paper airplane). Each card includes a star rating and price: \$82.78, \$23.44, \$73.60, and \$46.37 respectively. Each card has a "Ver detalles" button at the bottom.

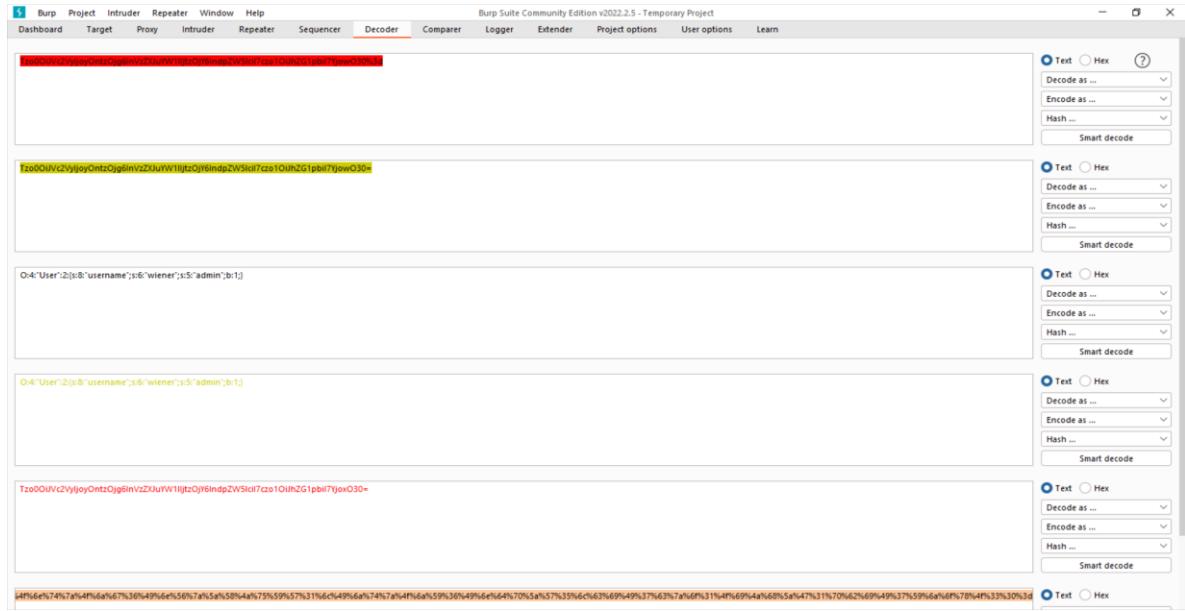
## Iniciar sesión my account



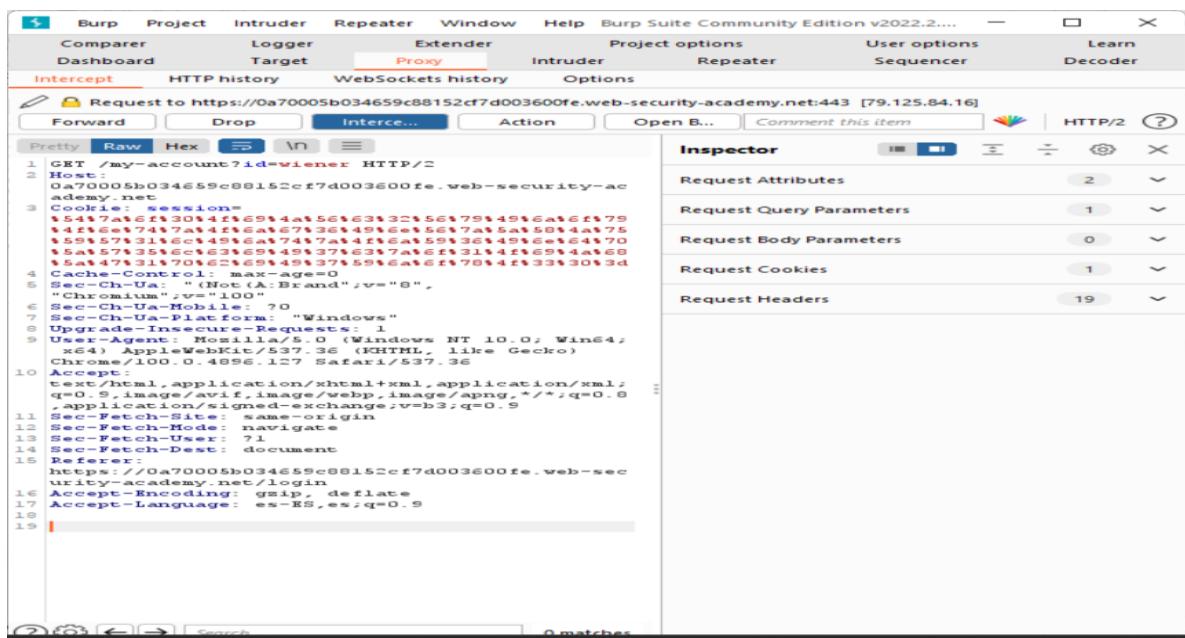
Usar nombre de Wiener y contraseña Peter.



## Cambio de credenciales de usuario normal a admin. en Decoder



Borrar la información anterior y pegar la que ya está codificada. Para que te pueda generar el Admin panel en el navegador.



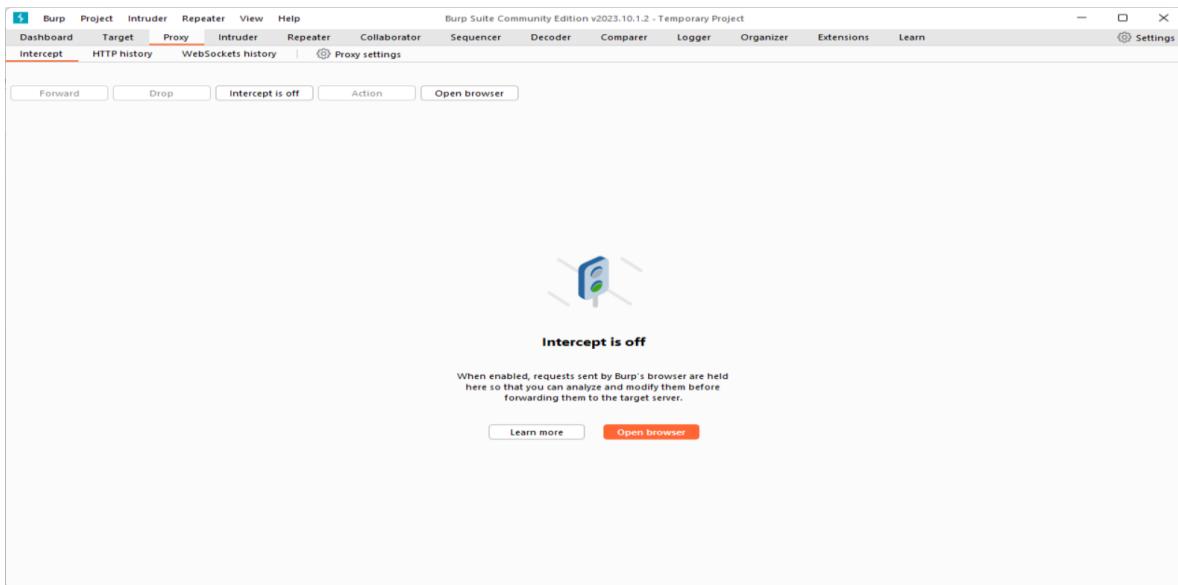
Una vez se hace el cambio de credenciales se actualiza el navegador, mi laptop se queda pensando...este paso es para que en el navegador aparezca el (admin panel). Y poder continuar con el siguiente paso borrar el nombre de Carlos.

### Etapa: 3

#### ➤ Ataque al sitio.

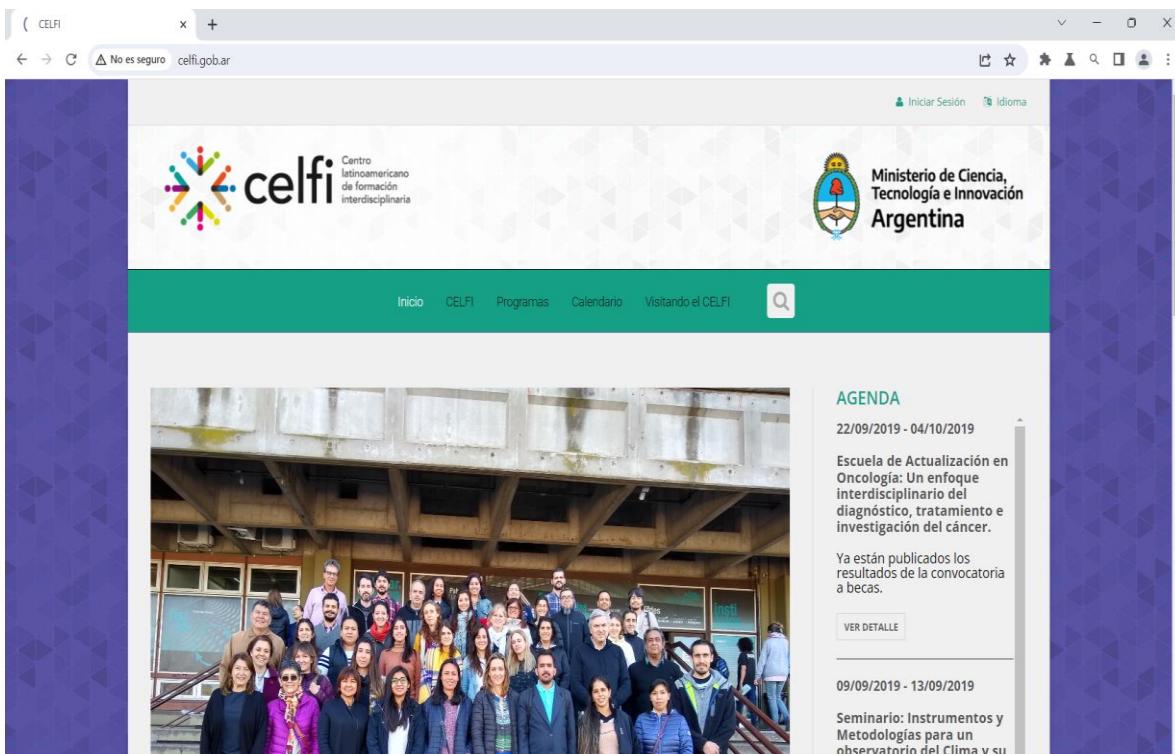
Entrar al Burp suite.

Ir a la sección proxy y dar click en abrir el navegador.

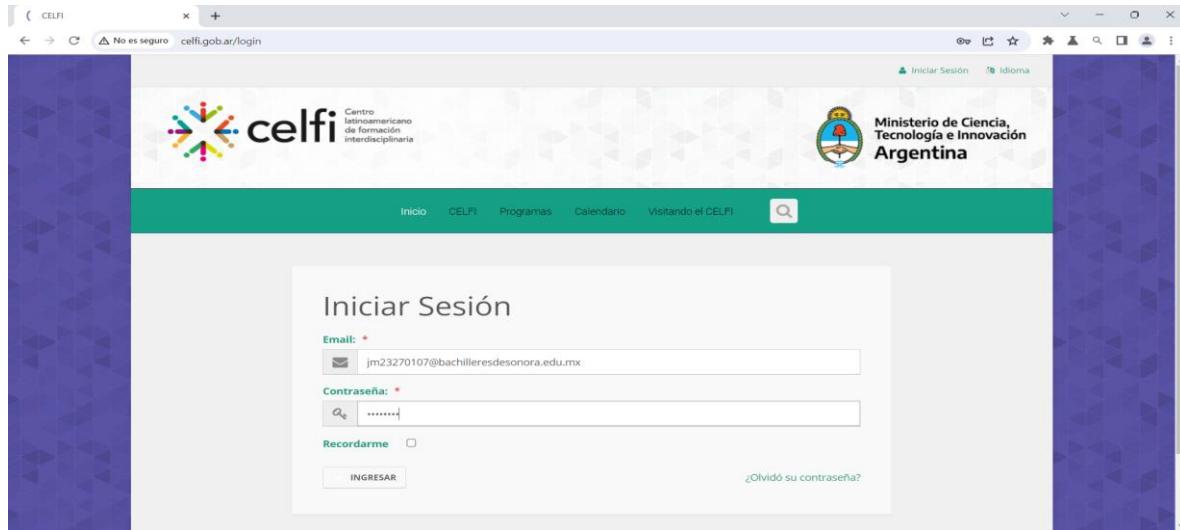


En el navegador que utiliza *Burp Suite*, entrar al sitio web del proyecto que se subió en la

### Actividad 1.



Dentro del sitio web, en la página de *login*, en el programa de Burp Suite, encender el interceptor. Luego, iniciar sesión con las credenciales correctas.



Iniciar sesión con las credenciales correctas y como podemos observar en Burp Suite a parecido la página que estamos interceptando, al final podemos ver las credenciales que inicio sesión y su contraseña.

Request to <http://www.celfi.gob.ar:80> [168.83.5.2]

Forw... Drop Action Open ... Comment this item HTTP/1

Pretty Raw Hex

```
1 POST /login HTTP/1.1
2 Host: www.celfi.gob.ar
3 Content-Length: 194
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://www.celfi.gob.ar
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.5938.132 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 Referer: http://www.celfi.gob.ar/login
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: es-ES,es;q=0.9
13 Cookie: celfimc_session=4CfjMSESpXWVQZLJyPmJHWT1FVTVHbkZ0cENnR
14 WzSUSQ1NxZiShB03gj1vsUbcZmgvN0x5ZhrM1ZrRjhFOH
15 d1SaqP2t5M3dsT31SPlhuvWdwDxndmZpZE5tMch5KySmNHr
16 w$XJ1enNpMCs3UTArPOVOWWUuHj1TMCTD7mhKOWS6drS1LmBL
NS91bDBCv2FxL1VGTOJyYTNIYmZPe1UOP50taySLN083Uugws
m5x4m4wNm0kOYTINLUTOS--0c112227948b85ee1785eeld7367
5le4ceS0487
Connection: close

ut_f0=%E2%9C%93&authenticity_token=
kBxgxOFRvCBZC046wGuljnrlruUA4oLUItjt%2FMGZ%2Bzj2DaM
+3D&user5Bemail%2B=jm23270107@bachilleresdesonora.edu.mx&
user5Bpassword%2D=1c345678&user5Bremember_me%2D=0
```

Inspector

Selection 39 (0x27)

Selected text jm23270107@bachilleresdesonora.edu.mx

Decoded from: URL encoding

jm23270107@bachilleresdesonora.edu.mx

Cancel Apply changes

Request attributes 2

Request query parameters 0

Request body parameters 5

Request cookies 1

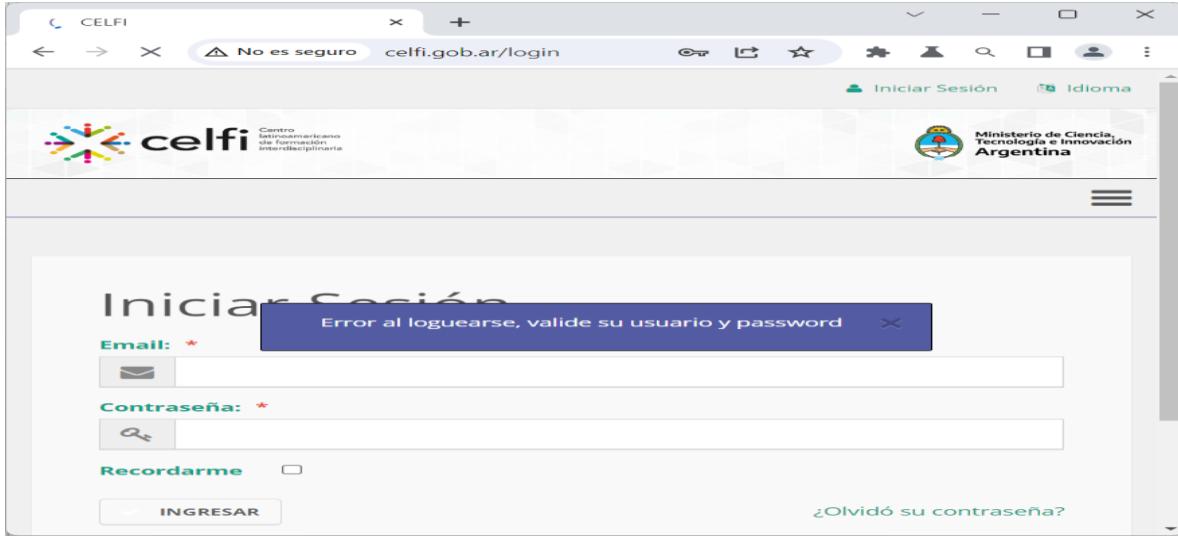
Request headers 13

En esta imagen alteramos la contraseña como va del 1 al 8, le vamos agregar dos números más que seria 9 y 10. (La contraseña 12345678910). Y le damos donde dice forward, como podemos observar nos manda un mensaje de error.

```

POST /login HTTP/1.1
Host: www.celfi.gob.ar
Content-Length: 190
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://www.celfi.gob.ar
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.5938.132 Safari/537.36
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
Referer: http://www.celfi.gob.ar/login
Accept-Encoding: gzip, deflate, br
Accept-Language: es-ES,es;q=0.9
Cookie: _celfims_session=WkIVZ3dybzEx0Eh3UEFxAc2VzSOZGbGIVamLZmhUUnIyaWQ1oWhUm3VlbkZGRmIca3dvhB10OWxuUhpzSUxHZkFtNDcrd0JoaF13cXBmN2tpZ2xqVmpRa2CPacNWeWVfQ25SSVY3VUQ5SFY0eHFwM1JZQ34DkC1kRGZ0lOTFUGGSwQ1avb1BpYnBo3Vw1M1ZSeml0BjyXp33sTDbh3ampmUnharUSG2nVzPsot+eWHNlcPpVQXqNMHGspsdlsWWNxZ2Jids09--c0a2926427aeffd09cdad7d96ce3d2067Se79de5a4
Connection: close
ut f8=%E2%9C%93&authenticity_token=TMTxhYVi03Mt2BxRhyghaeylX4pS2zW9NK5Y9rGzY38Y%3D&user%5Bemail%5D=jm23270107%40bachilleresdesonora.edu.mx&user%5Bpassword%5D=12345678910&user%5Bremember_me%5D=0

```



En esta segunda prueba vamos a alterar el correo electrónico [jm23270107@bachilleredesonora.edu.mx](mailto:jm23270107@bachilleredesonora.edu.mx). Ahora el correo se llamará [jm@bachilleredesonora.edu.mx](mailto:jm@bachilleredesonora.edu.mx) eliminando los números del correo y le damos en forward.

```

1 POST /login HTTP/1.1
2 Host: www.celfi.gob.ar
3 Content-Length: 190
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://www.celfi.gob.ar
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.5939.132 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Referer: http://www.celfi.gob.ar/login
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: es-ES,es;q=0.9
13 Content-Type: application/x-www-form-urlencoded
14 Content-Length: 190
15 Connection: close
16 utf8&X25C9%3authenticity_token=TMTxkYVi03H%2BxHhuyghaey1X4p9Z2w9Nk65Y9rGy30T%3D&user%5Bemail%5D=jm4Obachilleredesonora.edu.mx&user%5Bpassword%5D=12345678&user%5Bremember_me%5D=0

```

Como podemos observar la alerta que nos envía error en el usuario y contraseña.

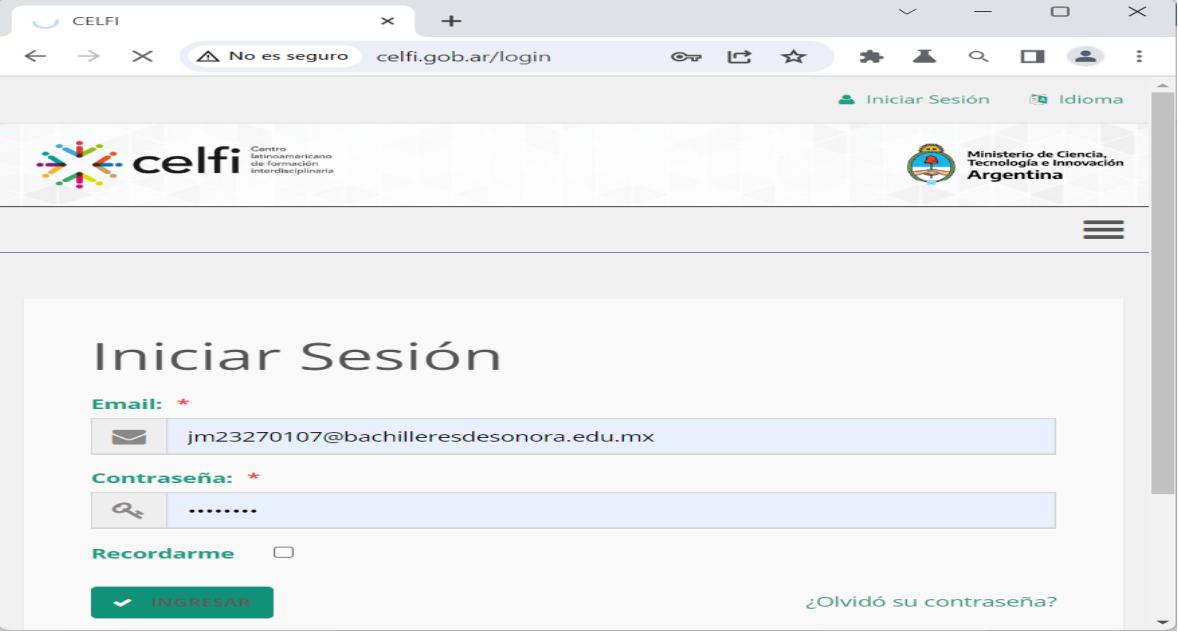


Se realizo una tercera prueba donde ingresaremos la misma cuenta del correo electrónico [jm23270107@bachilleresdesonora.edu.mx.](mailto:jm23270107@bachilleresdesonora.edu.mx.) Que utilizamos en las dos pruebas anteriores, dándole clic en forward y con la información que nos envía el sitio modificaremos los datos del usuario por los datos de otros usuarios dados de alta en la base de datos, de esta manera cambiaremos el correo y la contraseña, [jlmartin@gmail.com](mailto:jlmartin@gmail.com), y contraseña [abcd1234](#) como se muestra en la imagen.

```

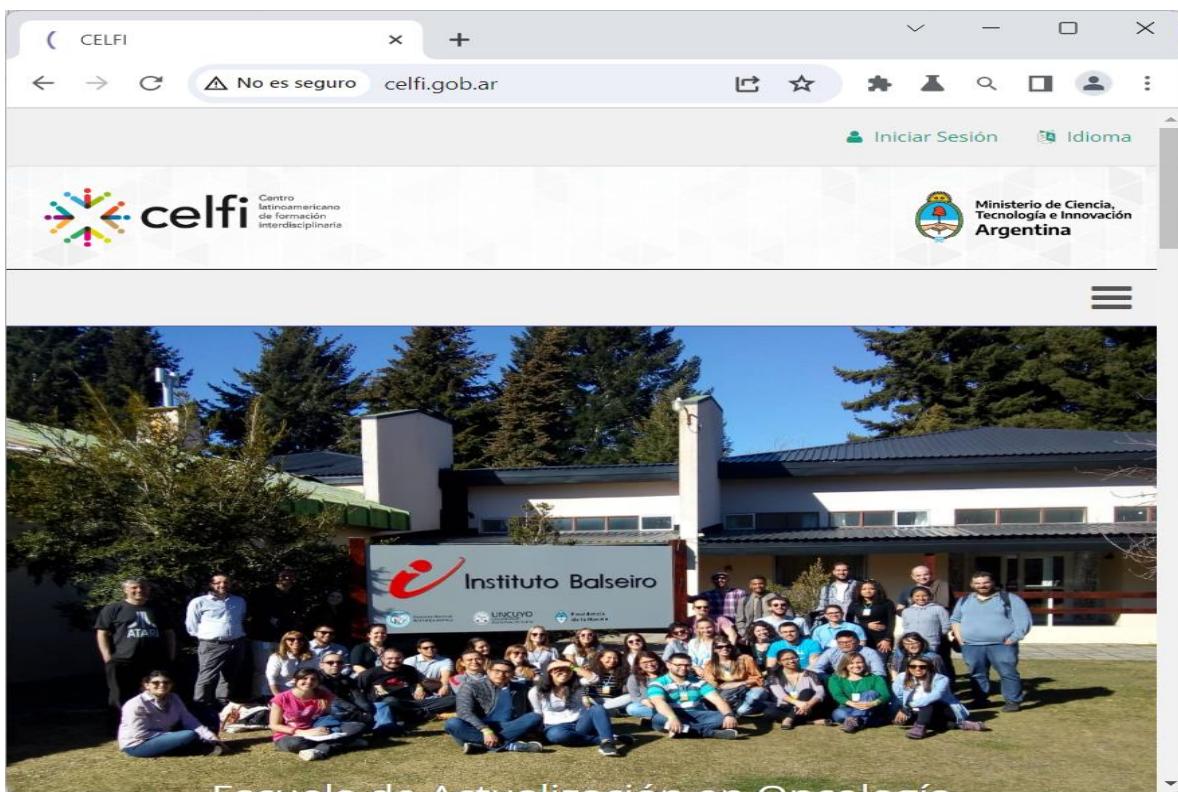
1 POST /login HTTP/1.1
2 Host: www.celfi.gob.ar
3 Content-Length: 177
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://www.celfi.gob.ar
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.5938.132 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 Referer: http://www.celfi.gob.ar/login
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: es-ES,es;q=0.9
13 Cookie: celficas_sessions=...; PHPSESSID=...; _ga=...; _gat_UA=...; _gid=...
14 Connection: close
15 ut f8+*E2tSCT93&authenticity_token=
16 0SuQvOZfujigoQSKEHt2FMP55gt2Pt2FSjZZoJpTt2FItqpNxV
17 kwt3D&user%5Bemail%5D=jlmartin%40gmail.com&
18 user%5Bpassword%5D=abcd1234&user%5Bremember_me%5D=0

```



The screenshot shows a web browser window for the CELFI website ([celfi.gob.ar/login](http://celfi.gob.ar/login)). The title bar says "CELFI". The address bar shows "No es seguro" and the URL "celfi.gob.ar/login". The page header includes the CELFI logo, the text "Centro Latinoamericano de formación interdisciplinaria", and the "Ministerio de Ciencia, Tecnología e Innovación Argentina" logo. The main content area is titled "Iniciar Sesión" (Log In). It has fields for "Email:" (jm23270107@bachilleresdesonora.edu.mx) and "Contraseña:" (redacted), a "Recordarme" checkbox, and a green "INGRESAR" (Enter) button. A link "¿Olvidó su contraseña?" (Forgot your password?) is also visible.

Como podemos observar si se pudo iniciar sesión con otras credenciales ya que encuentran grabadas en la base de datos.



## Conclusión.

Conocer y entender las vulnerabilidades establecidas en nuestro sitio web, con la ayuda de la herramienta Wireshark, podemos saber que estrategias de seguridad podemos implementar para evitar que nuestro software tenga vulnerabilidad y los datos puedan ser robados. En definitiva, para lograrlo, es vital saber cómo realizar auditorías que nos permita verificar la calidad y seguridad del programa o el sitio web que se está utilizando. Así es como identificar qué tipo de vulnerabilidad pudiéramos tener. La deserialización insegura es una vulnerabilidad crítica que ocurre cuando una aplicación o una API de serializa datos manipulados por un atacante en el lado del servidor. Durante este proceso, un atacante puede abusar de la lógica de la aplicación y realizar ataques de denegación de servicio (DoS), omitir autenticaciones o incluso ejecutar código malicioso de forma remota. Para prevenir esta vulnerabilidad, es importante implementar medidas de seguridad adecuadas, como la validación y autenticación de datos, y utilizar bibliotecas y marcos de trabajo seguros. El impacto de las amenazas a las vulnerabilidades de los sitios web ha sido tan alto que OWASP ha realizado año con año la lista de las 10 amenazas más peligrosas para los softwares y sus usuarios, incluidas las dos amenazas que vimos en esta unidad número dos. En esta actividad hemos aprendido a utilizar la herramienta de trabajo de BurpSuite. y así poder hackear la información, para entrar en modo incognito a cierta página para poder hacer modificaciones en sus sistemas sin que se den cuenta los usuarios. El objetivo principal de este ataque es robar los datos de identidad de un usuario, como cookies, tokens de sesión y otra información. En la mayoría de los casos, este ataque se utiliza para robar las cookies del usuario. Como sabemos, las cookies nos ayudan a iniciar la sesión automáticamente. Por lo tanto, con las

cookies robadas, podemos iniciar sesión con otras identidades. Y esta es una de las razones por las que este ataque se considera uno de los más arriesgados.

### **Link GitHub.**

<https://github.com/Jose-desarrollador/Jose-desarrollador.git>

### **Referencias.**

*Wireshark · go deep.* (s/f). Wireshark. Recuperado el 25 de septiembre de 2023, de <https://www.wireshark.org/>

*CELFI.* (s/f). Gob.ar. Recuperado el 25 de septiembre de 2023, de <http://www.celfi.gob.ar/>

*Professional / Community 2022.2.5.* (2022, April 20). Burp Suite Release Notes. <https://portswigger.net/burp/releases/professional-community-2022-2-5?requestededition=community&requestedplatform>

Castillo, A. (1586827274000). Deserialización insegura – OWASP Top 8.

Linkedin.com. <https://es.linkedin.com/pulse/deserializaci%C3%B3n-insegura-owasp-top-8-alexander-castillo>