



## **Actividad | 3 |**

### **Cross Site Scripting (XSS)**

#### **Auditoría Informática**

**Ingeniería en Desarrollo de Software**



**TUTOR: Jessica Hernández Romero**

**ALUMNO: Yanira Lizbeth Lopez Navarro**

**FECHA: 24/06/2024**

# Índice

Introducción .....	2
Descripción .....	3
Justificación .....	5
Etapa 1: .....	6
Etapa 2: .....	15
Etapa 3: .....	24
Conclusión .....	31
Referencias .....	32

## Introducción

El Cross Site Scripting (XSS) es una de las vulnerabilidades más comunes y peligrosas en las aplicaciones web. Esta vulnerabilidad permite a los atacantes insertar scripts maliciosos en páginas web legítimas, que luego son ejecutados por los navegadores de los usuarios que visitan dichas páginas. Los ataques XSS pueden tener consecuencias serias, como el robo de cookies de sesión, credenciales de usuario, la realización de acciones no autorizadas en nombre del usuario y la redirección a sitios web maliciosos.

En esta actividad, realizaremos una prueba de vulnerabilidad de Cross Site Scripting utilizando un sitio web previamente subido a Internet y la herramienta Burp Suite. Nuestro objetivo es determinar si el sitio web es vulnerable a ataques XSS y, de ser así, demostrar cómo un atacante podría capturar y modificar las credenciales de inicio de sesión. Con Burp Suite, interceptaremos y analizaremos el tráfico web para comprender mejor cómo funciona esta vulnerabilidad y cómo puede ser explotada.

Esta actividad no solo nos ayudará a entender la gravedad de los ataques XSS, sino que también nos proporcionará un entorno práctico para aplicar técnicas de pruebas de penetración. Al finalizar, tendremos un conocimiento más profundo sobre cómo identificar y mitigar las vulnerabilidades XSS, lo que contribuirá a mejorar la seguridad general de las aplicaciones web.

## Descripción

En el contexto presentado, una empresa de software está llevando a cabo una serie de pruebas de seguridad en sitios web que carecen de medidas de seguridad adecuadas, como los candados de seguridad HTTPS. Estas pruebas están diseñadas para identificar y corregir posibles vulnerabilidades que podrían ser explotadas por atacantes malintencionados. En particular, la actividad se enfoca en la detección y explotación de una vulnerabilidad conocida como Cross Site Scripting (XSS).

XSS es un tipo de vulnerabilidad que permite a un atacante injectar scripts maliciosos en páginas web vistas por otros usuarios. Estos scripts pueden ser utilizados para robar información sensible, como credenciales de inicio de sesión, ejecutar acciones no autorizadas en nombre del usuario, o redirigir a los usuarios a sitios maliciosos.

La actividad específica que se solicita en esta tercera etapa implica utilizar el sitio web que se subió a Internet en una actividad previa y el programa Burp Suite, una herramienta de prueba de penetración que permite interceptar, modificar y analizar tráfico web. El objetivo es realizar una prueba de vulnerabilidad XSS de la siguiente manera:

1. Capturar las credenciales que los usuarios ingresan al iniciar sesión en el sitio web. Esto se hace inyectando un script malicioso en la página web que capture y envíe estas credenciales al atacante.
2. Utilizar Burp Suite para interceptar y modificar la información capturada, con el fin de comprobar si es posible utilizar estas credenciales para iniciar sesión en el sitio web.

Al realizar esta prueba, se pretende demostrar la gravedad de las vulnerabilidades XSS y la importancia de implementar medidas de seguridad adecuadas para proteger los datos de los usuarios y la integridad del sitio web. Esta actividad no solo ayuda a identificar fallos de seguridad, sino que también proporciona un entorno controlado para aprender y aplicar técnicas de pruebas de penetración, contribuyendo al fortalecimiento de las defensas ciberneticas de la empresa.

## Justificación

En esta actividad es esencial garantizar la seguridad y la integridad de las aplicaciones web que utilizamos a diario. En un mundo donde cada vez más aspectos de nuestra vida dependen de la tecnología y de las interacciones en línea, la protección de nuestros datos personales y financieros se vuelve fundamental.

Realizar este tipo de pruebas nos permite identificar puntos débiles en el sitio web antes de que los atacantes puedan explotarlos. Al comprender cómo funciona XSS y cómo los hackers pueden aprovecharse de estas vulnerabilidades, podemos desarrollar estrategias más efectivas para proteger la información sensible de los usuarios. Además, utilizar herramientas como Burp Suite nos ofrece una visión detallada del tráfico web, ayudándonos a detectar y corregir problemas de seguridad que podrían pasar desapercibidos de otra manera.

Implementar estas soluciones no solo nos prepara para enfrentar amenazas actuales, sino que también fortalece nuestra postura de seguridad a largo plazo. Al aprender y aplicar estas técnicas, no solo protegemos nuestros sistemas, sino que también mejoramos nuestra capacidad para anticipar y responder a futuras amenazas. En resumen, las pruebas de XSS son una inversión crucial para mantener la confianza de los usuarios y garantizar que las aplicaciones web sean seguras y confiables.

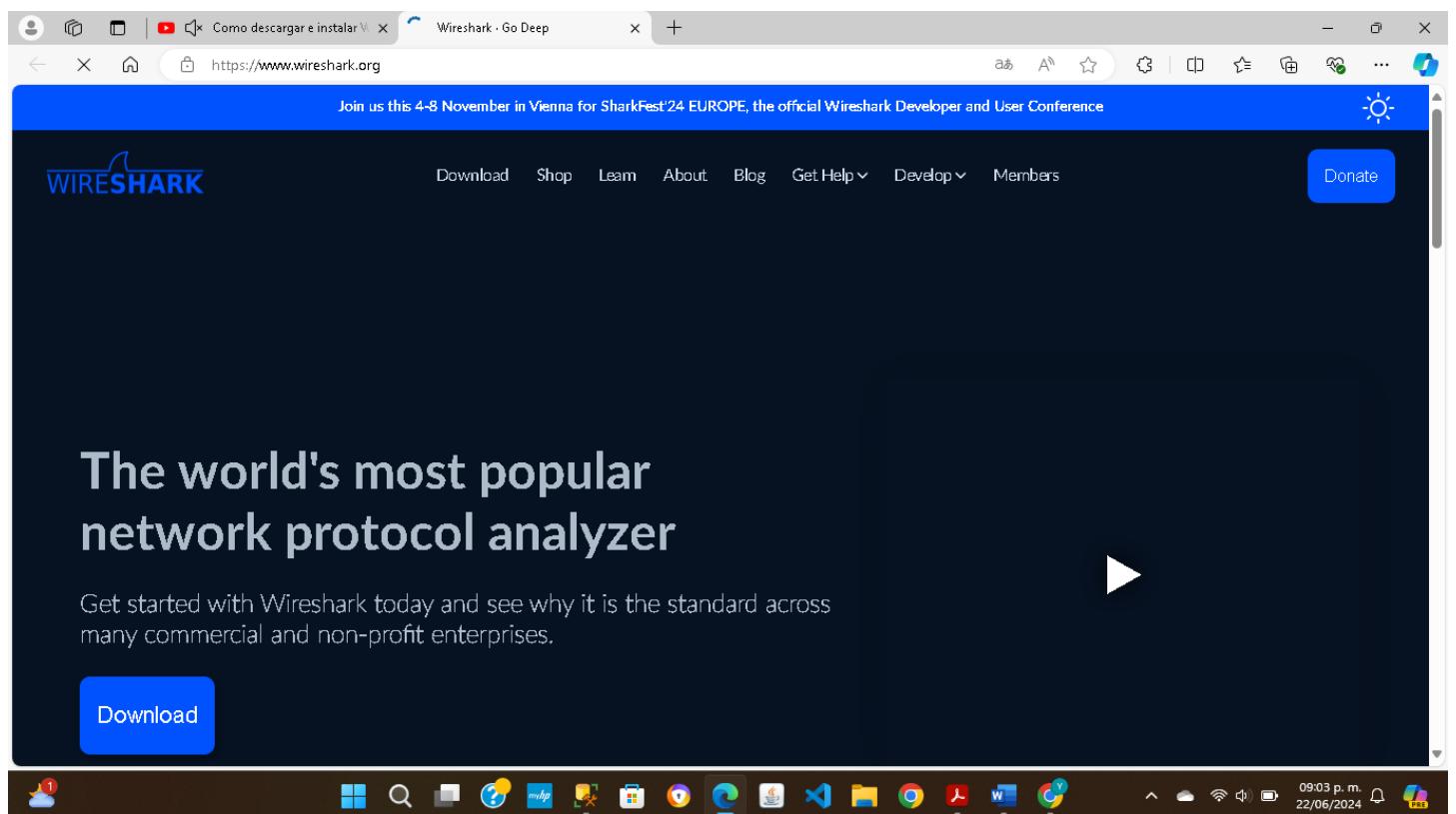
## Etapa 1: Descripción del sitio web

De acuerdo a lo solicitado en la actividad se llevó a cabo la Selección de un proyecto web realizado anteriormente, aunque no fue de mi autoría cumple con las características solicitadas en la actividad.

- Función de iniciar sesión y de registro de usuarios
- Conexión con una base de datos

<http://www.pruebadeuso.com/index.php?r=site/login>

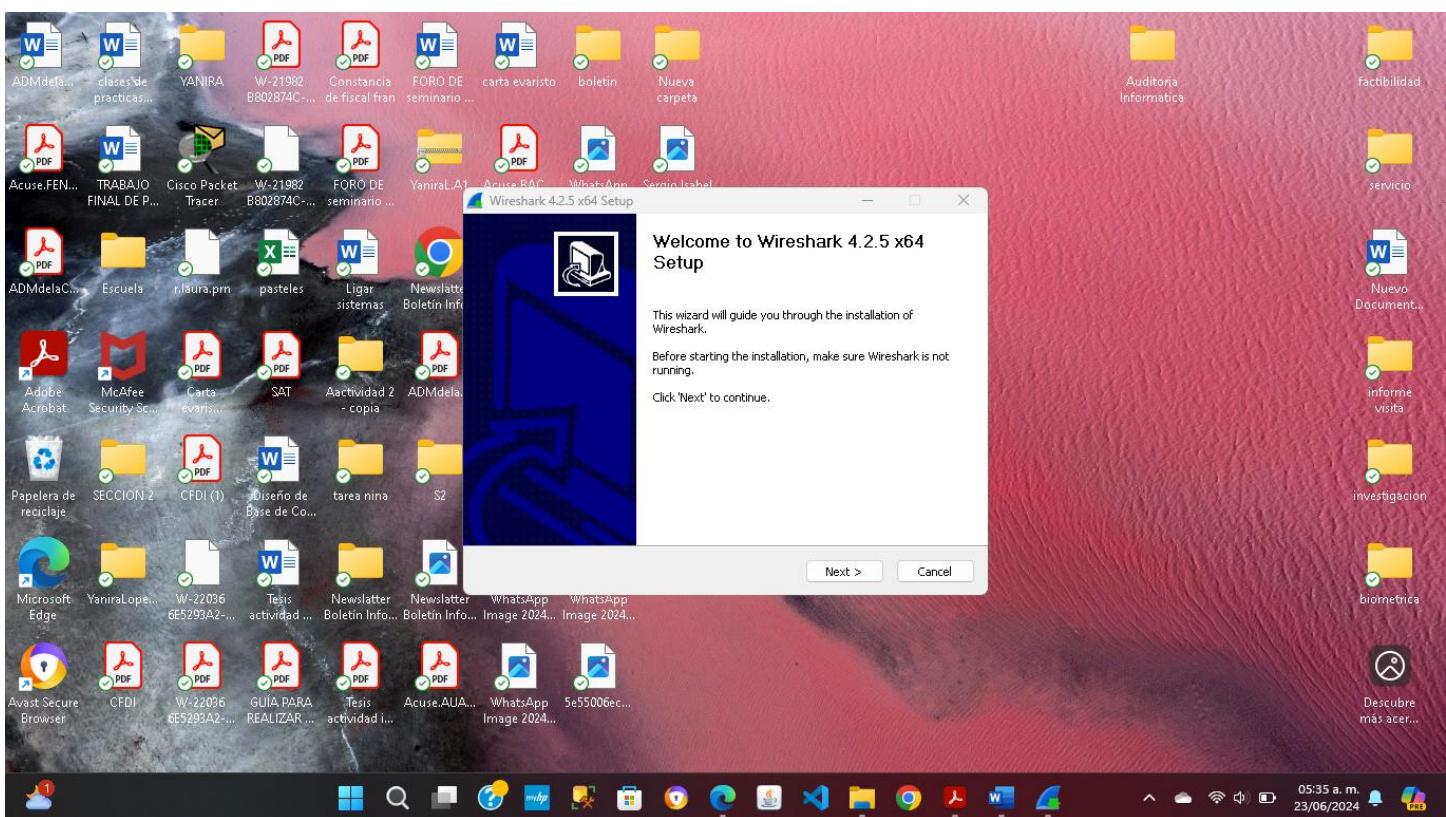
A continuación, en la siguiente imagen podemos observar la página que nos permite descargar la herramienta recomienda para el desarrollo de la actividad.



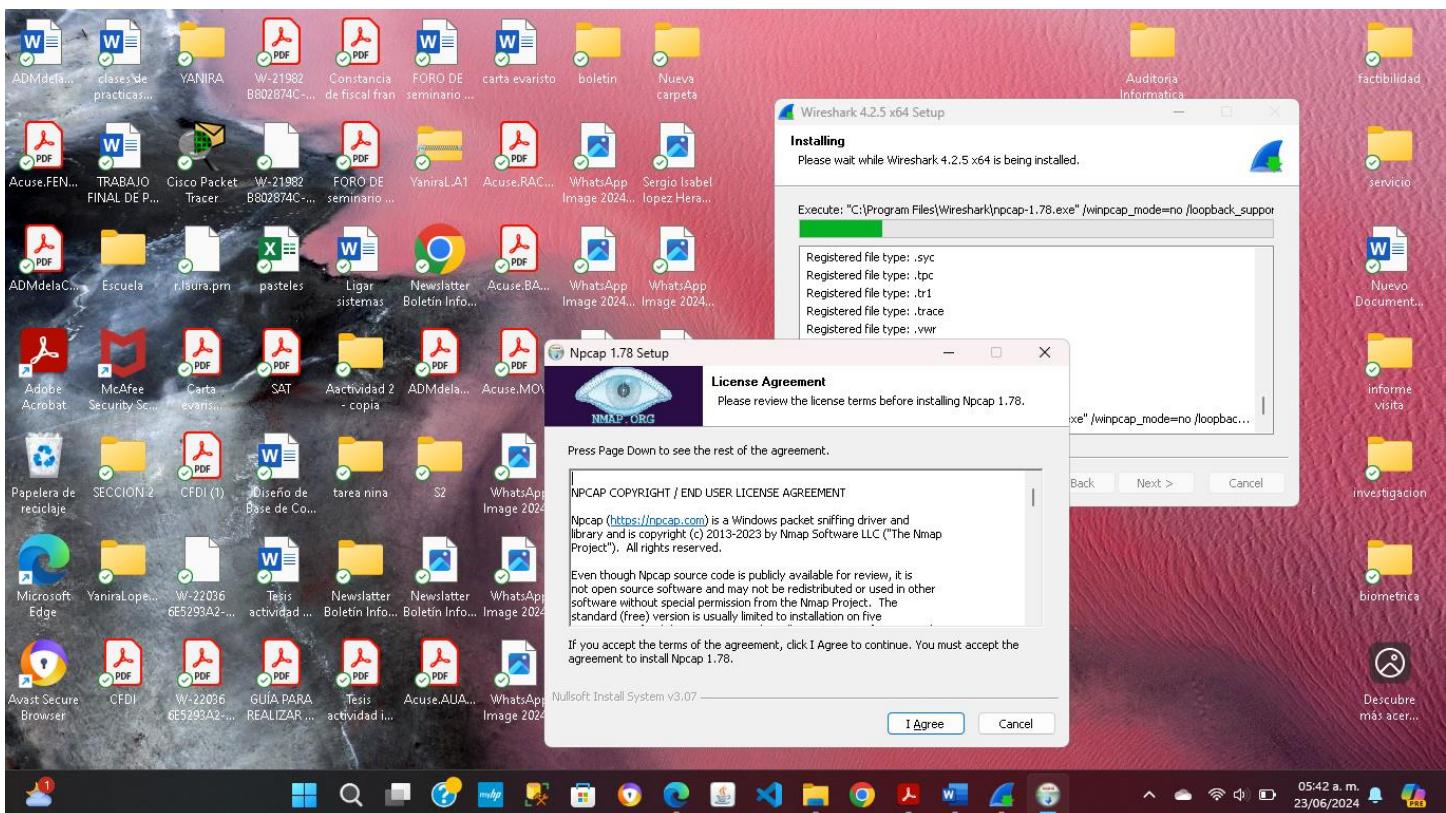
A continuación, seleccionamos es instalador para Windows x64 ya que es el compatible con mi equipo

The screenshot shows the official Wireshark download page. On the left, there's a sidebar with a list of download links for different platforms. The main content area has a heading "Descargar Wireshark". Below it, there's a section for the "Versión estable: 4.2.5" which includes links for "Instalador de Windows x64", "Instalador de Windows Arm64", "Windows x64 PortableApps®", "Imagen de disco de macOS Arm", "Imagen de disco Intel de macOS", and "Código fuente". To the right of this, there are three ads: one for LiveAction (Unmatched Network Visibility, Actionable Intelligence), one for FMADIO (10G 40G 100G PACKET CAPTURE, Never Drop Packets!), and one for Veeam (FREE TRIAL, Veeam Data Platform 23H2 Update). The bottom of the screen shows the Windows taskbar with various pinned icons and the system tray.

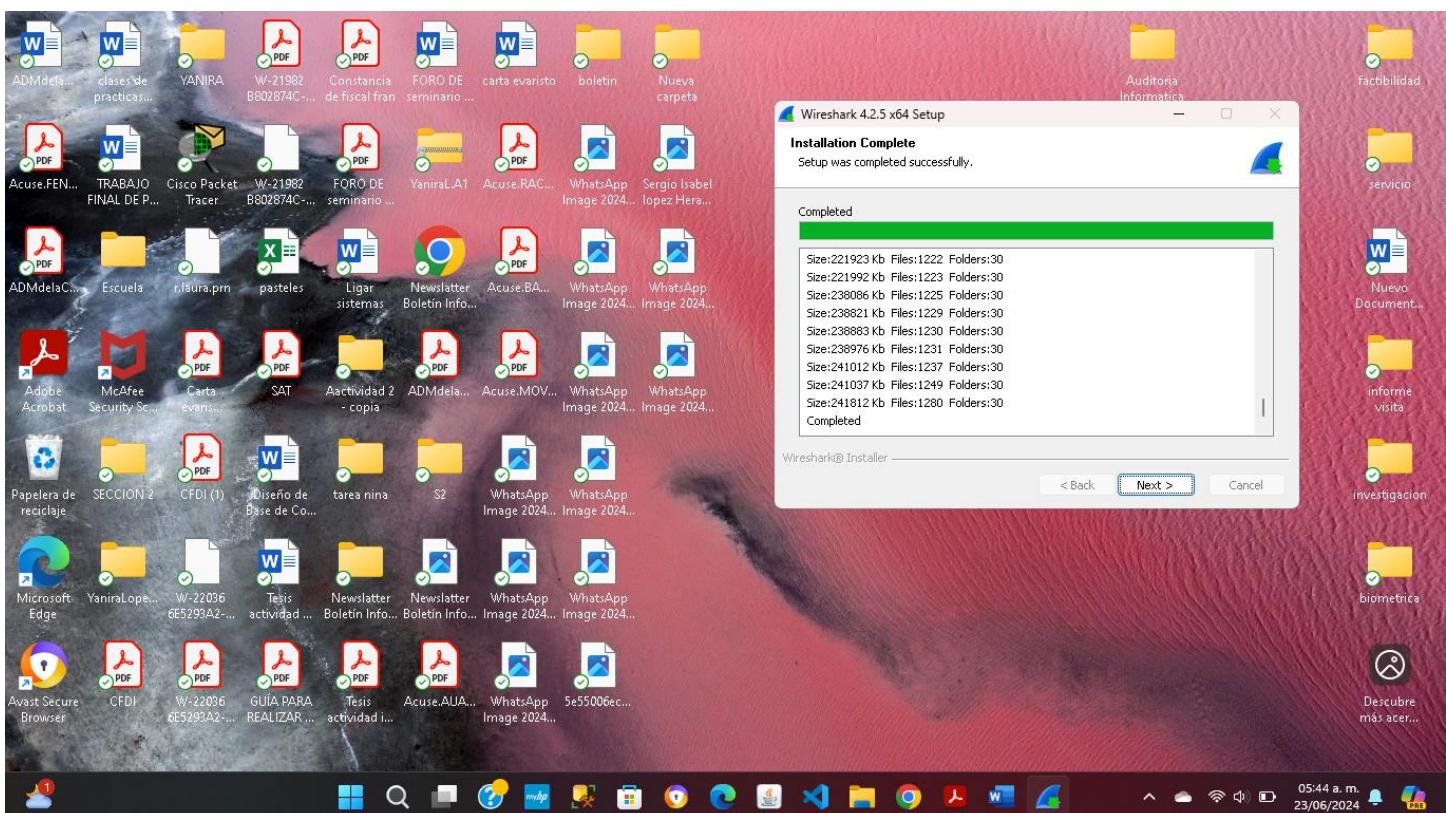
Una vez que Wireshark fue descargado procedemos su instalación.



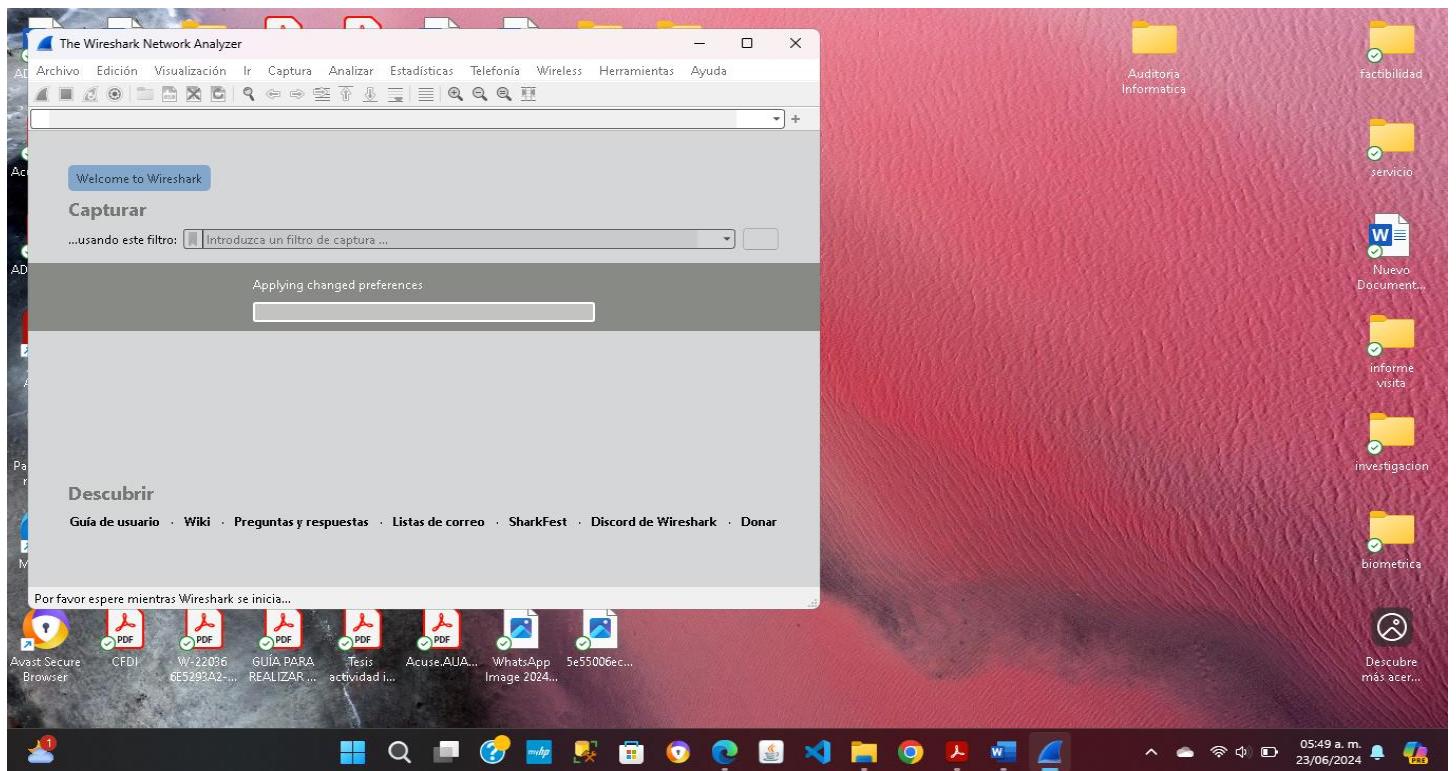
En la siguiente imagen se observa el avance de la instalación de Wireshark.



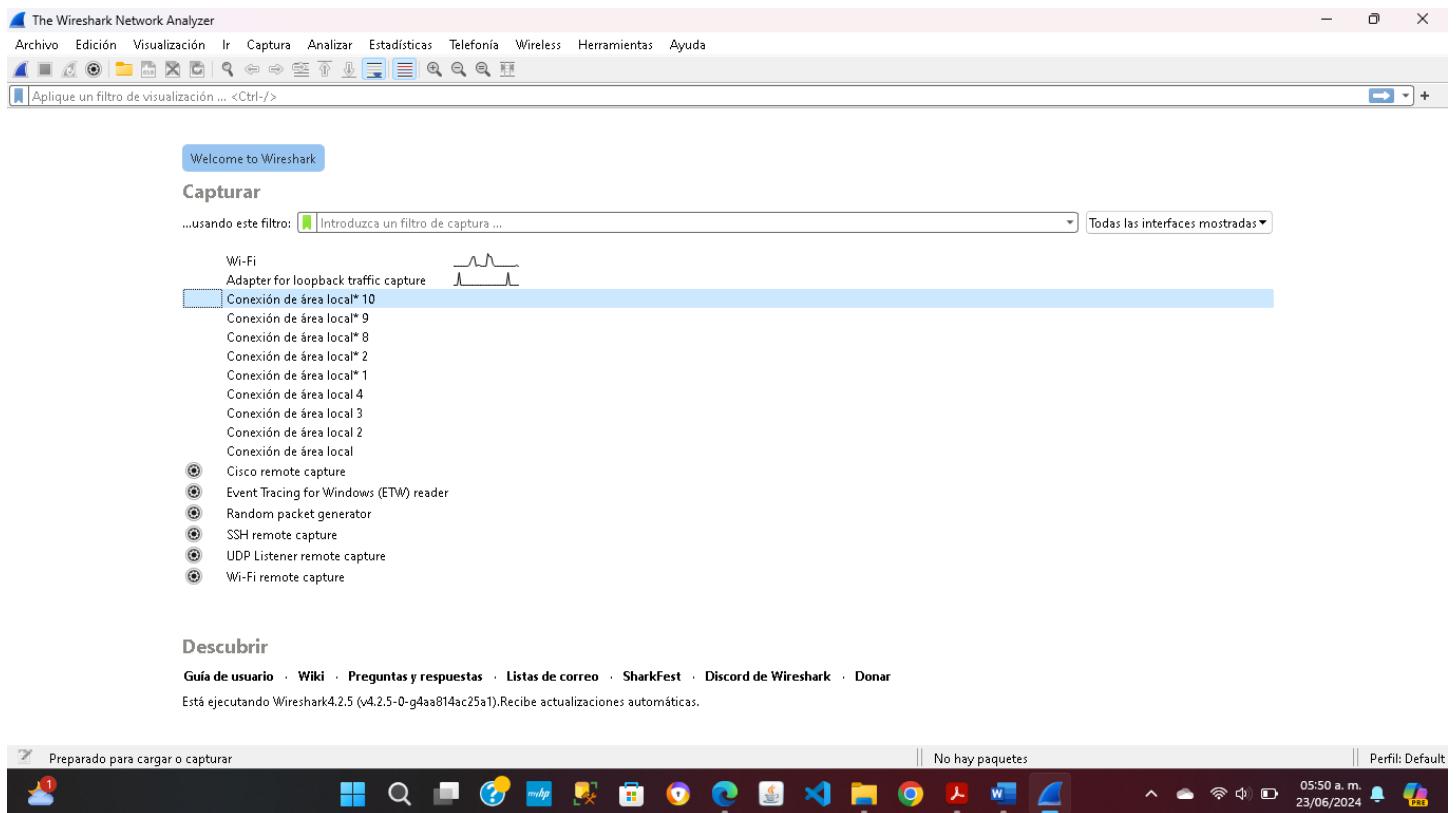
A continuación, podemos observar que esta por finalizar la instalación Wireshark.



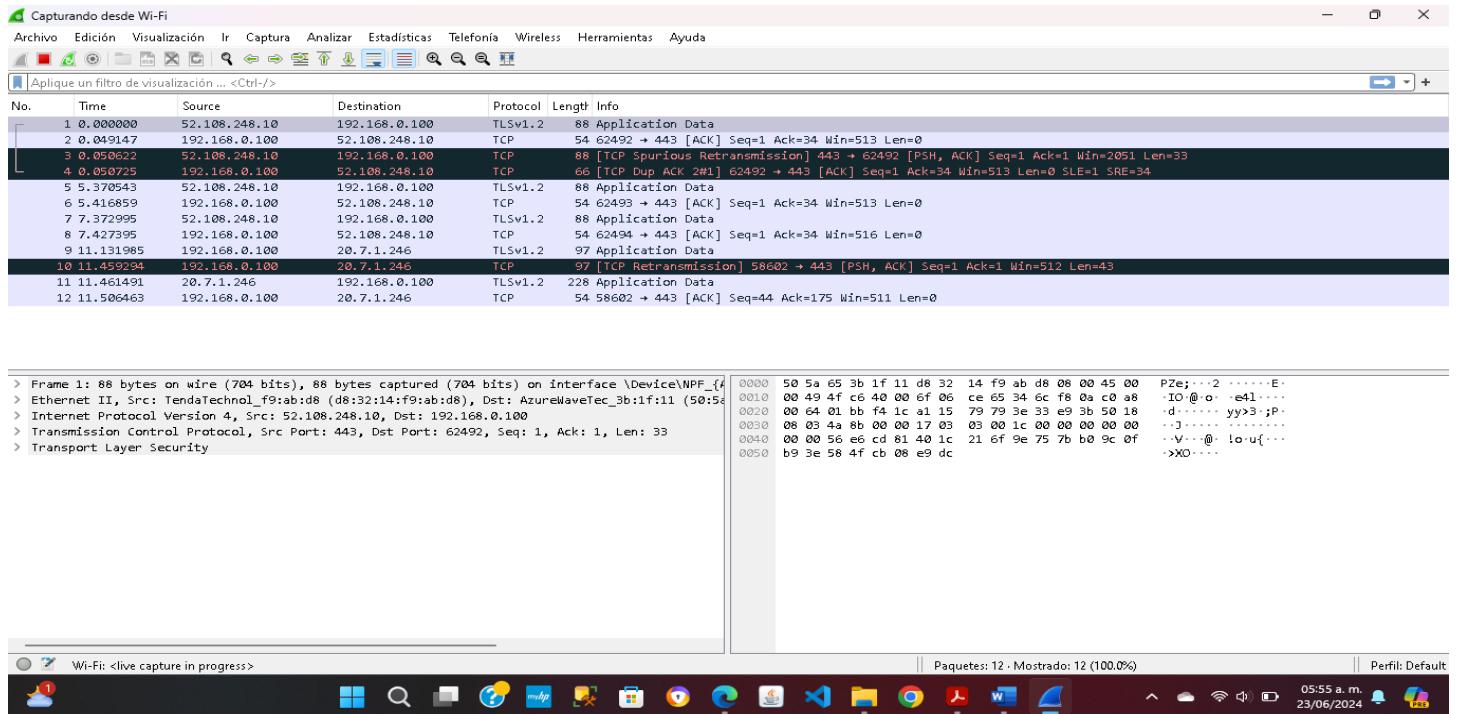
En la siguiente imagen se me muestra la pantalla de inicio de Wireshark una vez que esta la fue instalada y le damos iniciar como lo indica la actividad.



En la siguiente imagen se podemos observar que se abrir el programa *WireShark*.

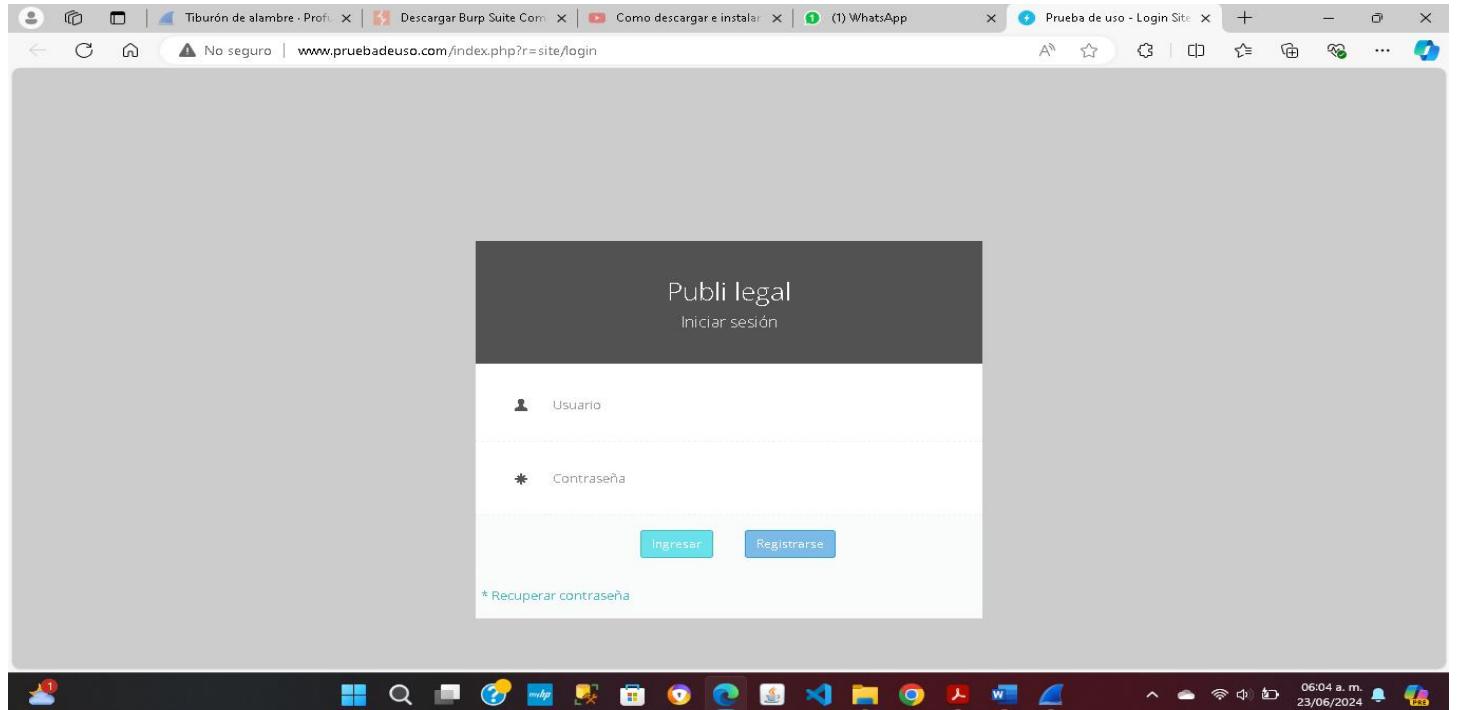


Una vez que ya logramos el ingreso a la opción *Wifi* nos permite visualizar la siguiente pantalla.

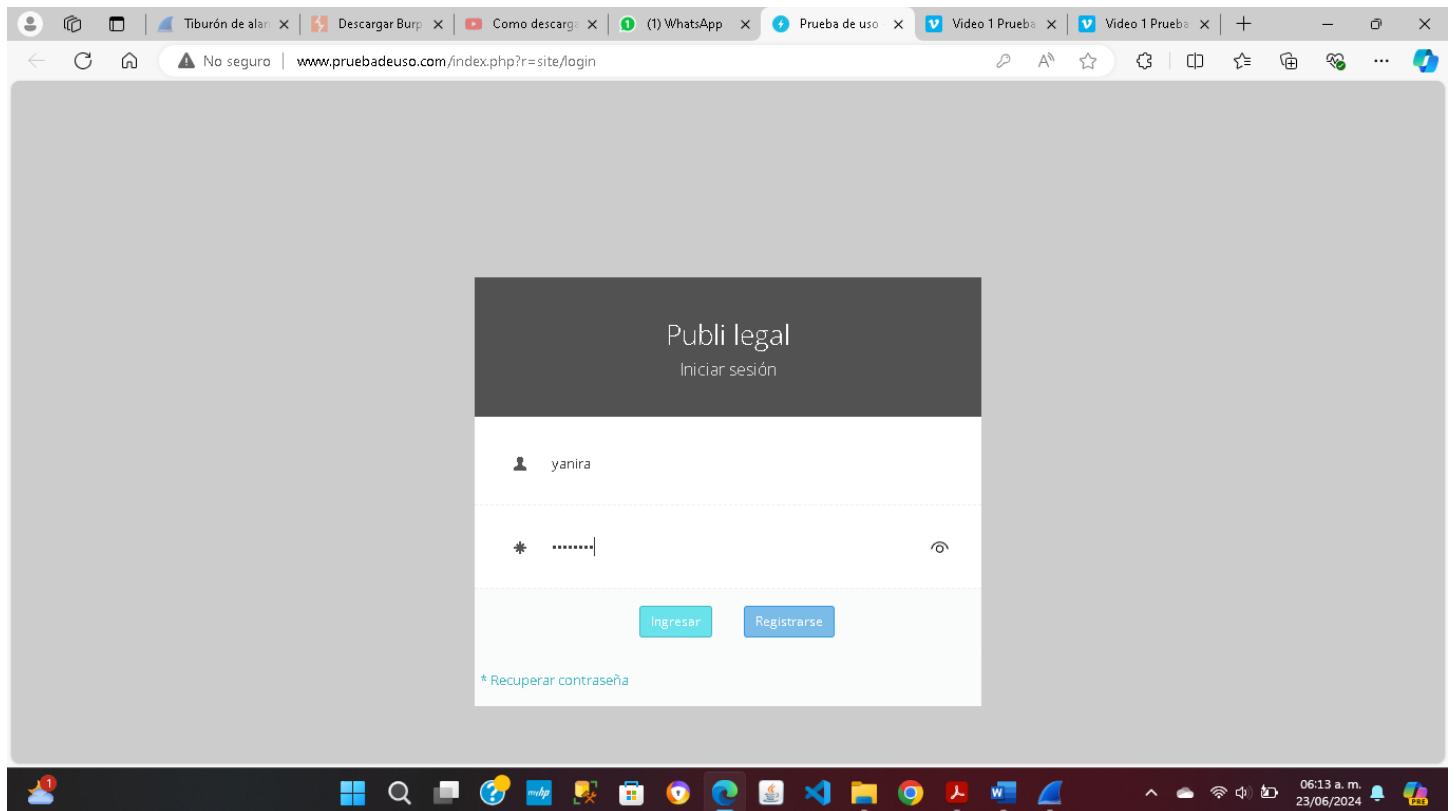


## Ataque al sitio

A continuación, ingresare al sitio web en el navegador de mi preferencia mediante el siguiente link <http://www.pruebadeuso.com/index.php?r=site/login>, en el cual llevare a cabo el ataca al sitio web.



A continuación, intentare iniciar sesión utilizando credenciales incorrectas (esto no permitirá iniciar sesión).



En la siguiente imagen podemos observar que se logró entrar a la configuración del servidor del sitio web, y buscar su dirección IP.

Aun cuando ya conocemos la ip del sitio web que vamos a atacar realice una confirmación de que la ip es correcto mediante el CMD de mi computadora.

```
C:\Users\yanir>ping pruebadeuso.com

Haciendo ping a pruebadeuso.com [107.180.119.56] con 32 bytes de datos:
Respueta desde 107.180.119.56: bytes=32 tiempo=54ms TTL=40
Respueta desde 107.180.119.56: bytes=32 tiempo=53ms TTL=40
Respueta desde 107.180.119.56: bytes=32 tiempo=54ms TTL=40
Respueta desde 107.180.119.56: bytes=32 tiempo=80ms TTL=40

Estadísticas de ping para 107.180.119.56:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
        (% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Minimo = 53ms, Máximo = 80ms, Media = 60ms

C:\Users\yanir>
```

Wi-Fi: <live capture in progress> | Paquetes: 591617 - Mostrado: 591617 (100.0%) | Perfil: Default

A continuación, se realizó la *búsqueda* de la dirección IP en *WireShark* mediante el siguiente comando:

ip. Add == dirección IP

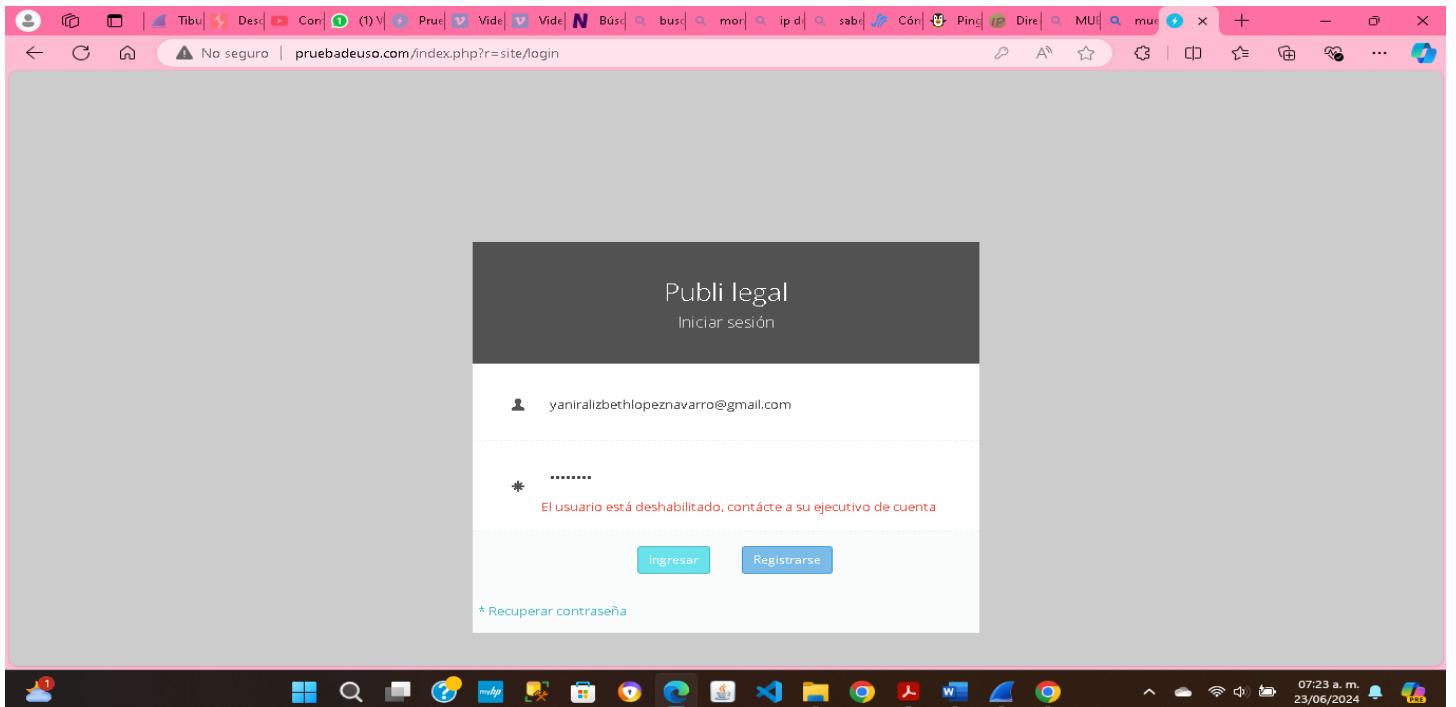
No.	Time	Source	Destination	Protocol	Length	Info
23907	475.075797	192.168.0.100	107.180.119.56	TCP	66	63585 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
23908	475.128889	107.180.119.56	192.168.0.100	TCP	68	80 → 63585 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1452 SACK_PERM WS=512
23909	475.129046	192.168.0.100	107.180.119.56	TCP	54	63585 → 80 [ACK] Seq=1 Ack=1 Win=132096 Len=0
23910	475.183311	192.168.0.100	107.180.119.56	TCP	66	63586 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
23917	475.235810	192.168.0.100	107.180.119.56	TCP	66	63587 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
23924	475.338132	107.180.119.56	192.168.0.100	TCP	68	443 → 63587 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1452 SACK_PERM WS=512
23925	475.338397	192.168.0.100	107.180.119.56	TCP	54	63587 → 443 [ACK] Seq=1 Ack=1 Win=132096 Len=0
23926	475.339560	192.168.0.100	107.180.119.56	TCP	1506	63587 → 443 [ACK] Seq=1 Ack=1 Win=132096 Len=1452 [TCP segment of a reassembled PDU]
23927	475.339560	192.168.0.100	107.180.119.56	TLSv1.2	331	Client Hello (SNI=www.pruebadeuso.com)
23934	475.438147	107.180.119.56	192.168.0.100	TCP	56	443 → 63587 [ACK] Seq=1 Ack=1730 Win=32768 Len=0
23935	475.445476	107.180.119.56	192.168.0.100	TLSv1.2	1311	Server Hello, Certificate, Server Key Exchange, Server Hello Done
23940	475.454910	192.168.0.100	107.180.119.56	TLSv1.2	61	Alert (Level: Fatal, Description: Certificate Unknown)
23941	475.454996	192.168.0.100	107.180.119.56	TCP	54	63587 → 443 [FIN, ACK] Seq=1737 Ack=1258 Win=130816 Len=0
23944	475.459417	192.168.0.100	107.180.119.56	HTTP	581	GET /index.php?=site/login HTTP/1.1
23960	475.628303	107.180.119.56	192.168.0.100	TCP	56	80 → 63585 [ACK] Seq=1 Ack=528 Win=30720 Len=0
23961	475.628303	107.180.119.56	192.168.0.100	TCP	56	443 → 63587 [FIN, ACK] Seq=1258 Ack=1738 Win=32768 Len=0

> Frame 23907: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface *\Device\NPF\_{...}*
> Ethernet II, Src: AzureWaveTec\_3b:1f:11 (50:5a:65:3b:1f:11), Dst: TendaTechnol\_f9:ab:d8 (d8:32:...)
> Internet Protocol Version 4, Src: 192.168.0.100, Dst: 107.180.119.56
> Transmission Control Protocol, Src Port: 63585, Dst Port: 80, Seq: 0, Len: 0

0000 d8 32 14 f9 ab d8 50 5a 65 3b 1f 11 08 00 45 00 .2...PZ e;... E-
0010 00 34 22 71 40 00 80 06 34 5a c0 a8 00 64 6b b4 .4\*q@... 4Z...dk-
0020 77 38 f8 61 00 50 48 a4 0a 1c 00 00 00 00 80 02 w8-a-PH- .....
0030 fa f0 84 b4 00 00 02 04 05 b4 01 03 03 08 01 01 ...
0040 04 02 .....

Wi-Fi: wireshark\_Wi-Fi3Q9IP2.pcapng | Paquetes: 612819 - Mostrado: 2540 (0.4%) | Perfil: Default

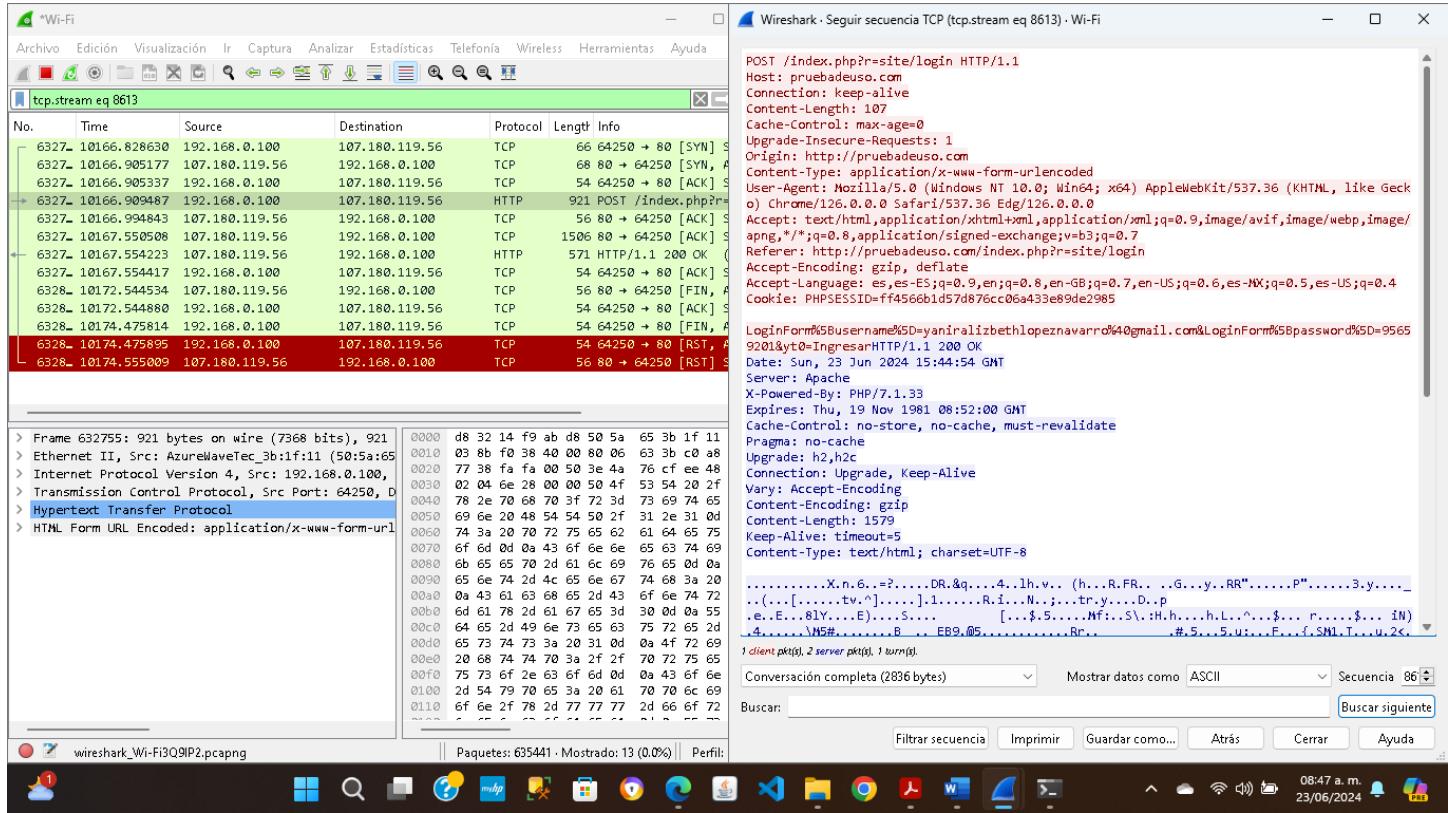
Intentamos volver al sitio web e ingresar los datos de manera correcta, aunque no nos permite debido a que el sitio web no es de mi propiedad y no cuento con las credenciales correctas.



A continuación, se muestra en *Wireshark* se puede ver las acciones que ha realizado la dirección IP del sitio web. Buscar mediante una opción que en protocolo tenga HTTP, así como la palabra POST.

A screenshot of the Wireshark network traffic analyzer. The search bar at the top contains the filter 'ip.addr==107.180.119.56 and http'. The main pane displays several TCP sessions. One session, highlighted in green, shows a POST request from '192.168.0.100' to '107.180.119.56' on port 80. The request payload is 'HTTP/1.1 (application/x-www-form-urlencoded)'. Other sessions show responses and other traffic. The bottom pane shows the raw hex and ASCII dump of the selected packet, which is the POST request. The status bar at the bottom indicates 'Hypertext Transfer Protocol: Protocol' and 'Paquetes: 638514 - Mostrado: 13 (0.0%)'.

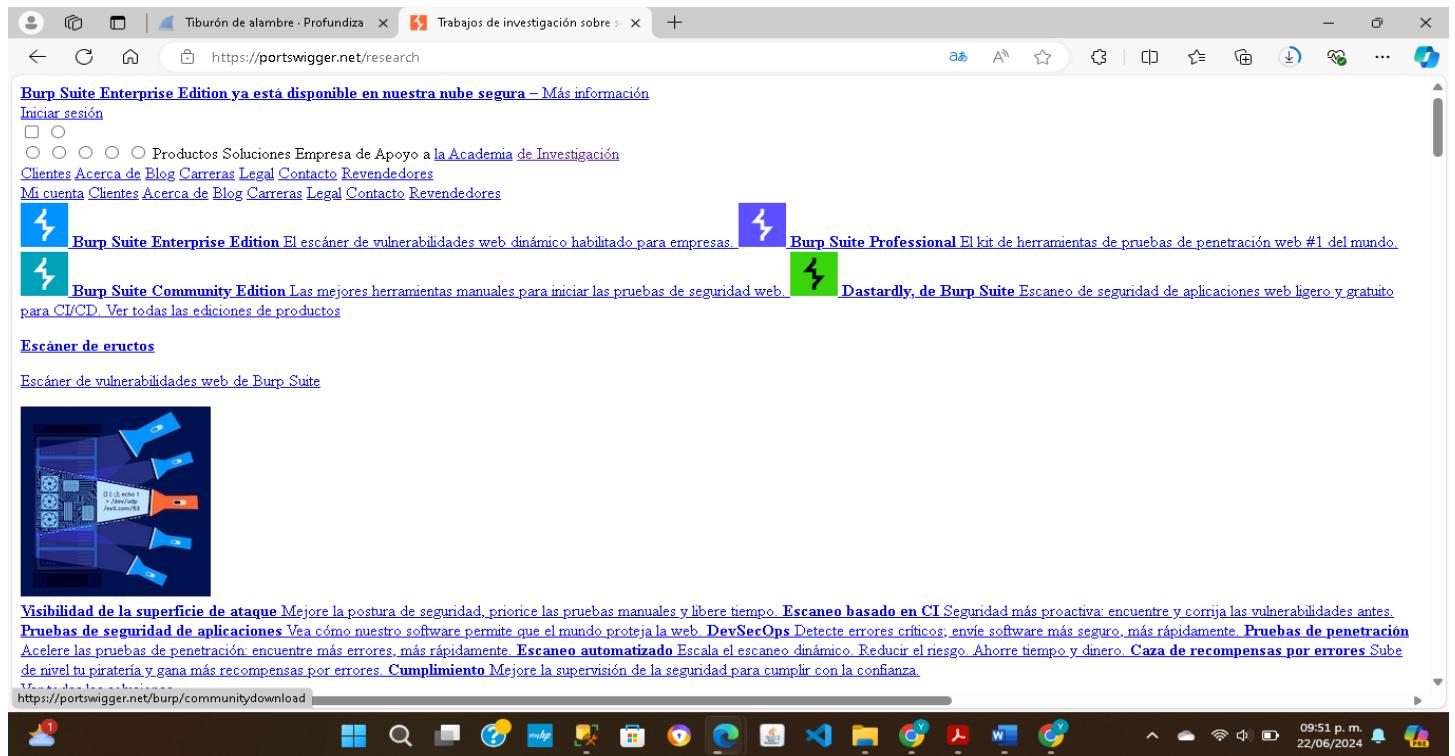
A continuación, se muestra el resultado una vez que se dio clic derecho sobre la opción con las características anteriores y seleccionar *Seguir*.



Con esto nos permite visualizar el usuario/correo y contraseña con el que se intentó el inicio de sesión en el sitio web.

## Etapa 2: Ataque al sitio

En la siguiente imagen nos muestra la página que nos permitirá descargar la herramienta sugerida en la actividad.

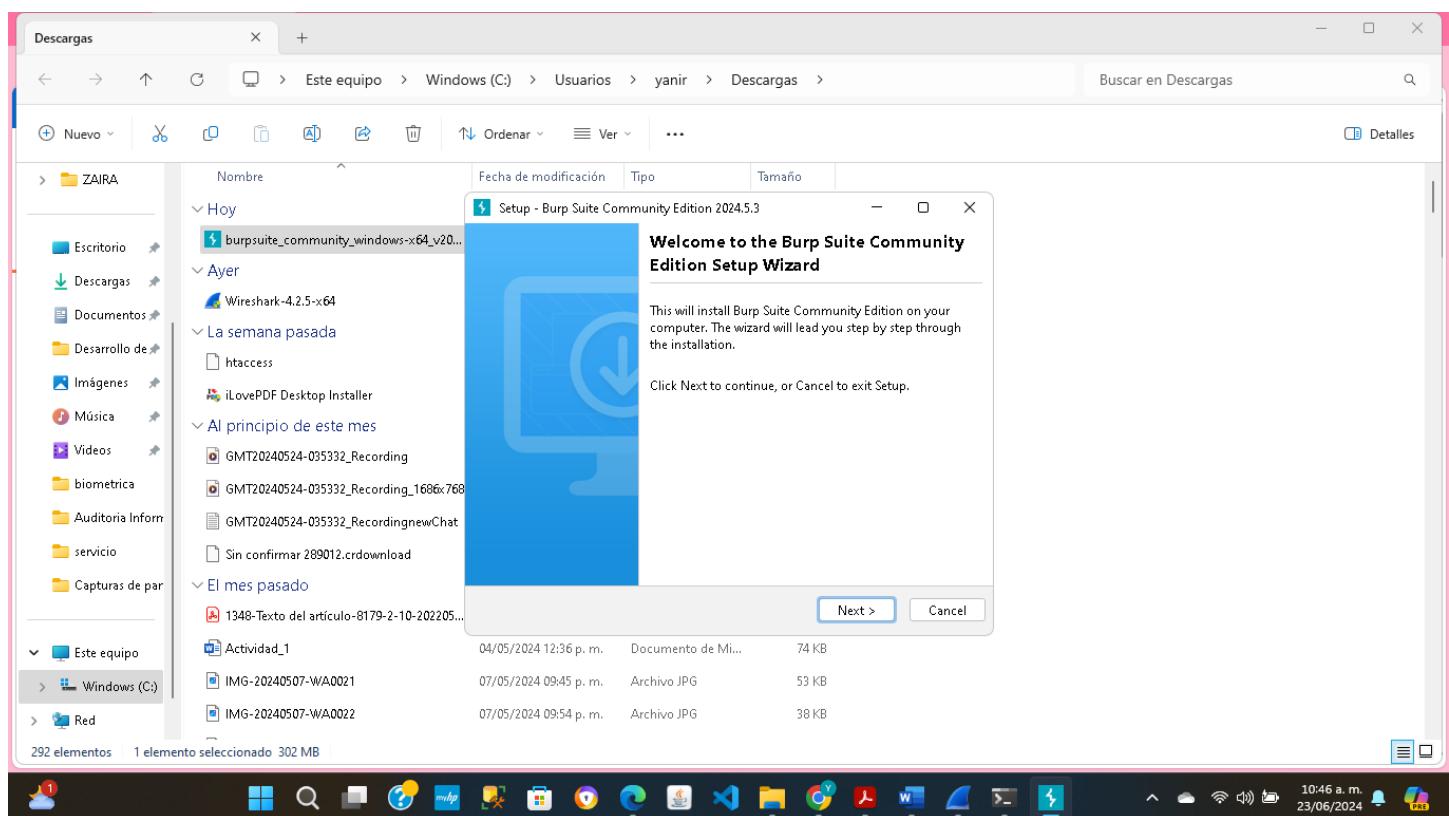


A continuación, procedemos con la selección Edición comunitaria de Burp Suite.

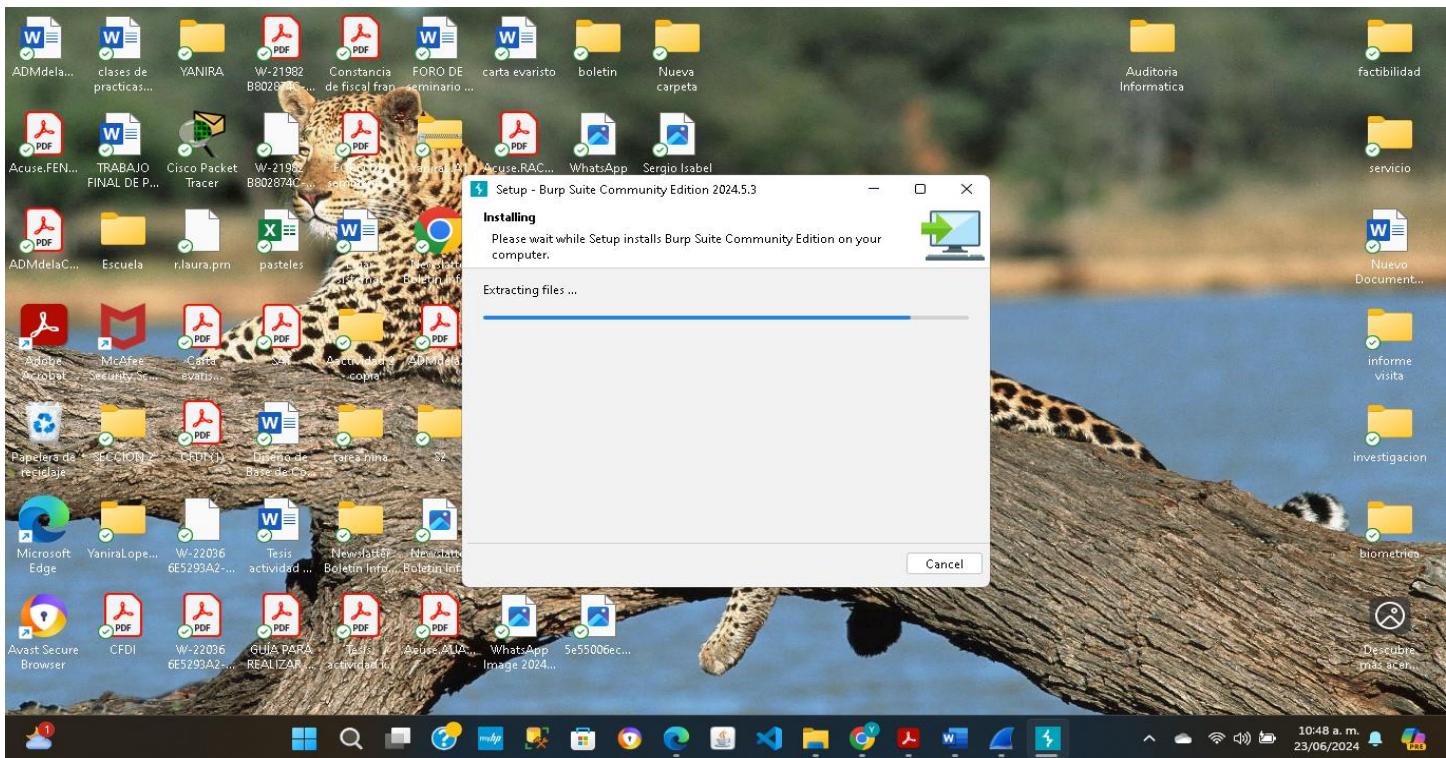
A continuación, seleccionamos la versión que sea compatible con mi equipo de cómputo.

The screenshot shows a browser window with multiple tabs open. The active tab is for the PortSwigger website, specifically the 'Profesional / Comunidad' section. The page displays a message about the availability of Burp Suite Enterprise Edition. It features a large 'PortSwigger' logo, a navigation bar with links like 'INICIAR SESIÓN', 'Productos', 'Soluciones', 'Investigación', 'Academia', 'Apoyo', and a menu icon. Below the navigation, it says 'Profesional / Comunidad 2024.5.3'. A dropdown menu shows 'Edición comunitaria de Burp Suite' and 'Ventanas (x64)'. A prominent orange 'DESCARGAR' button is visible, along with a link to 'Mostrar sumas de comprobación'. A note below the download button states: 'Esta versión presenta compatibilidad con Burp Scanner para WebSockets, mejoras para el editor de inicio de sesión grabado, reglas de coincidencia y reemplazo de WebSocket y una serie de mejoras de rendimiento. También hemos eliminado algunas comprobaciones de análisis redundantes.'

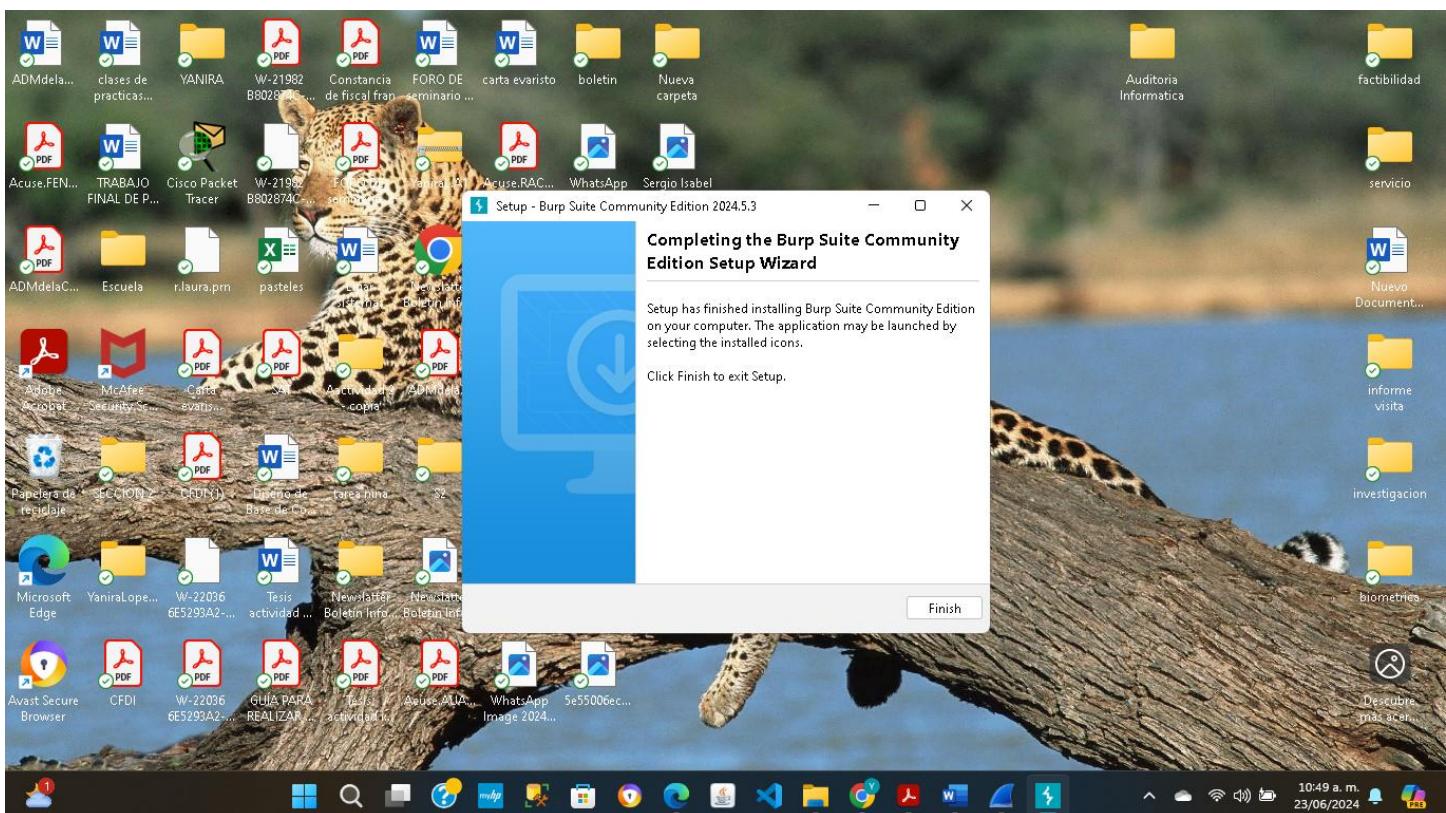
En la siguiente imagen nos indica que podemos iniciar con la instalación de Burp Suite Community Edition.



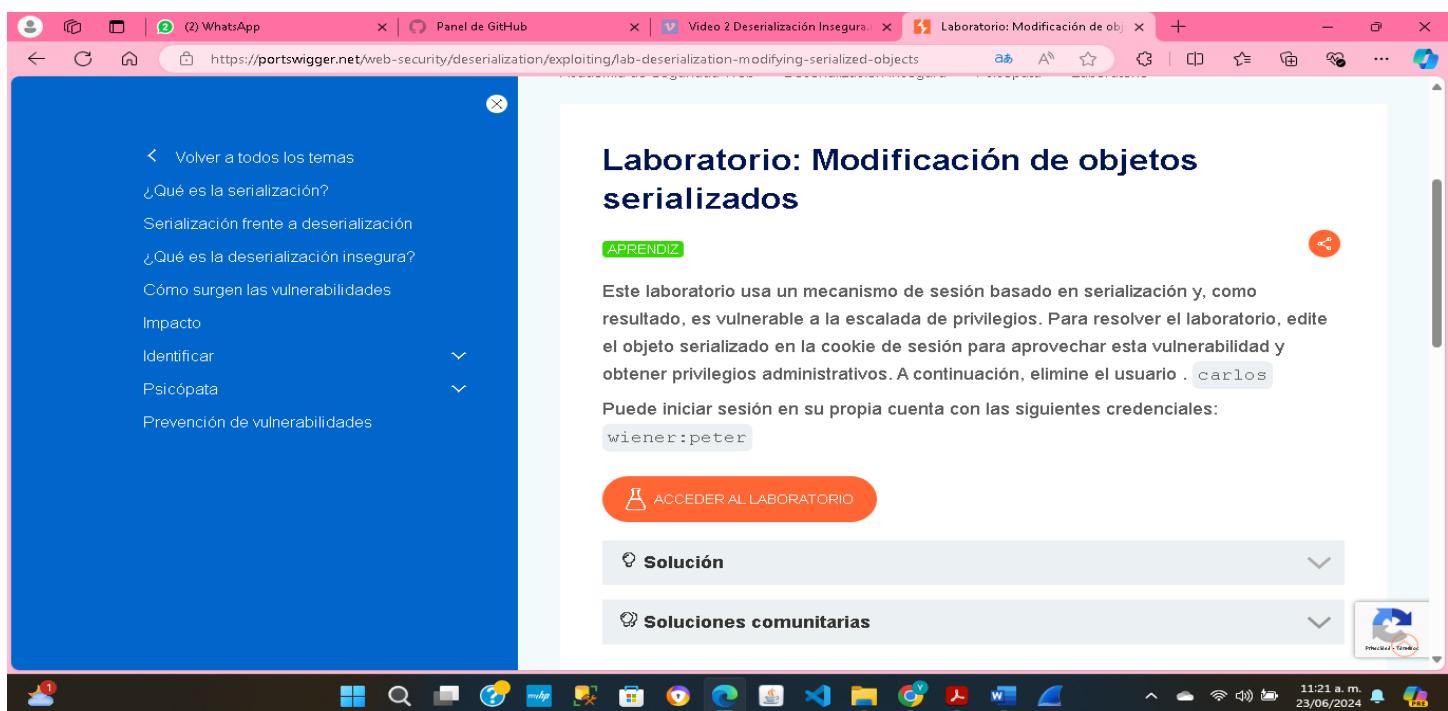
A continuación, la siguiente imagen nos muestra el avance de instalación de Burp Suite Community Edition.



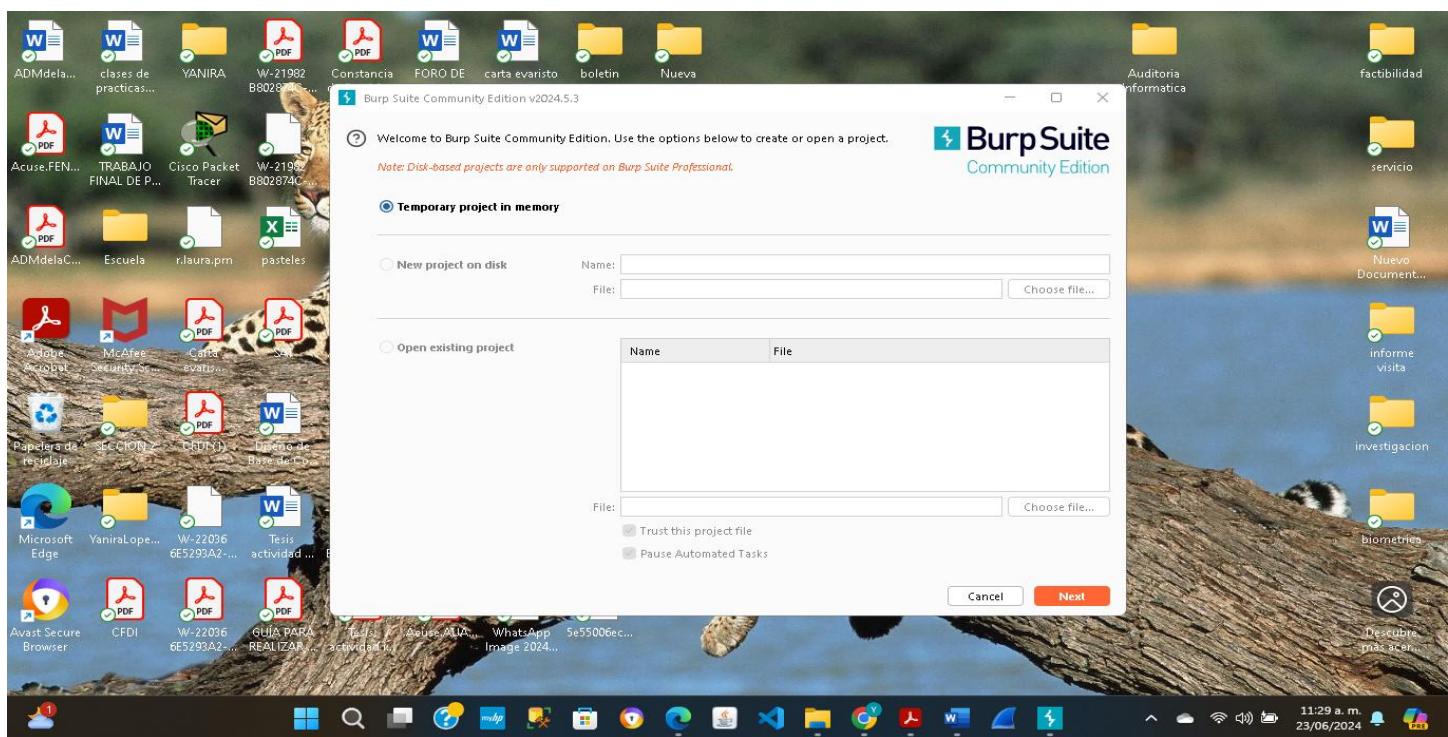
En la siguiente imagen podemos observar que se llevó a cabo la instalación de Burp Suite Community Edition de manera exitosa. Este es el software a utilizar para realizar la práctica del laboratorio.



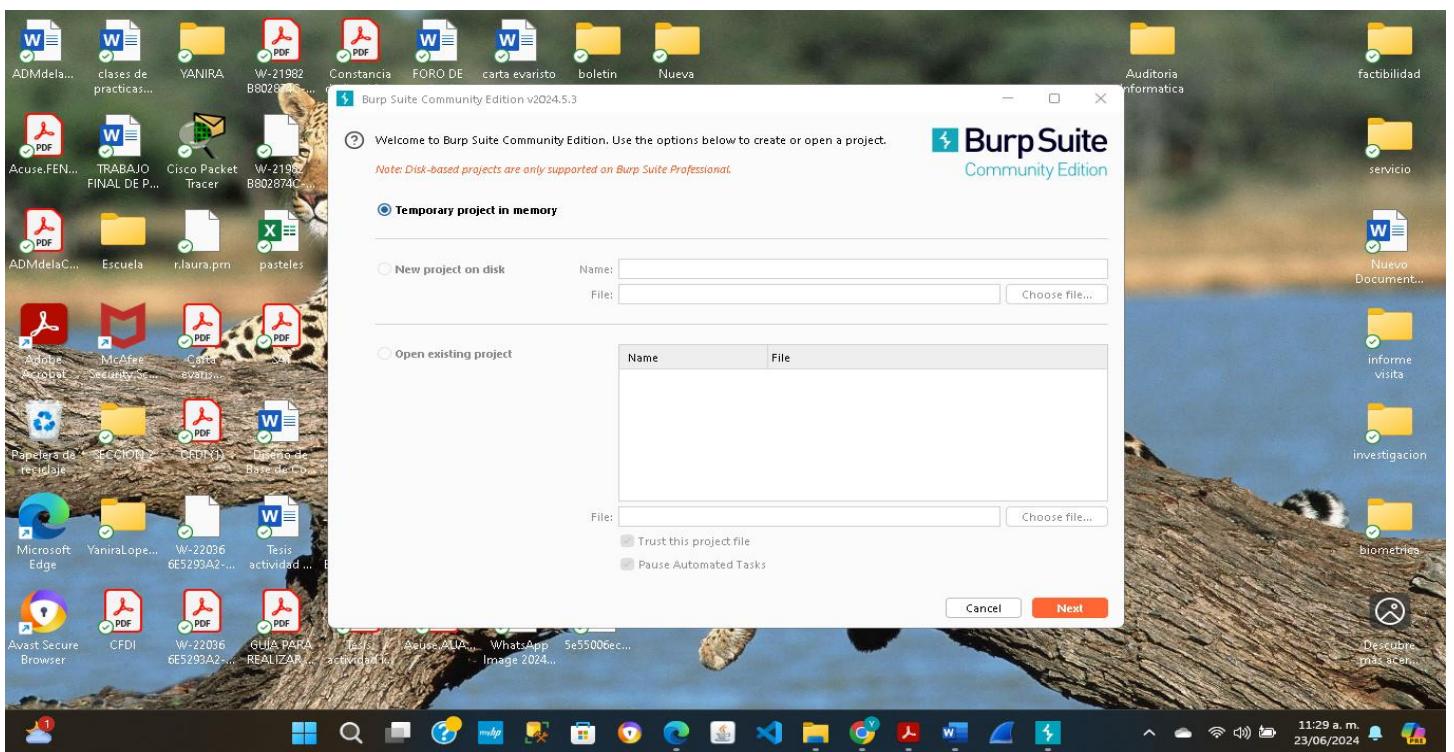
Una vez instalado el programa, procedemos a entrar al enlace del laboratorio de práctica que nos fue proporcionado en la sección Recursos del material brindado.



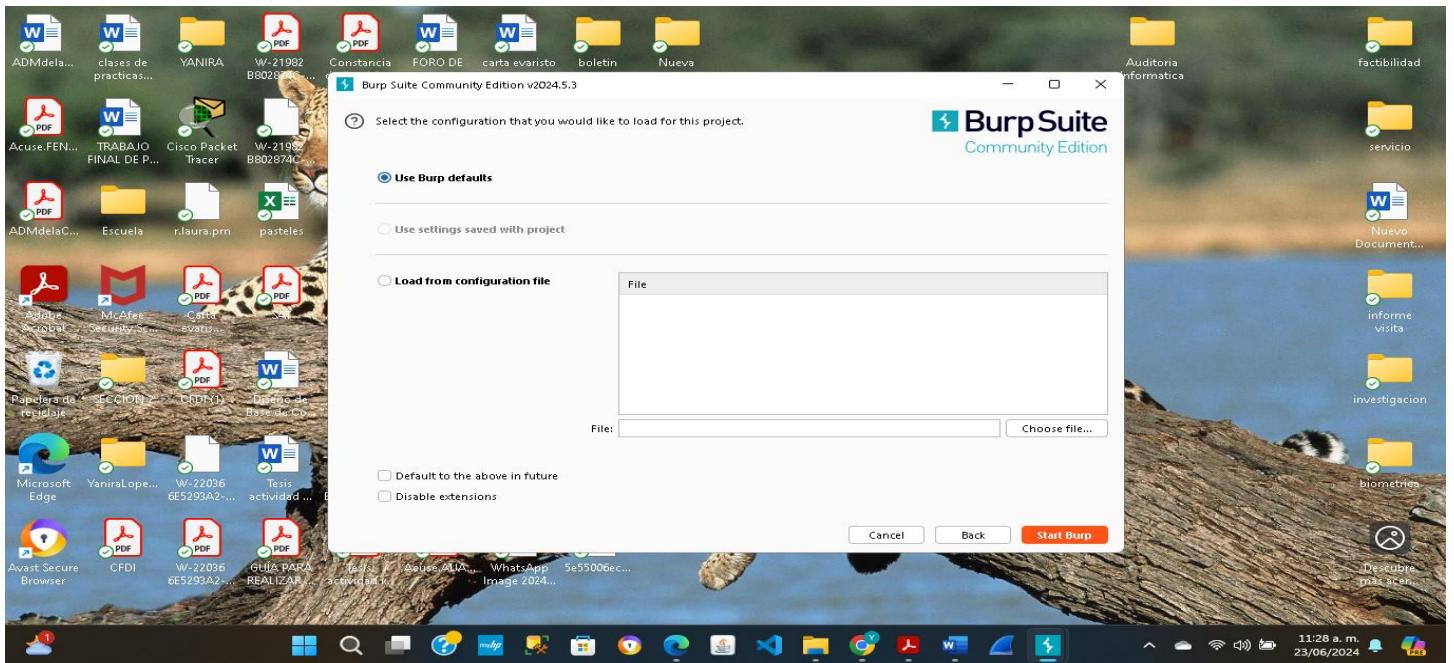
A continuación, nos muestra la siguiente imagen al abrir Burp Suite de acuerdo a lo que indica la actividad.



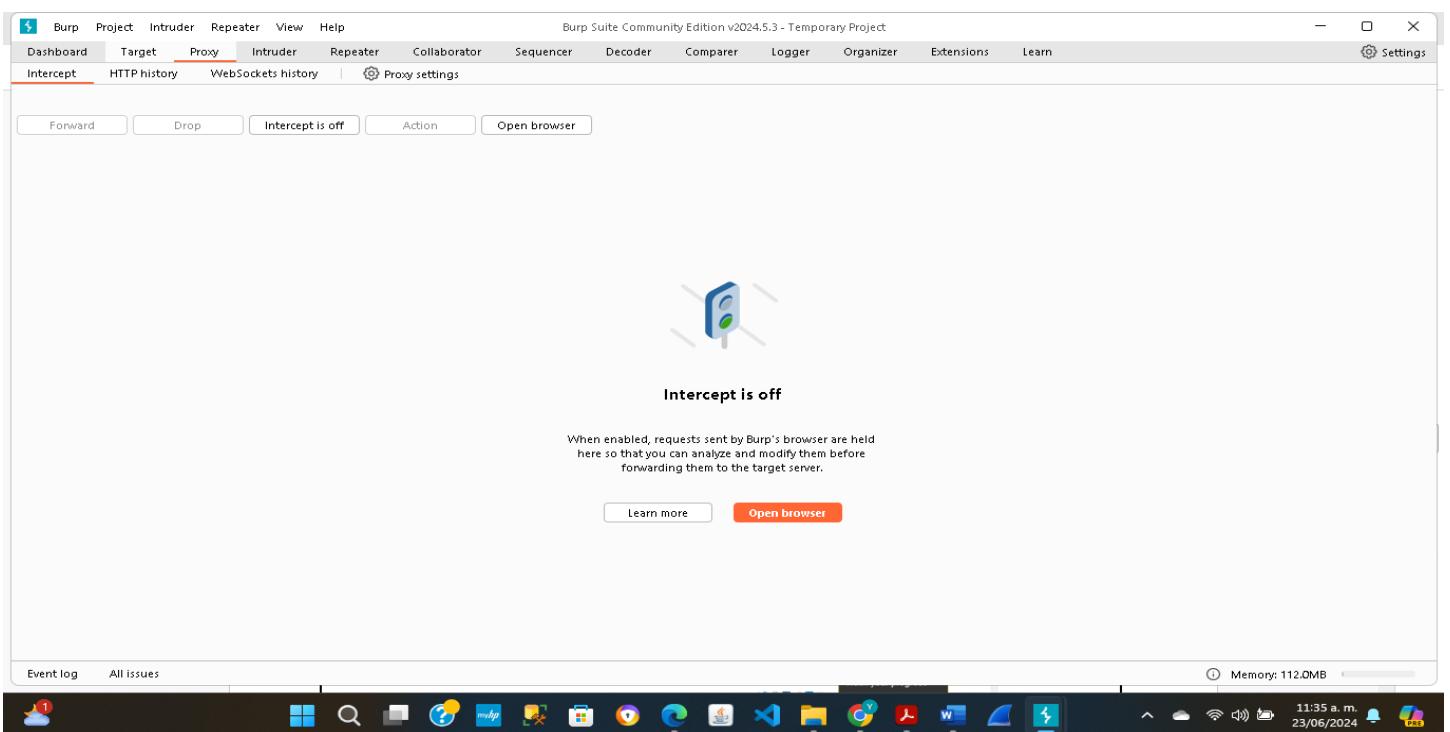
En la siguiente pantalla, nos muestra la seleccionar el tipo de proyecto a realizar. En esta ocasión, dejare el que viene por default: Temporary Project.



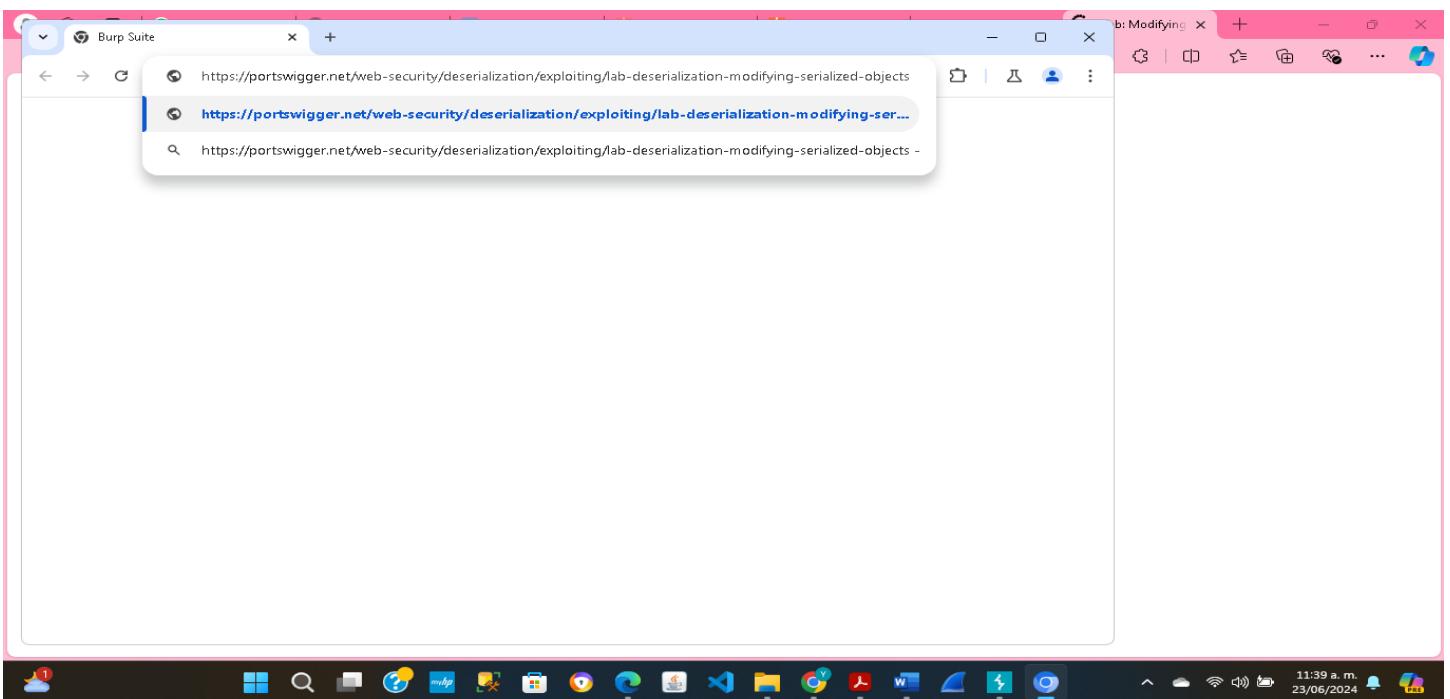
Después, dar clic en *Next*. Luego, pedirá realizar la configuración del proyecto. Por ello, dejar la opción que viene por defecto, y dar clic en *Start Burp*.



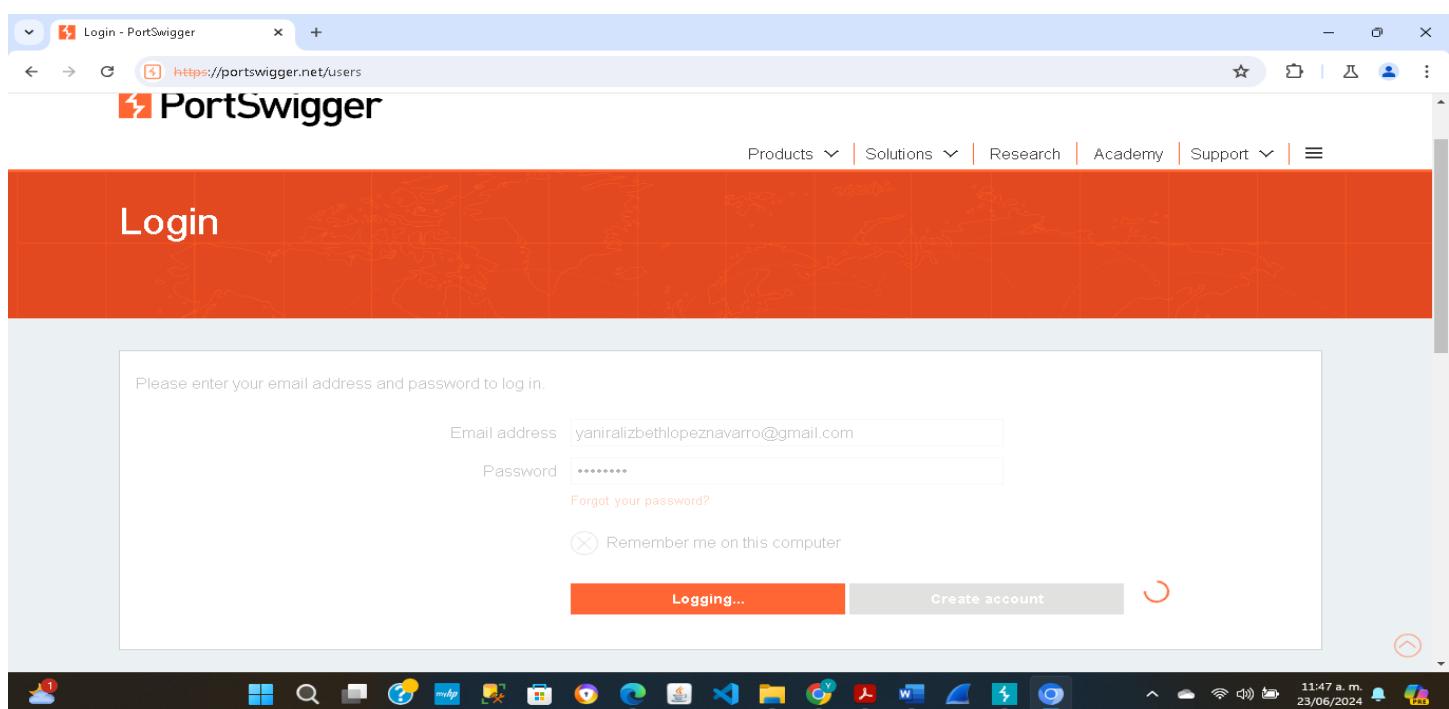
En la siguiente pantalla está la interfaz del programa en la cual, para realizar la práctica, entraremos a la interfaz *Proxy*, como se puede ver en la siguiente imagen.



Para iniciar con la práctica, daremos clic en Open Browser, lo cual abrirá un navegador que está vinculado con el programa. Una vez que se haya abierto el navegador, copiaremos el enlace de la página del laboratorio (este se encuentra en la sección Recursos del presente documento).



Una vez dentro de la página del laboratorio se verá la siguiente pantalla: Para poder realizar la práctica en el laboratorio, es importante generar una nueva cuenta en PortSwigger.



A continuación, podemos observar que, una vez creada la cuenta e iniciado sesión, entrar al laboratorio de práctica.

Welcome to the Web Security Academy | Iniciar sesión - PortSwigger | Iniciar sesión - PortSwigger | Modificar objetos serializados | +

0a51006e0441119b83b373c800630015.web-security-academy.net

Gmail YouTube Maps p6-minería-y-análisis... | Todos los marcadores

Web Security Academy Modificar objetos serializados Volver a la descripción del laboratorio » LABORATORIO No resuelto

WE LIKE TO SHOP

Hogar | Mi cuenta

02:09 p.m. 23/06/2024

A continuación, en la siguiente imagen ingresaremos las credenciales proporcionadas en el material de la actividad.

The screenshot shows a web browser window with several tabs open. The active tab is titled "Modificar objetos serializados". The main content area displays a login form for "Web Security Academy". The form includes fields for "Nombre de usuario" and "Contraseña", and a green "Acceso" button. Above the form, there's a banner with the "LABORATORIO" badge and the status "No resuelto". The browser interface includes a toolbar at the top and a taskbar at the bottom with various application icons.

La siguiente imagen nos muestra que ingresamos al Burp y al dar clic en el botón Intercept is off. Con esto, se encenderá el interceptador para captar todas las salidas de la página como se muestran a continuación.

The screenshot shows the Burp Suite Community Edition interface. The "Proxy" tab is selected, showing a list of captured network requests. The "Intercept" sub-tab is highlighted. The list includes requests such as "https://www.google.com", "https://www.youtube.com", and "https://www.gstatic.com". The interface includes a toolbar at the top and a taskbar at the bottom with various application icons.

En la siguiente imagen nos arroja el siguiente resultado siguiendo las indicaciones las cuales nos permiten identificar las cookies.

GET request to https://portswigger.net/research

**Request**

Pretty Raw Hex

```

1 GET /research HTTP/2
2 Host: portswigger.net
3 Cookie: AWSALBAPP-0=_remove_; AWSALBAPP-1=_remove_; AWSALBAPP-2=_remove_; stg_traffic_source_priority=1;
4 _pk_ses_267552c2-4917-4e00-888c-ba994aca73d7.1467a*; ts=HQUKUECLfmnlE54J10A13D+3D; SessionId=CEDfGKUD4Qxj5SNUvqUplhLhrisnqiq+RWA5tEBN1vHIt4vCjEKFNP8w4cSMl4ncI2nZPFW5j0w0BaB7rpSidID2uon0WrstgaNFUrzmb7vogitCFGy83NMd91axq27csNBuvW5KSxFcElv14qMqgt2746a6L6sScqVscqj1f9XSG1ExMNs; _pk_id_207552c2-4917-4e0-8982-ba994aca73d7.1467*a7854a59daaa7c607.1719168038.1.1719176684.1719168038; stg_last_interaction=Sun%2C%2023%20Jun%202024%2021:04:55%20GMT; stg_returning_visitor=Sun%2C%2023%20Jun%202024%2021:04:55%20GMT
5 Sec-Ch-UA: "Not/A/Brand";v="8", "Chromium";v="126"
6 Sec-Ch-UA-Mobile: 20
7 Sec-Ch-UA-Platform: "Windows"
8 Accept-Language: es-419
9 Upgrade-Insecure-Requests: 1
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.57 Safari/537.36
11 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
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: navigate
14 Sec-Fetch-User: ?1
15 Sec-Fetch-Dest: document
16 Referer: https://portswigger.net/web-security/deserialization/exploiting/lab-deserialization-modifying-serialized-objects
17 Accept-Encoding: gzip, deflate, br
18 Priority: u=0, i
19

```

0 highlights

ESP ES 02:24 p.m. 23/06/2024

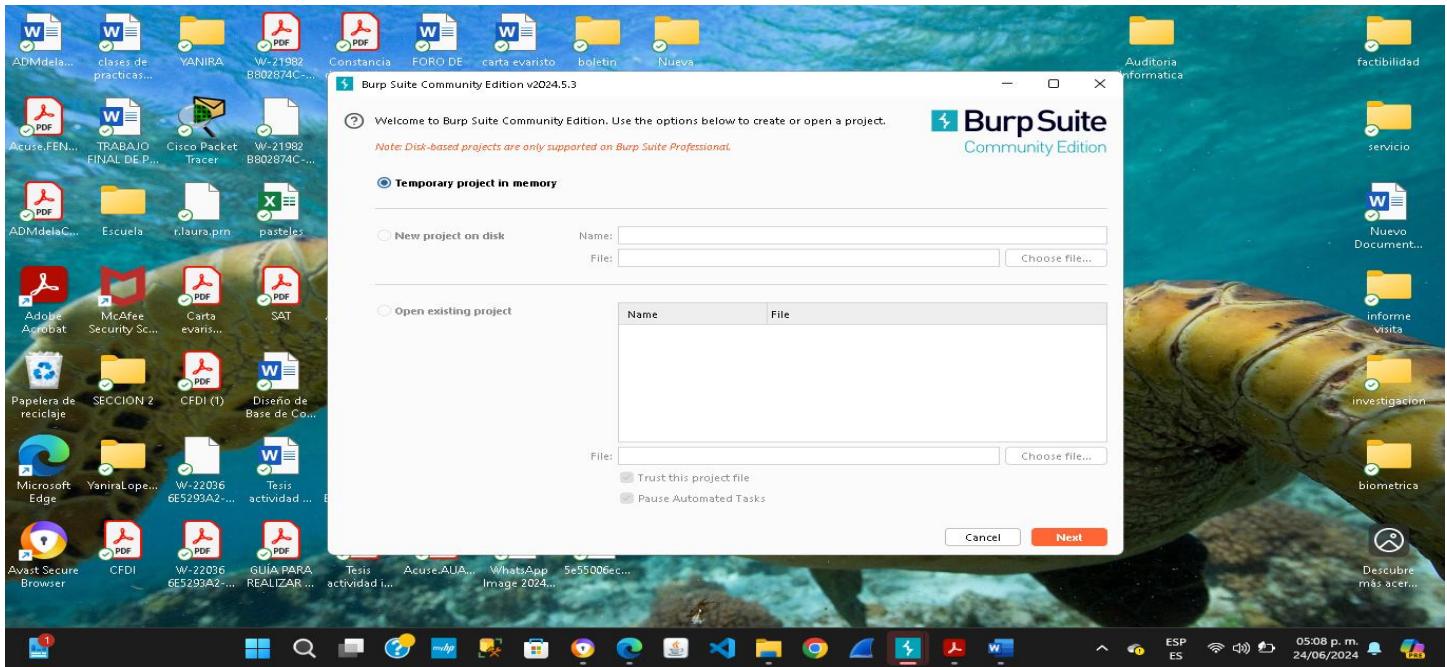
A continuación, en la siguiente imagen nos muestra la donde se está convirtiendo las cookies en URL.

Event log All issues 02:34 p.m. 23/06/2024

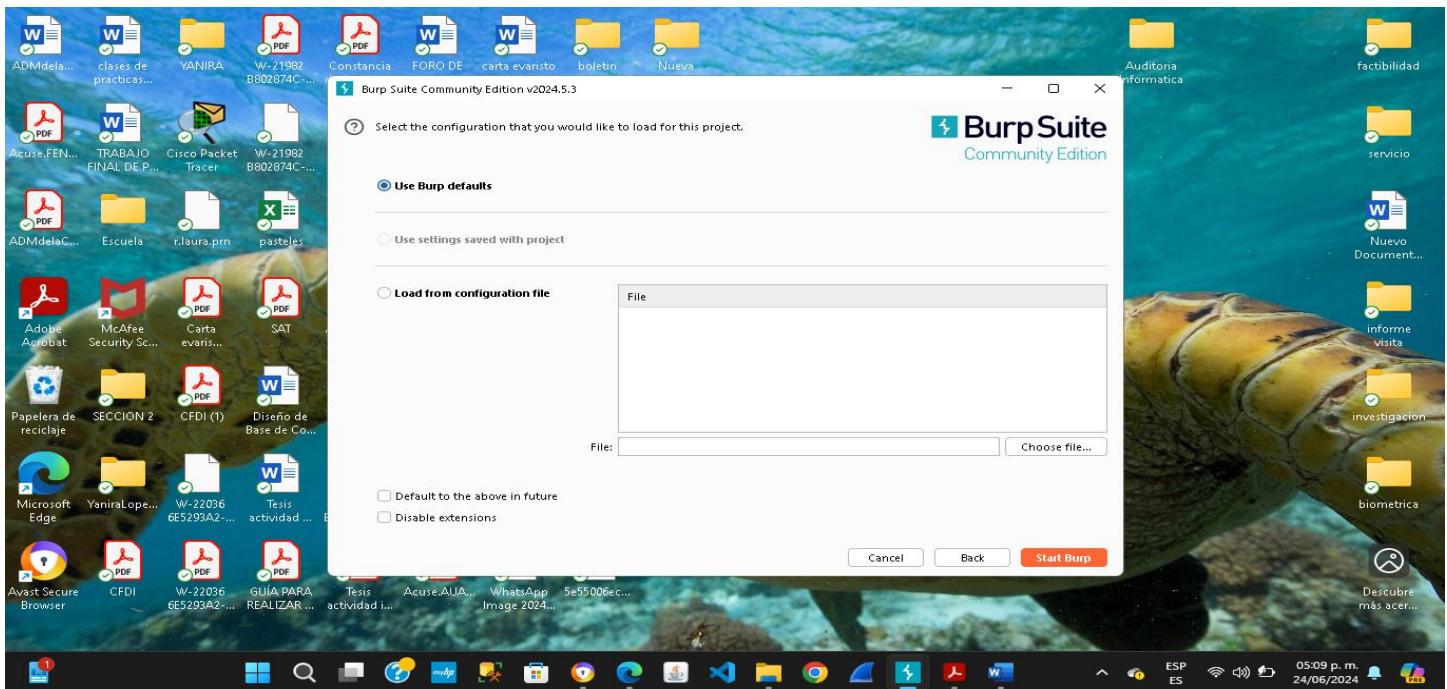
Debido a problemas con la conexión con el sitio web perdí lo realizado en la actividad y no me permitió seguir avanzando para poder cumplir con lo solicitado en la actividad por lo que me quedo pendiente algunos puntos

## Etapa 3: Ataque al sitio

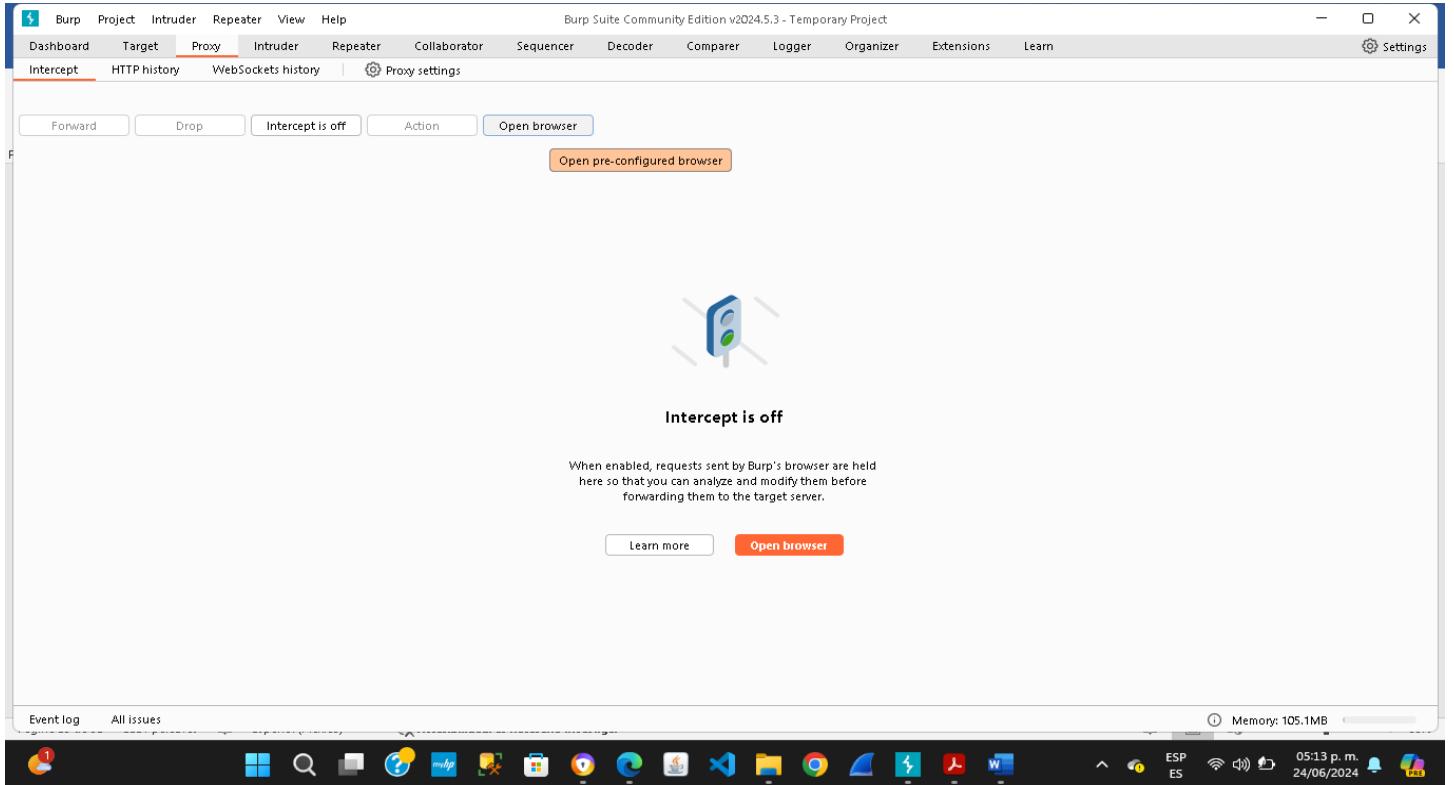
A continuación, en la siguiente imagen podemos observar que se abrió el programa *Burp Suite* y se creó un nuevo proyecto.



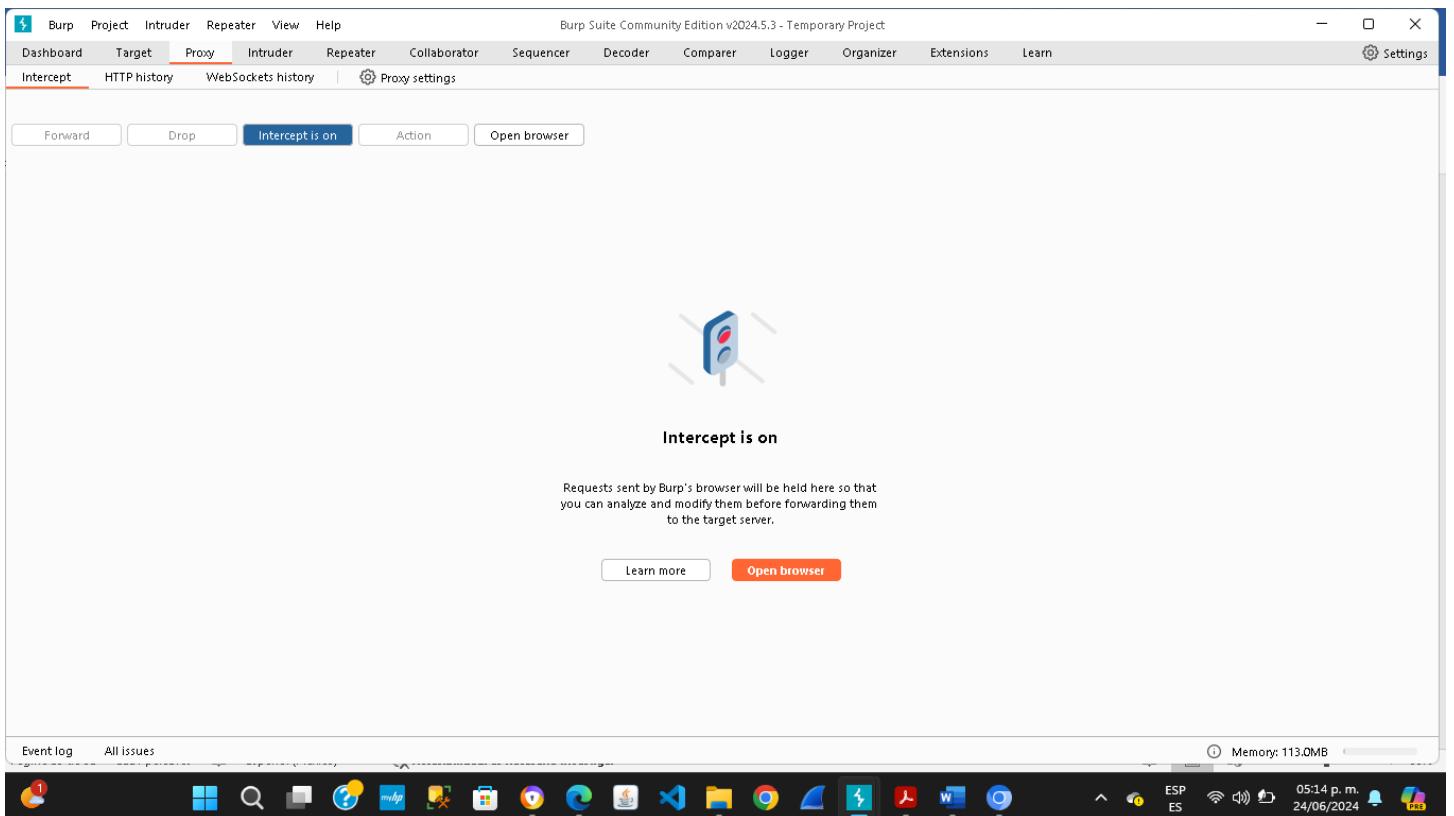
En la siguiente imagen nos muestra que dejamos por default las configuraciones que arroja la herramienta.



Una vez generado, pasamos a la sección Proxy y abrimos el navegador.

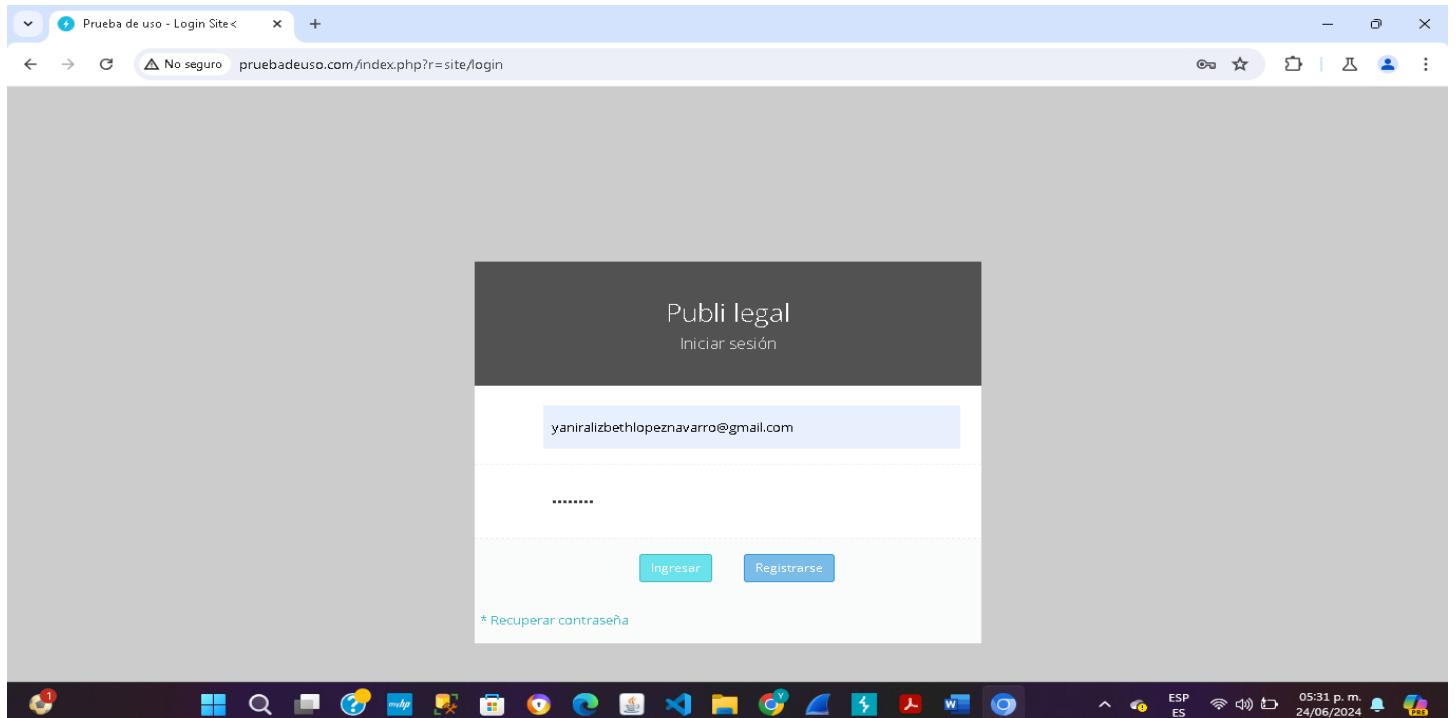


A continuación, nos muestra que encendimos el interceptor de datos.

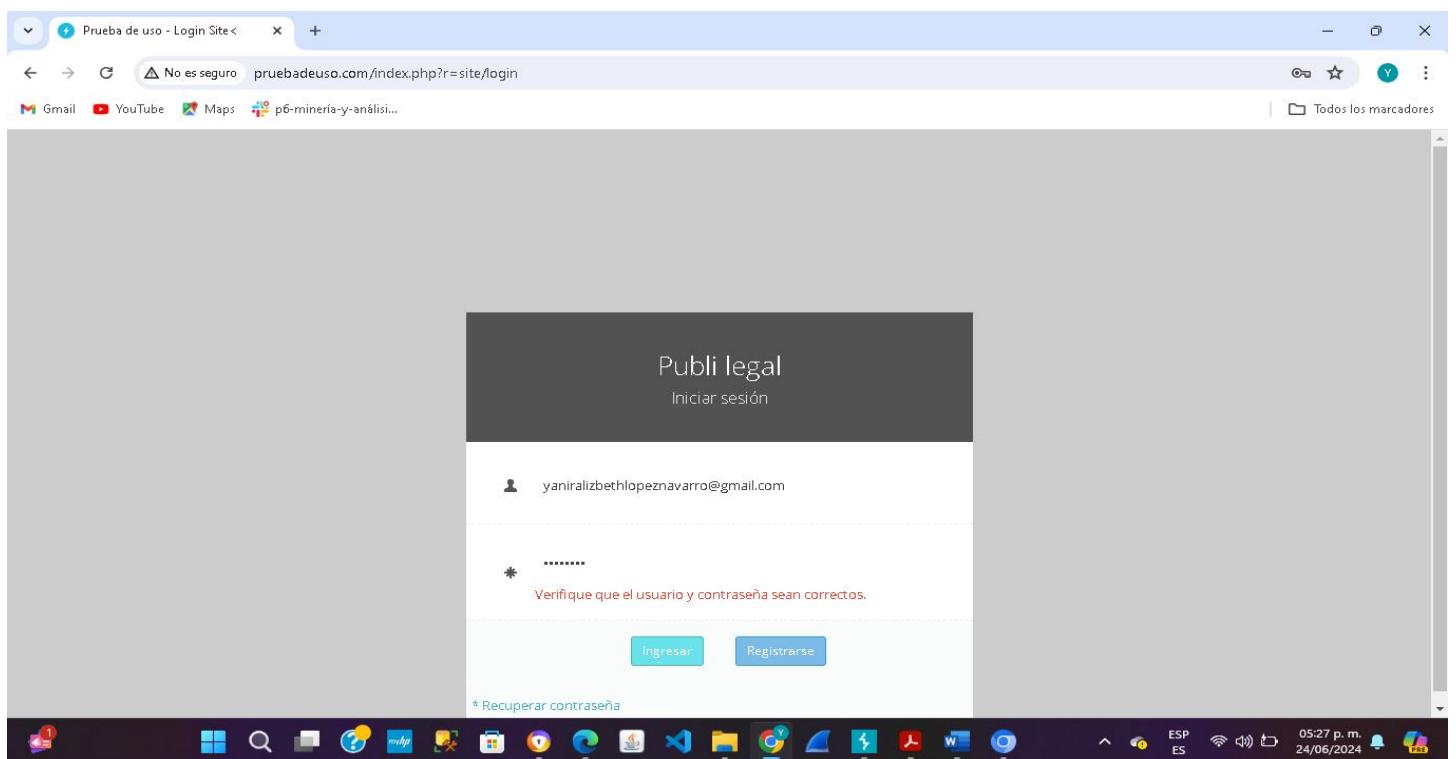


En seguida podemos observar que se utilizó el navegador que utiliza Burp Suite y se intentó entrar al sitio web del proyecto que se subió en la Actividad 1.

<http://www.pruebadeuso.com/index.php?r=site/login>



A continuación, nos muestra el siguiente mensaje debido a que no ingresamos con las credenciales correctas.



En la siguiente imagen podemos observar que una vez que intenté entrar al sitio web, en la página de login, en el programa de Burp Suite, se encendió el interceptor y di clic en Forward, nos muestra los datos captados que con los que se intentó iniciar sesión.

En la siguiente imagen nos muestra los datos captados.

A continuación, la siguiente imagen nos muestra las alteraciones que se llevaron acabo en el correo electrónico debido a las indicaciones brindadas en la actividad

The screenshot shows a browser window titled "Prueba de uso - Login Site<". The URL is "pruebadeuso.com/index.php?r=site/login". The page displays a login form for "Publi legal" with fields for "Iniciar sesión" and "yaniralizbethnava@gmail.com". Below the email field is a password input field containing "\*\*\*\*\*". At the bottom of the form are "Ingresar" and "Registrarse" buttons, and a "Recuperar contraseña" link.

The Burp Suite interface is overlaid on the browser. The "Proxy" tab is selected, showing the raw request. The "Inspector" panel on the right shows the request attributes, query parameters, body parameters, cookies, and headers. The "Raw" tab of the proxy interface displays the following POST request:

```
POST /index.php?r=site/login HTTP/1.1
Host: www.pruebadeuso.com
Content-Length: 100
Cache-Control: max-age=0
Accept-Language: es-419
Upgrade-Insecure-Requests: 1
Origin: http://www.pruebadeuso.com
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/126.0.6478.57 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.pruebadeuso.com/index.php?r=site/login
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=f1d139842265d059710749b47955b6a39
Connection: keep-alive
LoginForm$Username$D=yaniralizbethnava4@gmail.com&LoginForm$Password$D=123456789&yt0=Ingresar
LoginForm$Username$D=yaniralizbethnava4@gmail.com&LoginForm$Password$D=ylni9892000&yt0=Ingresar
```

A continuación, podemos observar las Alteraciones que se realizaron a la contraseña.

The screenshot shows a browser window titled "Prueba de uso - Login Site<". The URL is "pruebadeuso.com/index.php?r=site/login". The page displays a login form for "Publi legal" with fields for "Iniciar sesión" and "yaniralizbethlopeznavarro@gmail.c". Below the email field is a password input field containing "\*\*\*\*\*". At the bottom of the form are "Ingresar" and "Registrarse" buttons, and a "Recuperar contraseña" link.

The Burp Suite interface is overlaid on the browser. The "Proxy" tab is selected, showing the raw request. The "Inspector" panel on the right shows the request attributes, query parameters, body parameters, cookies, and headers. The "Raw" tab of the proxy interface displays the following POST request:

```
POST /index.php?r=site/login HTTP/1.1
Host: www.pruebadeuso.com
Content-Length: 107
Cache-Control: max-age=0
Accept-Language: es-419
Upgrade-Insecure-Requests: 1
Origin: http://www.pruebadeuso.com
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/126.0.6478.57 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.pruebadeuso.com/index.php?r=site/login
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=f1d139842265d059710749b47955b6a39
Connection: keep-alive
LoginForm$Username$D=yaniralizbethlopeznavarro4@gmail.com&LoginForm$Password$D=ylni9892000&yt0=Ingresar
LoginForm$Username$D=yaniralizbethlopeznavarro4@gmail.com&LoginForm$Password$D=ylni9892000&yt0=Ingresar
```

En la siguiente imagen nos muestra otra cuenta de correo electrónico y contraseña diferentes que no están registrados en el sitio web.

The screenshot shows a browser window with the URL [pruebadeuso.com/index.php?r=site/login](http://pruebadeuso.com/index.php?r=site/login). The page displays a login form with fields for 'Usuario' and 'Contraseña', and buttons for 'Ingresar' and 'Registrarse'. The 'Ingresar' button is highlighted in blue. Below the form is a link to 'Recuperar contraseña'.

The Burp Suite interface is overlaid on the browser. The 'Proxy' tab is selected, showing a captured request to <http://fonts.googleapis.com/80> [192.178.56.10]. The 'Raw' tab displays the following request:

```
1 GET /css?family=Open+Sans:300,300italic,400,400italic,600,600italic,700,700italic HTTP/1.1
2 Host: fonts.googleapis.com
3 Accept-Language: es-419
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.57 Safari/537.36
5 Accept: text/css,*/*;q=0.1
6 Referer: http://www.pruebadeuso.com/
7 Accept-Encoding: gzip, deflate, br
8 If-Modified-Since: Mon, 24 Jun 2024 01:08:14 GMT
9 Connection: Keep-alive
10
11
```

The 'Inspector' panel on the right shows various request details such as attributes, query parameters, body parameters, cookies, and headers. The status bar at the bottom indicates 'Memory: 117.8MB'.

A continuación, podemos observar los cambios realizados a la cuenta y contraseña.

The screenshot shows the same browser and Burp Suite interface as the previous one, but with a modified request. The 'Raw' tab now contains a POST request to <http://www.pruebadeuso.com/80> [107.180.119.56]. The request includes the following data:

```
1 POST /index.php?r=site/login HTTP/1.1
2 Host: www.pruebadeuso.com
3 Content-Length: 97
4 Cache-Control: max-age=0
5 Accept-Encoding: gzip, deflate, br
6 Upgrade-Insecure-Requests: 1
7 Origin: http://www.pruebadeuso.com
8 Content-Type: application/x-www-form-urlencoded
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.57 Safari/537.36
10 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
11 Referer: http://www.pruebadeuso.com/index.php?r=site/login
12 Accept-Encoding: gzip, deflate, br
13 Cookie: PHPSESSID=fdf139e4226d859710749b47955b6a39
14 Connection: Keep-alive
15
16 LoginForm[5$Username]=yaniranava@gmail.com
17 LoginForm[5$Password]=1234567891011&y=0
18 Ingresar
```

The 'Inspector' panel shows the updated request details. The status bar at the bottom indicates 'Memory: 119.8MB'.

En la siguiente imagen podemos observar que se llevó a cabo el proceso realizado a lo largo de la práctica y aun cuando se realizaron los cambios mencionados no me fue posible ingresar de manera exitosa debido a que el sitio web no es de mi propiedad y nouento con las credenciales correctas que me permitan ingresar.

The screenshot shows a browser window titled "Prueba de uso - Login Site<". The address bar indicates the site is "No seguro" and the URL is "pruebadeuso.com/index.php?r=site/login". The page itself is a login form for "Publi legal". It features a dark header with "Publi legal" and "Iniciar sesión". Below this, there's a text input field containing "yaniranava@gmail.com" and a password input field with masked content. A red message states: "El usuario está deshabilitado, contáctate a su ejecutivo de cuenta". At the bottom are two buttons: "Ingresar" (highlighted in blue) and "Registrarse". A link "Recuperar contraseña" is also present. The right side of the screen displays the Burp Suite interface. The "Proxy" tab is selected, showing the captured POST request. The request details pane shows the following headers and body:

```
POST /index.php?r=site/login HTTP/1.1
Host: www.pruebadeuso.com
Content-Length: 97
Cache-Control: max-age=0
Accept-Language: es-419
Upgrade-Insecure-Requests: 1
Origin: http://www.pruebadeuso.com
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/126.0.6478.57 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.pruebadeuso.com/index.php?r=site/login
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=f1139842265d859710749b47955b6a39
Connection: keep-alive
LoginForm[5]username[5D]=yaniranava4@gmail.com&LoginForm[5Bpassword[5D]=1234567891011&t0=Ingresar
```

The "Inspector" tab is open, showing the request attributes, query parameters, body parameters, cookies, and headers. The status bar at the bottom right shows "Memory: 119.8MB".

## Conclusión

La realización de esta actividad de pruebas de vulnerabilidad Cross Site Scripting (XSS) ha demostrado ser de vital importancia tanto en el ámbito laboral como en nuestra vida cotidiana. En un mundo donde la tecnología y las aplicaciones web están profundamente integradas en nuestras rutinas diarias, garantizar la seguridad de estas plataformas no es solo una responsabilidad profesional, sino una necesidad para proteger nuestra información personal y la de los demás.

A través de esta actividad, hemos aprendido a identificar y mitigar vulnerabilidades XSS, mejorando así nuestras habilidades técnicas y nuestra capacidad para proteger entornos digitales. Estas habilidades son esenciales en el campo laboral, donde la seguridad de los datos y la integridad de los sistemas informáticos son cruciales para el éxito y la confianza de los clientes. Pero más allá del ámbito profesional, este conocimiento también se traduce en una mayor conciencia y capacidad para proteger nuestra información personal en nuestras interacciones diarias en línea.

La actividad no solo nos ha mostrado la gravedad de las amenazas XSS, sino también la importancia de estar siempre un paso adelante en términos de seguridad cibernetica. Al aplicar estos conocimientos, estamos contribuyendo a crear un entorno digital más seguro y confiable para todos

## Referencias

Ingeniería en desarrollo de software. Universidad México Internacional. Recuperado el día 21 de junio de 2024, [umi.edu.mx/coppel/IDS/mod/scorm/player.php](http://umi.edu.mx/coppel/IDS/mod/scorm/player.php)

*Video conferencing, web conferencing, webinars, screen sharing.* (s. f.). Zoom. [https://academiaglobal-mx.zoom.us/rec/play/1MpPOitg1mPH7hMrQbeKHuOfNATsJi8d-11SrXSJAu47yV86hS2ucF5HuPqQNqN-5pZJMImBn4JUyp-k.dq6TBS1JS98frpn?canPlayFromShare=true&from=share\\_recording\\_detail&continueMode=true&componentName=rec-play&originRequestUrl=https%3A%2F%2Facademiaglobal-mx.zoom.us%2Frec%2Fshare%2FMpClRdjf8kiSF7ceZKjOQ\\_bXHsOk1vjK9p0eC9-NBgN1d51EH3XfjvPqcYahxers.doPPNRS\\_HIQiVvgg](https://academiaglobal-mx.zoom.us/rec/play/1MpPOitg1mPH7hMrQbeKHuOfNATsJi8d-11SrXSJAu47yV86hS2ucF5HuPqQNqN-5pZJMImBn4JUyp-k.dq6TBS1JS98frpn?canPlayFromShare=true&from=share_recording_detail&continueMode=true&componentName=rec-play&originRequestUrl=https%3A%2F%2Facademiaglobal-mx.zoom.us%2Frec%2Fshare%2FMpClRdjf8kiSF7ceZKjOQ_bXHsOk1vjK9p0eC9-NBgN1d51EH3XfjvPqcYahxers.doPPNRS_HIQiVvgg)

Global, A. (2024, 23 junio). *Video 1 Pruebas de Vulnerabilidades Pérdida de Autenticación y Gestión de Sesiones.mp4* [Vídeo]. Vimeo. <https://vimeo.com/711845557/a5ae411ce9>

*Video conferencing, web conferencing, webinars, screen sharing.* (s. f.-b). Zoom. [https://academiaglobal-mx.zoom.us/rec/play/OtAXnEL1KvZCjkXJkpzzVl0deAtnsgRptKkBAbTm7N7ypHlfF7y44GmC4JcYgfvGc8ROwNAb0qYXgATS.g5vSQmrZNdA2qsCR?canPlayFromShare=true&from=share\\_recording\\_detail&continueMode=true&componentName=rec-play&originRequestUrl=https%3A%2F%2Facademiaglobal-mx.zoom.us%2Frec%2Fshare%2FwyoBfUZGMNtoBmg63kvFI\\_KCdXuxAfTJ153juoc3ZCjR7nEBp1P6YZxcUrLde6cI.Pn4JF23e-0hKmIt](https://academiaglobal-mx.zoom.us/rec/play/OtAXnEL1KvZCjkXJkpzzVl0deAtnsgRptKkBAbTm7N7ypHlfF7y44GmC4JcYgfvGc8ROwNAb0qYXgATS.g5vSQmrZNdA2qsCR?canPlayFromShare=true&from=share_recording_detail&continueMode=true&componentName=rec-play&originRequestUrl=https%3A%2F%2Facademiaglobal-mx.zoom.us%2Frec%2Fshare%2FwyoBfUZGMNtoBmg63kvFI_KCdXuxAfTJ153juoc3ZCjR7nEBp1P6YZxcUrLde6cI.Pn4JF23e-0hKmIt)

Global, A. (2024b, junio 23). *Video 2 Deserialización Insegura.mp4* [Vídeo]. Vimeo. <https://vimeo.com/711846733/1d604d66b2>

*Video conferencing, web conferencing, webinars, screen sharing.* (s. f.). Zoom. [https://academiaglobal-mx.zoom.us/rec/play/2hW11RqqiyAh3xoL0mqvscc2cXyhYW9q1Qgu41MQN7tUH0XUjAytbHF\\_ZIYL3uvKn0qe50hAB-r41sDe.cLoNdDrLxNfUxOQE?canPlayFromShare=true&from=share\\_recording\\_detail&continueMode=true&componentName=rec-play&originRequestUrl=https%3A%2F%2Facademiaglobal-mx.zoom.us%2Frec%2Fshare%2FoG6gen18Wkc\\_8h4EAH2lghD5TS\\_E4WHHu-cUWX1LA28PknlKiVdn0Yu70aAo\\_nfF.FB1fyDBoLCGspiOC](https://academiaglobal-mx.zoom.us/rec/play/2hW11RqqiyAh3xoL0mqvscc2cXyhYW9q1Qgu41MQN7tUH0XUjAytbHF_ZIYL3uvKn0qe50hAB-r41sDe.cLoNdDrLxNfUxOQE?canPlayFromShare=true&from=share_recording_detail&continueMode=true&componentName=rec-play&originRequestUrl=https%3A%2F%2Facademiaglobal-mx.zoom.us%2Frec%2Fshare%2FoG6gen18Wkc_8h4EAH2lghD5TS_E4WHHu-cUWX1LA28PknlKiVdn0Yu70aAo_nfF.FB1fyDBoLCGspiOC)

Global, A. (2024, 25 junio). *Video 3 Cross Site Scripting XSS.mp4* [Vídeo]. Vimeo.

<https://vimeo.com/711848472/79fbb3539b>