Universidad Corporativa Coppel | Programas Académicos

Ingeniería en Desarrollo de Software

Actividad | 2 |

Deserialización Insegura

Auditoría Informática

Ingeniería en Desarrollo de Software

TUTOR: Jessica Hernández Romero

ALUMNO: Yanira Lizbeth Lopez Navarro

FECHA: 23/06/2024

Índice

Introducción

El ataque de pérdida de autenticación de datos es una seria amenaza en el mundo digital que afecta directamente a la seguridad y privacidad de los usuarios de internet. Este tipo de ataque ocurre cuando los sistemas de verificación de identidad fallan, permitiendo que personas no autorizadas accedan a información personal y confidencial. Los usuarios se enfrentan a riesgos significativos, como el robo de identidad, donde sus datos personales, incluyendo contraseñas y detalles financieros, pueden ser utilizados de manera fraudulenta.

Para los usuarios, este ataque puede resultar en la pérdida de acceso a sus cuentas en servicios esenciales como correos electrónicos, redes sociales y plataformas de banca en línea, causando una interrupción significativa en sus vidas cotidianas. Además, la exposición de información sensible puede llevar a consecuencias financieras graves y a la erosión de la confianza en las plataformas digitales.

Desde una perspectiva empresarial, la pérdida de autenticación no solo pone en riesgo a los usuarios, sino que también puede dañar la reputación de la empresa y resultar en pérdidas económicas sustanciales. Este tipo de ataque resalta la necesidad de sistemas de seguridad robustos y la importancia de proteger la integridad de los datos en el entorno digital.

Descripción

En esta actividad, espero aprender cómo identificar y explotar vulnerabilidades de deserialización insegura en aplicaciones web, utilizando Burp Suite Community Edition. Este tipo de ataque, centrado en la manipulación de cookies para escalar privilegios, es una lección crucial en el ámbito de la ciberseguridad.

El proceso comenzará iniciando sesión en una página web proporcionada por PortSwigger, usando credenciales de usuario normal. Mediante el análisis y modificación de cookies, buscaremos cambiar los privilegios de usuario para acceder al modo administrador. Este ejercicio práctico nos permitirá comprender a fondo cómo la deserialización insegura puede ser utilizada por atacantes para comprometer la seguridad de una aplicación.

La meta final de eliminar la cuenta de Carlos servirá como prueba de la efectividad del ataque y de nuestra capacidad para manipular correctamente los objetos serializados en las cookies de sesión. Este conocimiento es valioso tanto en el campo laboral como en la vida cotidiana, ya que nos dota de las habilidades necesarias para proteger aplicaciones web y datos sensibles, evitando que usuarios malintencionados puedan explotar estas vulnerabilidades. Además, fortalecerá nuestra comprensión sobre la importancia de implementar y mantener medidas de seguridad robustas en el desarrollo de software.

Justificación

En un entorno donde la seguridad de la información es primordial, comprender cómo las vulnerabilidades pueden ser explotadas es esencial para proteger tanto a los usuarios como a las organizaciones. Realizar pruebas de deserialización insegura es vital para identificar debilidades específicas en el manejo de sesiones y la gestión de privilegios dentro de aplicaciones web. Utilizando herramientas como Burp Suite Community Edition y la plataforma PortSwigger, podemos simular ataques realistas que nos permiten analizar y modificar cookies, escalando de un usuario normal a un administrador.

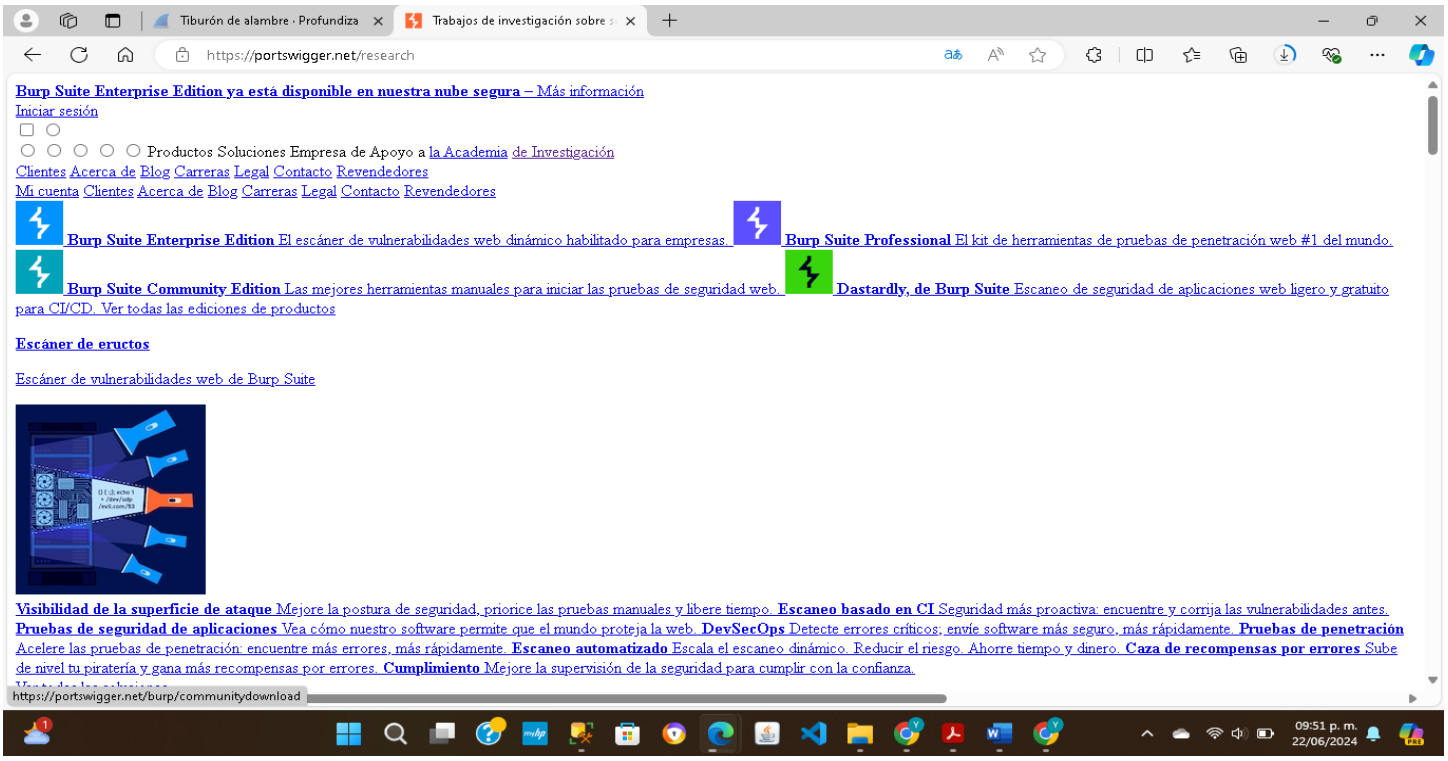
Esta experiencia es crucial para desarrollar habilidades prácticas en la detección y mitigación de amenazas de deserialización insegura. Al simular estos ataques, los profesionales de seguridad pueden entender mejor cómo los atacantes podrían explotar estas vulnerabilidades, lo que les permite anticipar y prevenir posibles brechas de seguridad. Además, capacita a los desarrolladores para implementar mejores prácticas de seguridad en el desarrollo de software, asegurando que las aplicaciones sean más robustas frente a este tipo de amenazas.

La deserialización insegura es una vulnerabilidad crítica que puede tener consecuencias devastadoras si no se aborda adecuadamente. Puede permitir a los atacantes ejecutar código arbitrario, escalar privilegios y acceder a datos sensibles, comprometiendo la integridad y confidencialidad de la información. Por lo tanto, realizar estas pruebas no solo es una práctica recomendada, sino una necesidad imperante para cualquier organización que valore la seguridad de sus sistemas y datos.

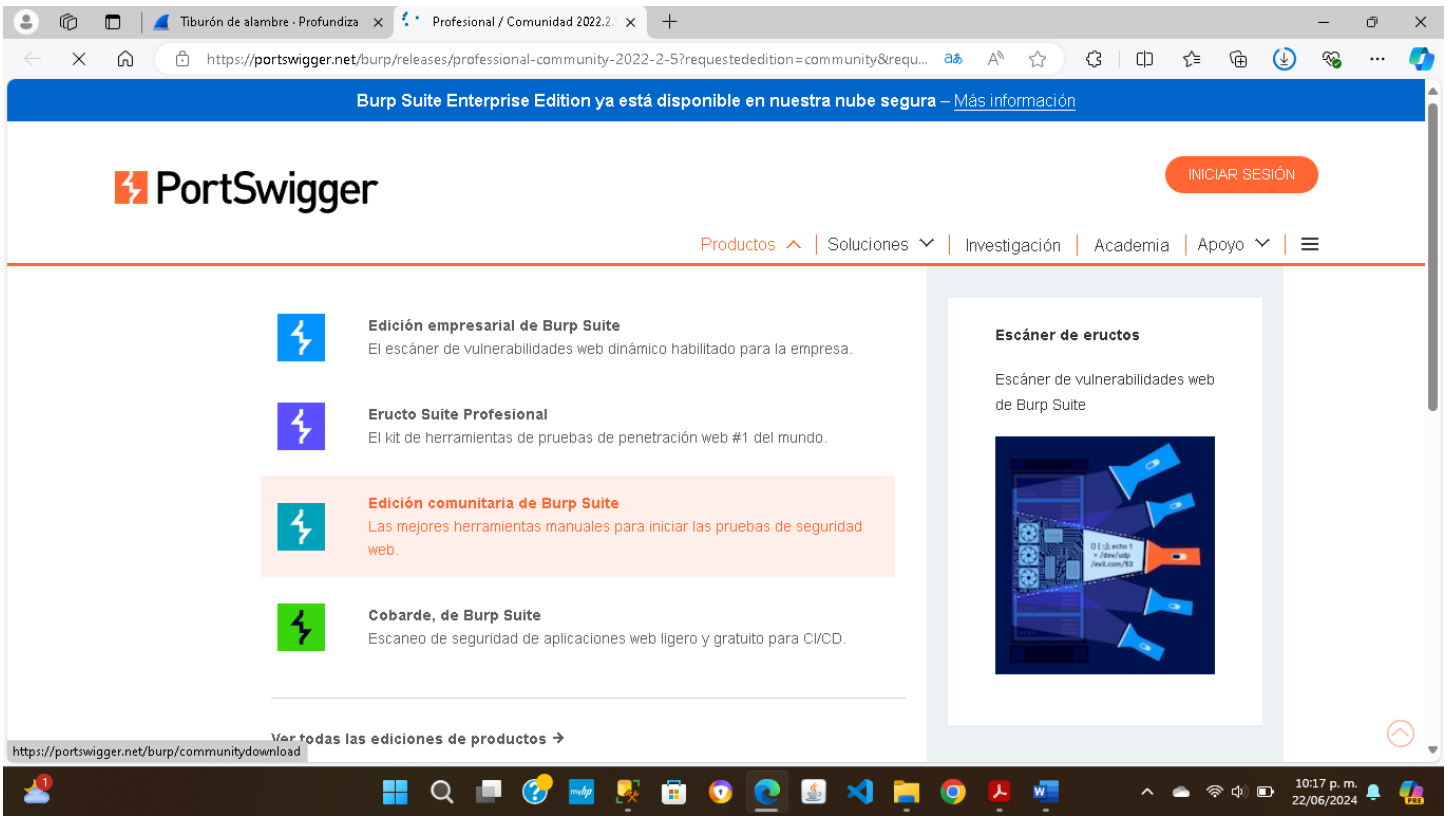
En última instancia, esta prueba refuerza la importancia de la seguridad en el diseño y la implementación de aplicaciones web, garantizando un entorno digital más seguro y confiable. Nos permite desarrollar un enfoque proactivo hacia la ciberseguridad, fortaleciendo nuestras defensas contra posibles ataques y protegiendo la información crítica. Al mejorar nuestra capacidad para detectar y mitigar estas vulnerabilidades, contribuimos a un ecosistema digital más seguro para todos los usuarios.

Ataque al sitio

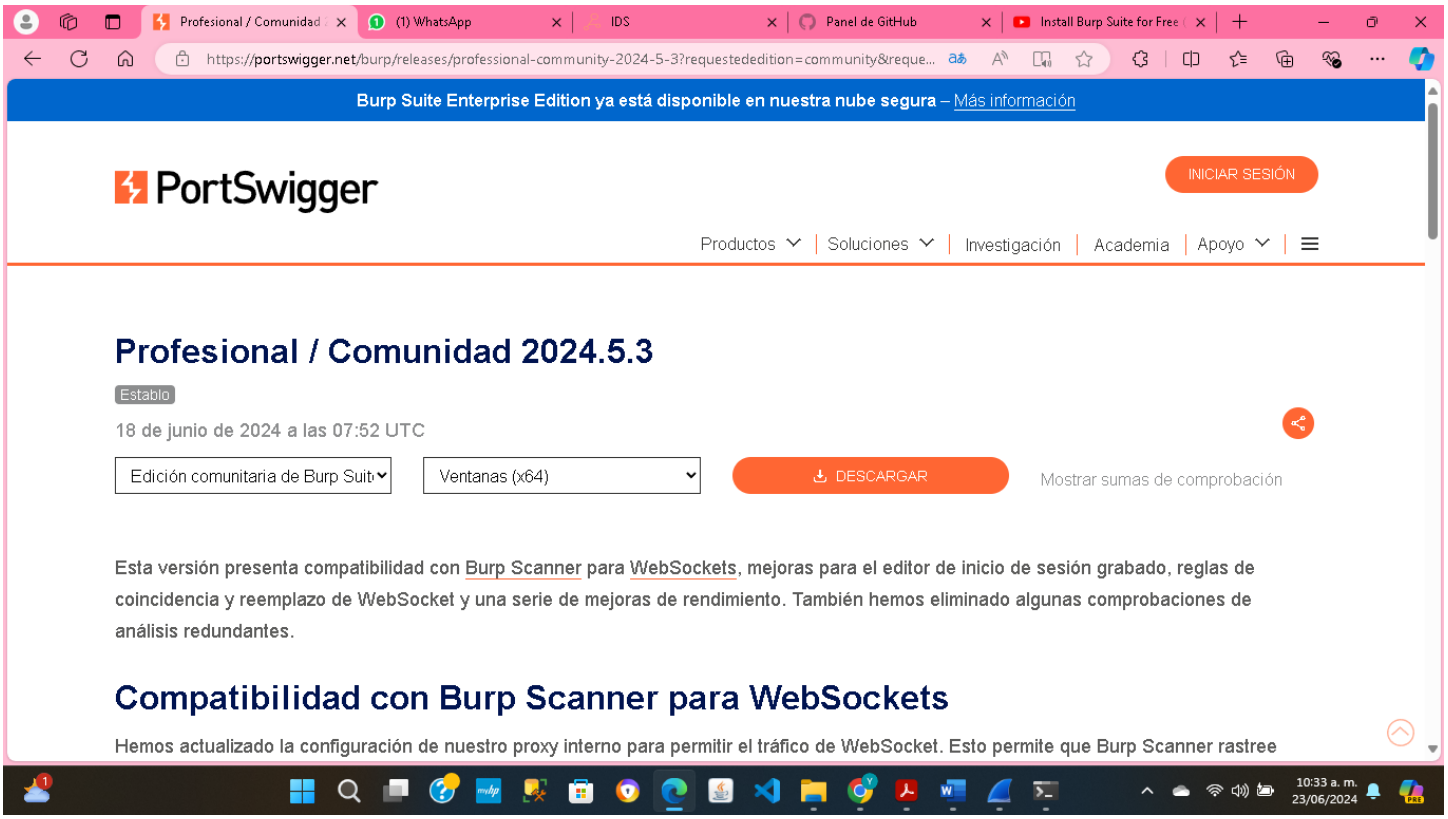
En la siguiente imagen nos muestra la página que nos permitirá descargar la herramienta sugerida en la actividad.



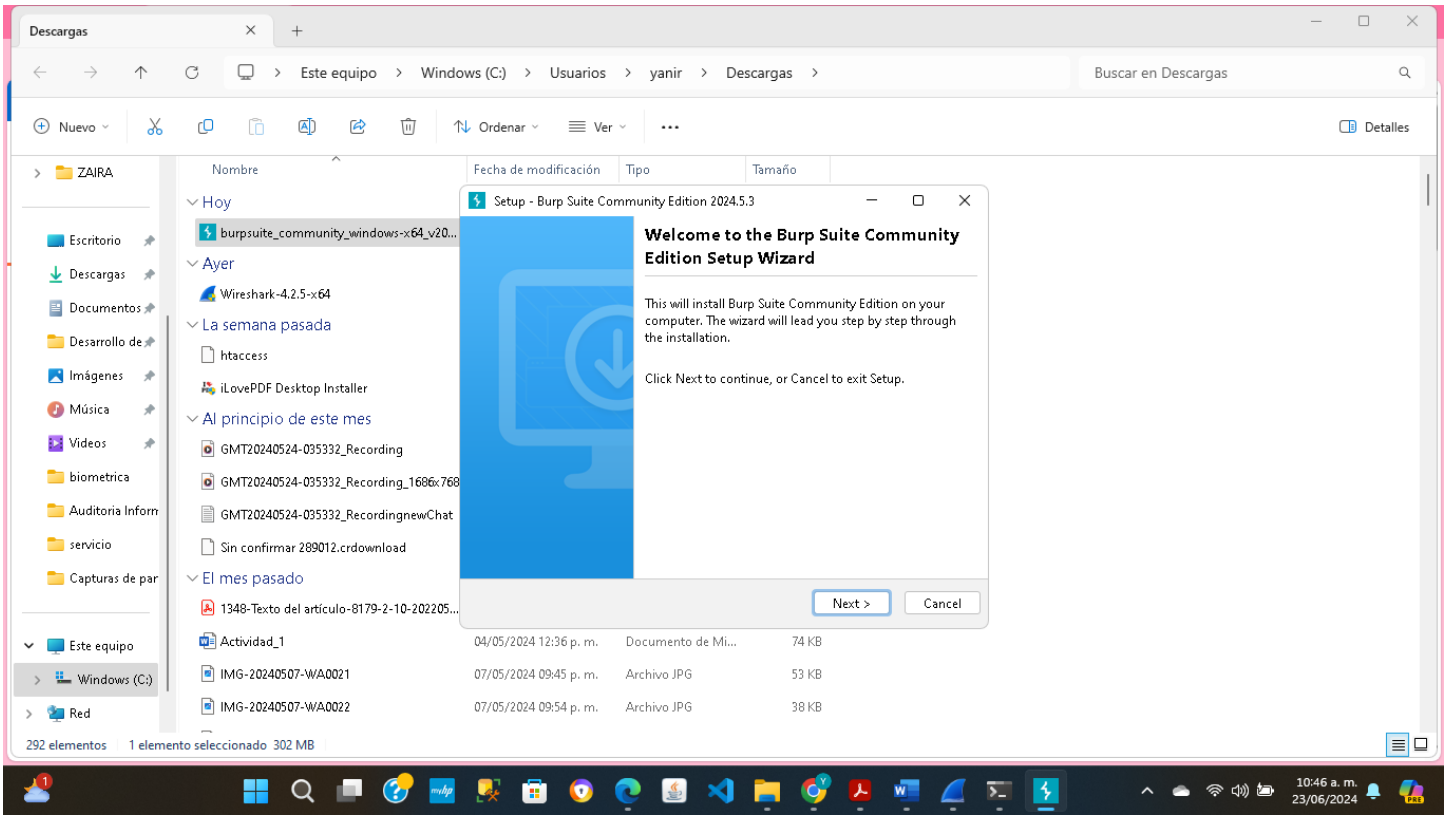
A continuación, procedemos con la selección Edición comunitaria de Burp Suite.



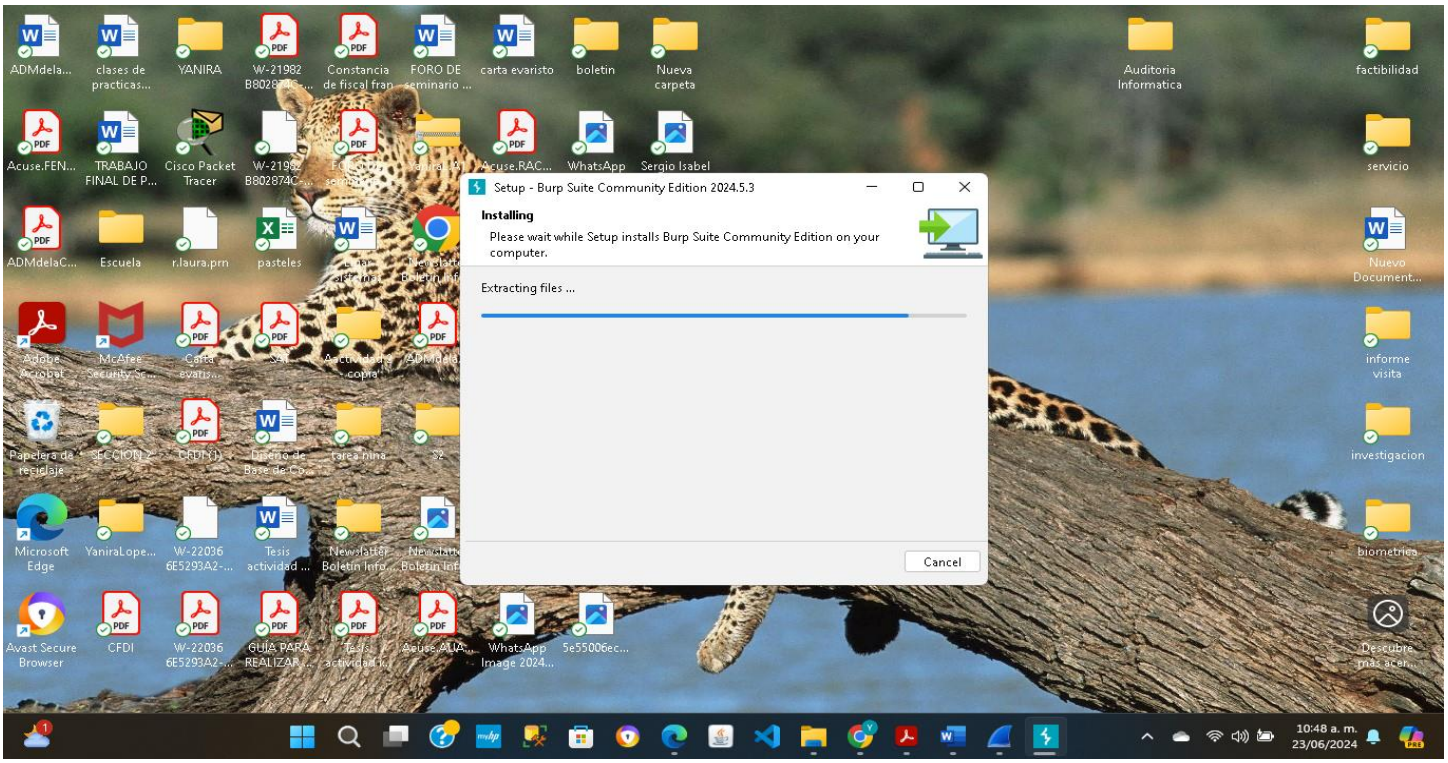
A continuación, seleccionamos la versión que sea compatible con mi equipo de cómputo.



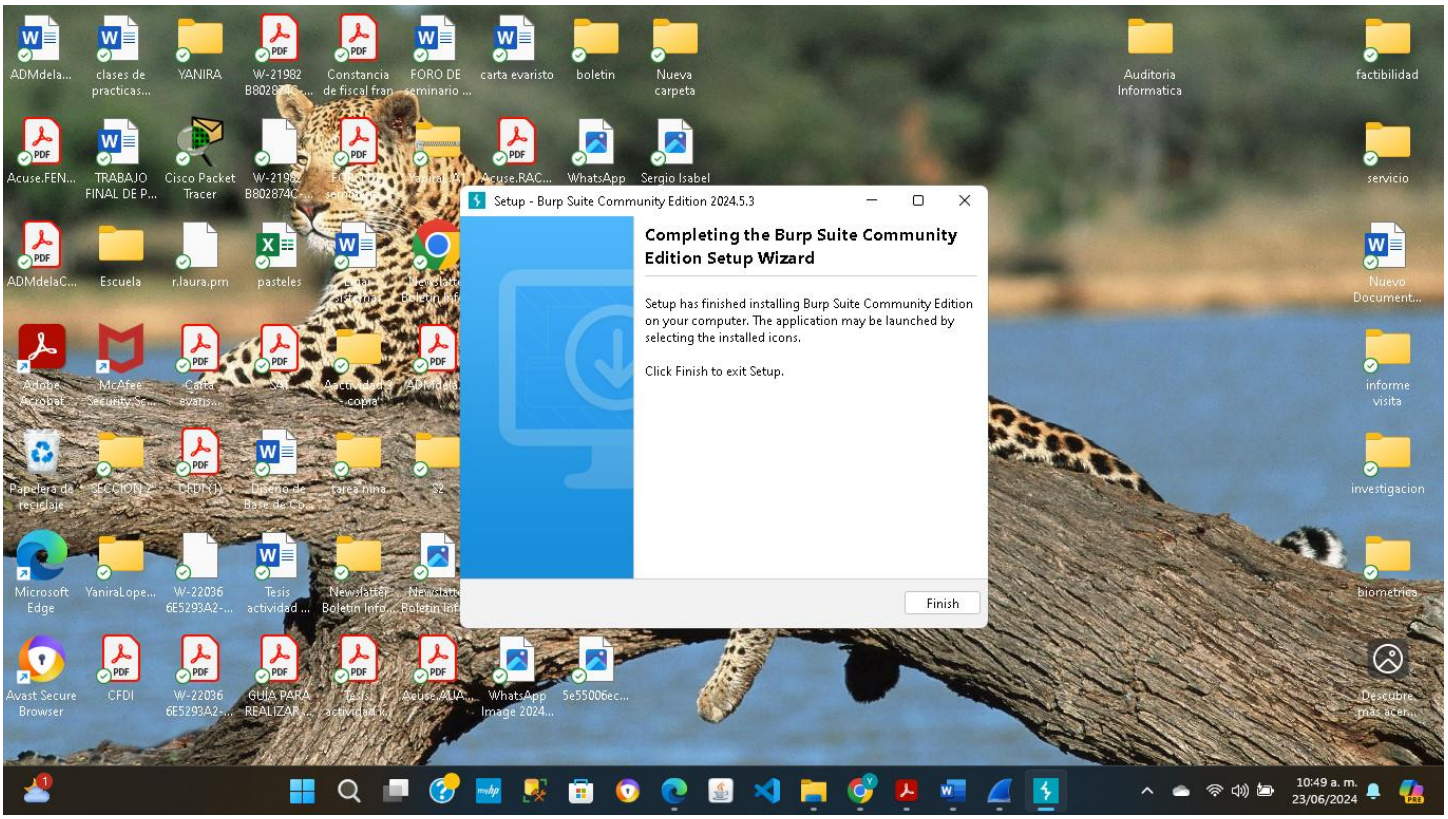
En la siguiente imagen nos indica que podemos iniciar con la instalación de Burp Suite Community Edition.



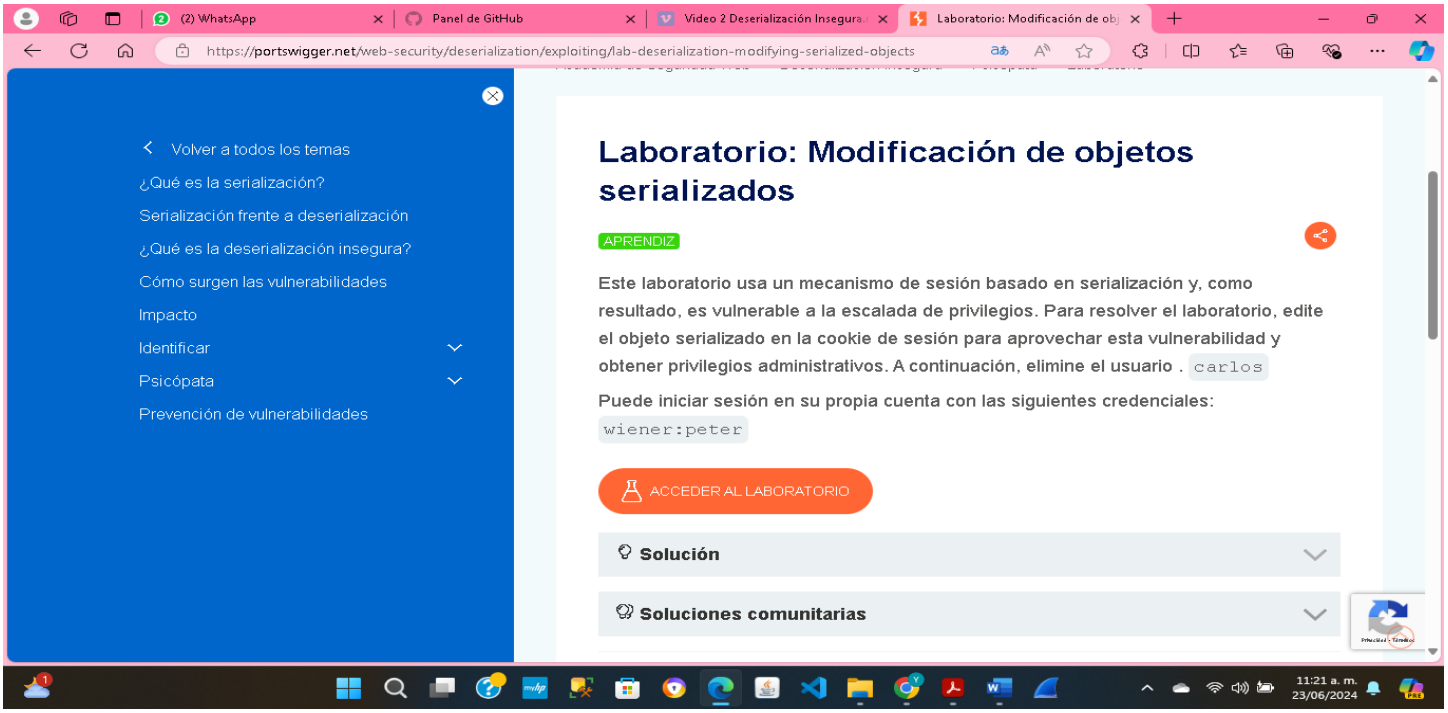
A continuación, la siguiente imagen nos muestra el avance de instalación de Burp Suite Community Edition.



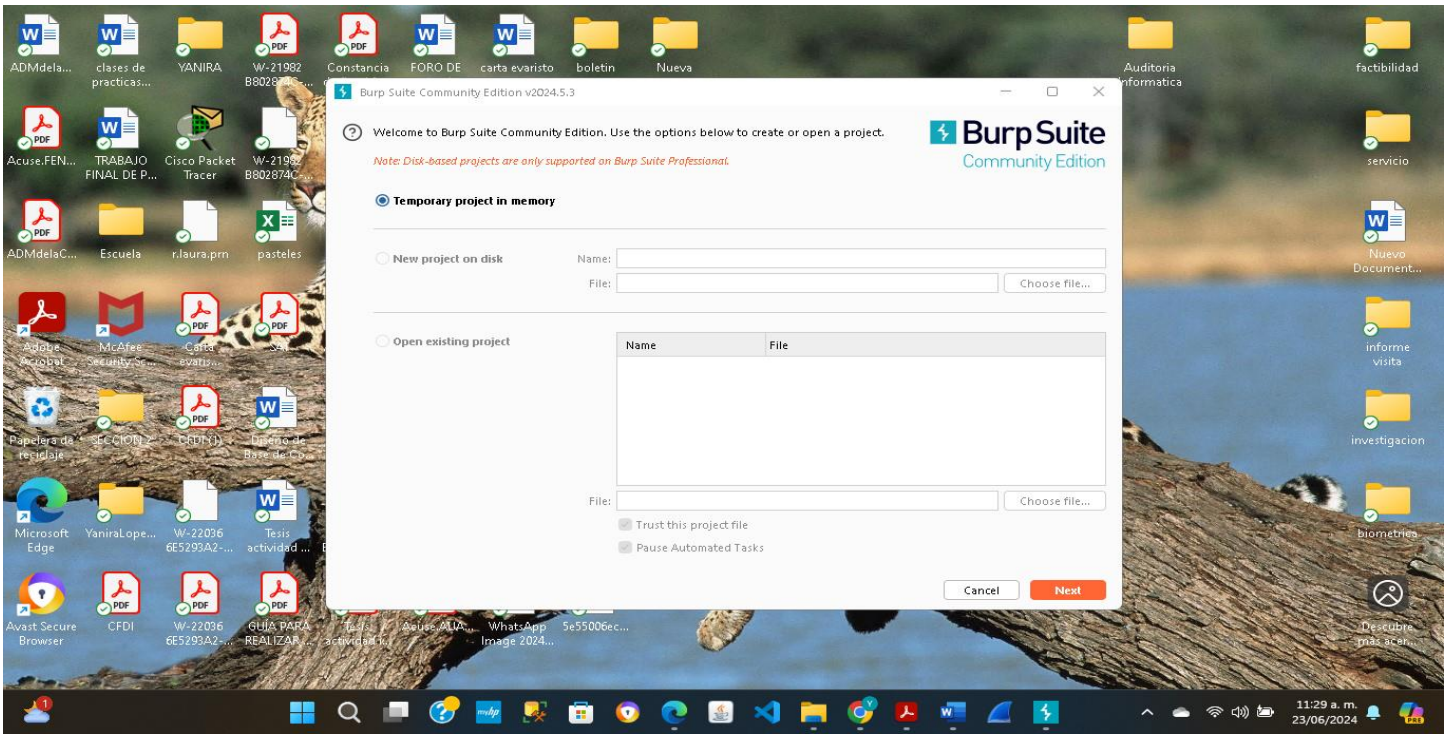
En la siguiente imagen podemos observar que se llevó a cabo la instalación de Burp Suite Community Edition de manera exitosa. Este es el software a utilizar para realizar la práctica del laboratorio.



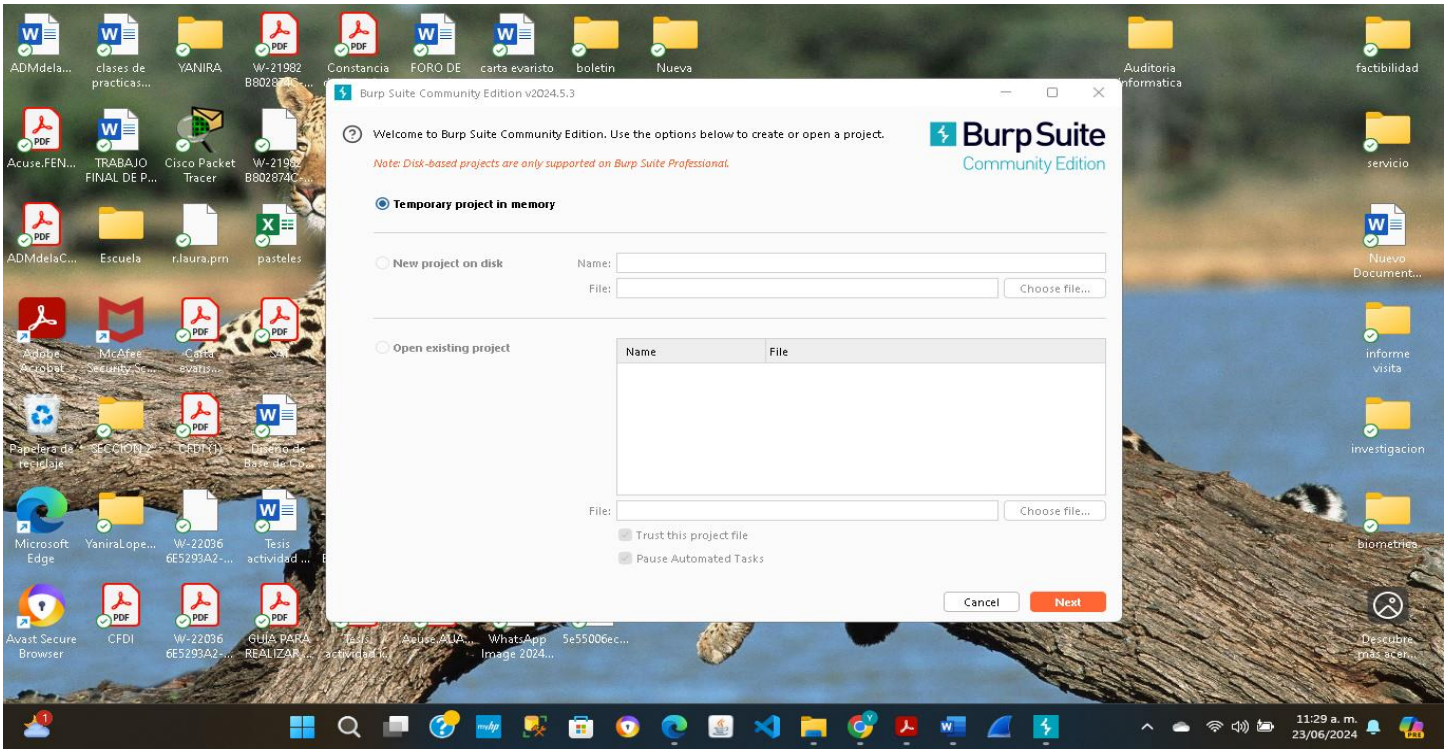
Una vez instalado el programa, procedemos a entrar al enlace del laboratorio de práctica que nos fue proporcionado en la sección Recursos del material brindado.



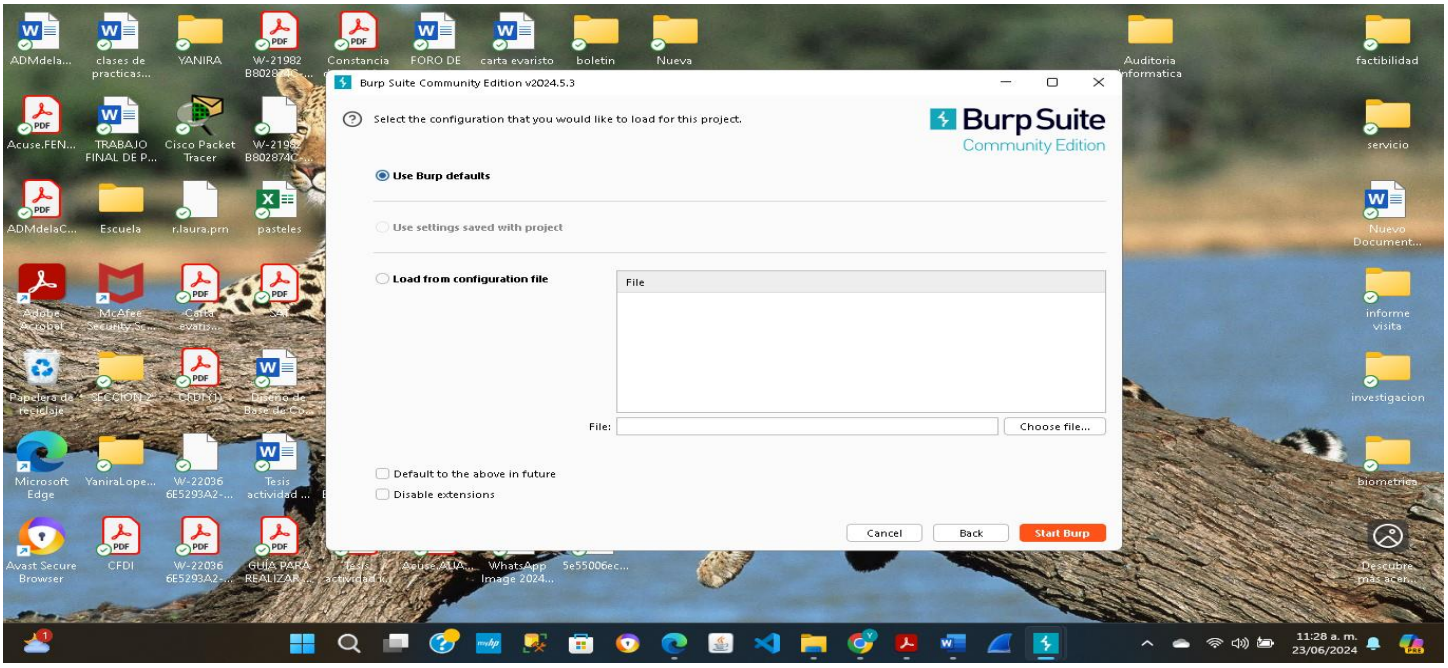
A continuación, nos muestra la siguiente imagen al abrir Burp Suite de acuerdo a lo que indica la actividad.



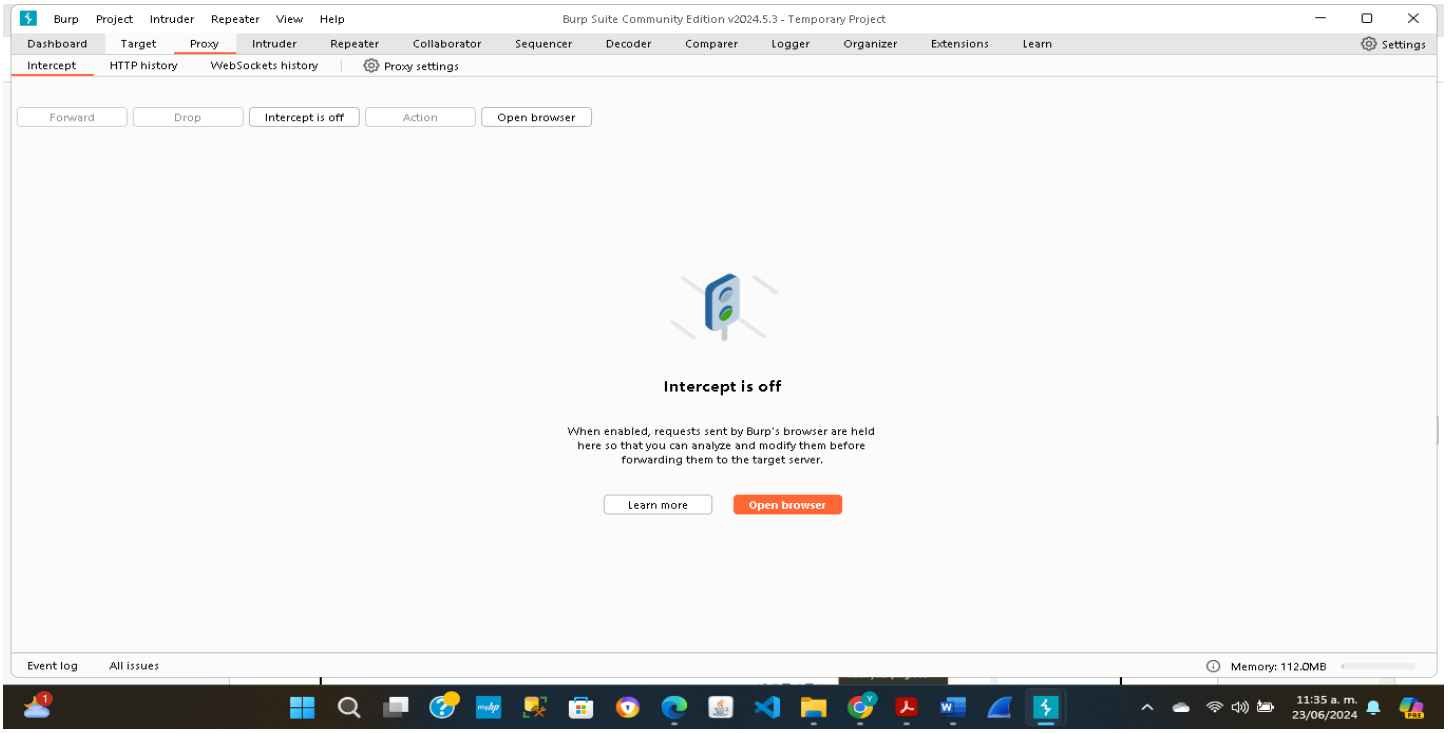
En la siguiente pantalla, nos muestra la seleccionar el tipo de proyecto a realizar. En esta ocasión, dejare el que viene por default: Temporary Project.



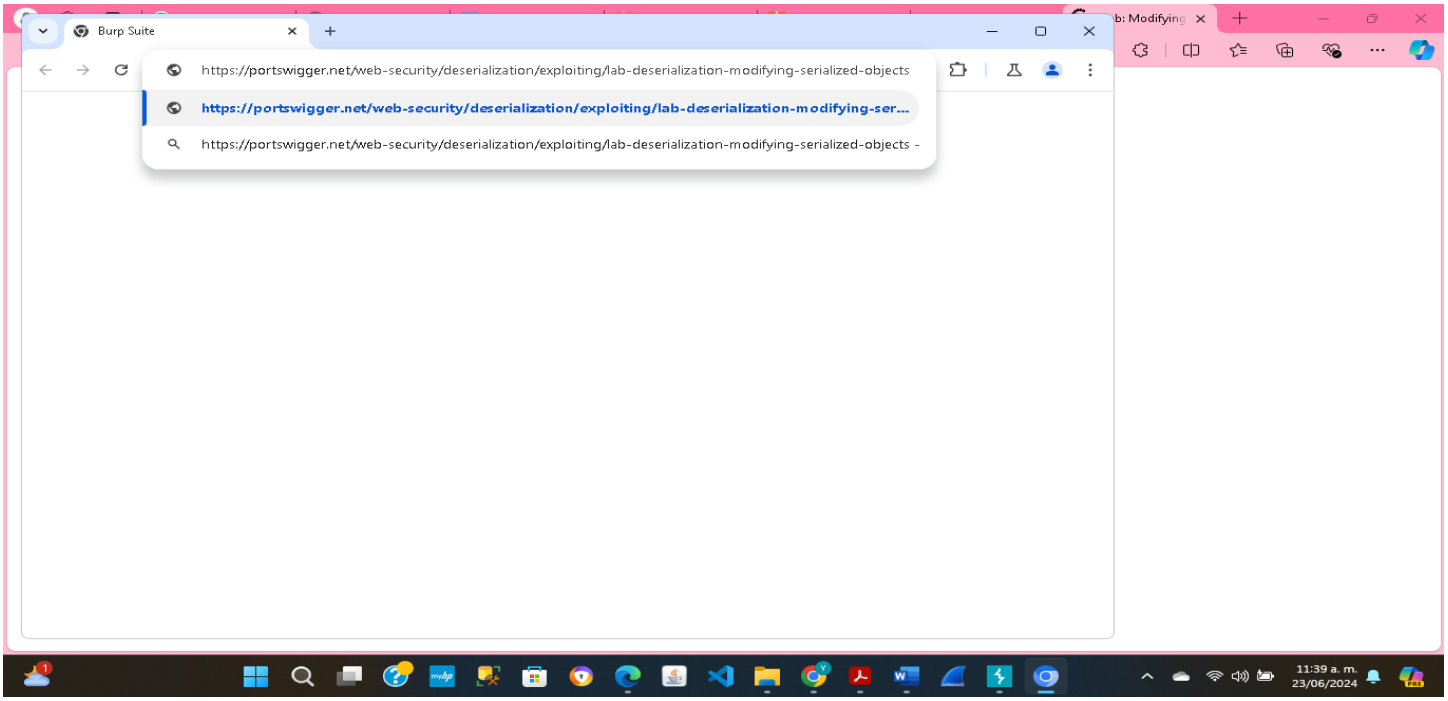
Después, dar clic en *Next*. Luego, pedirá realizar la configuración del proyecto. Por ello, dejar la opción que viene por defecto, y dar clic en *Start Burp*.



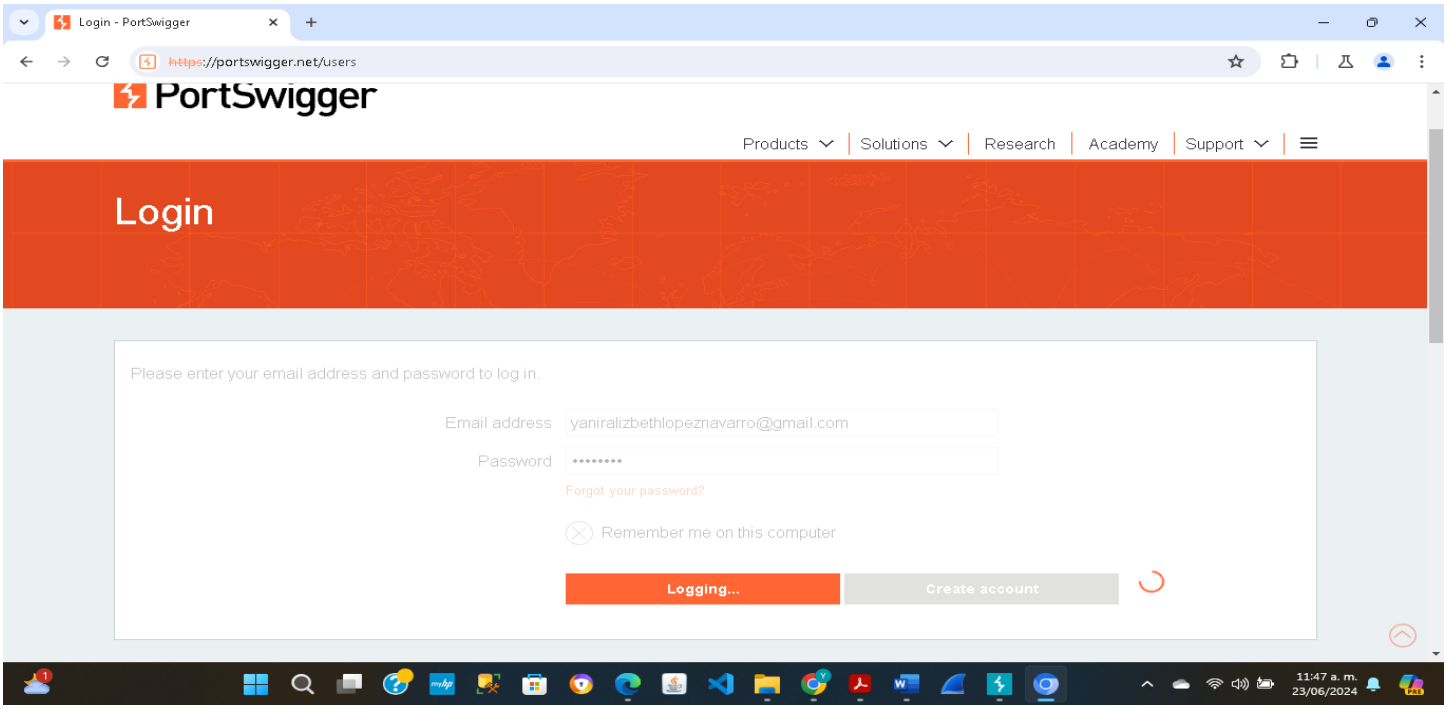
En la siguiente pantalla está la interfaz del programa en la cual, para realizar la práctica, entraremos a la interfaz *Proxy*, como se puede ver en la siguiente imagen.



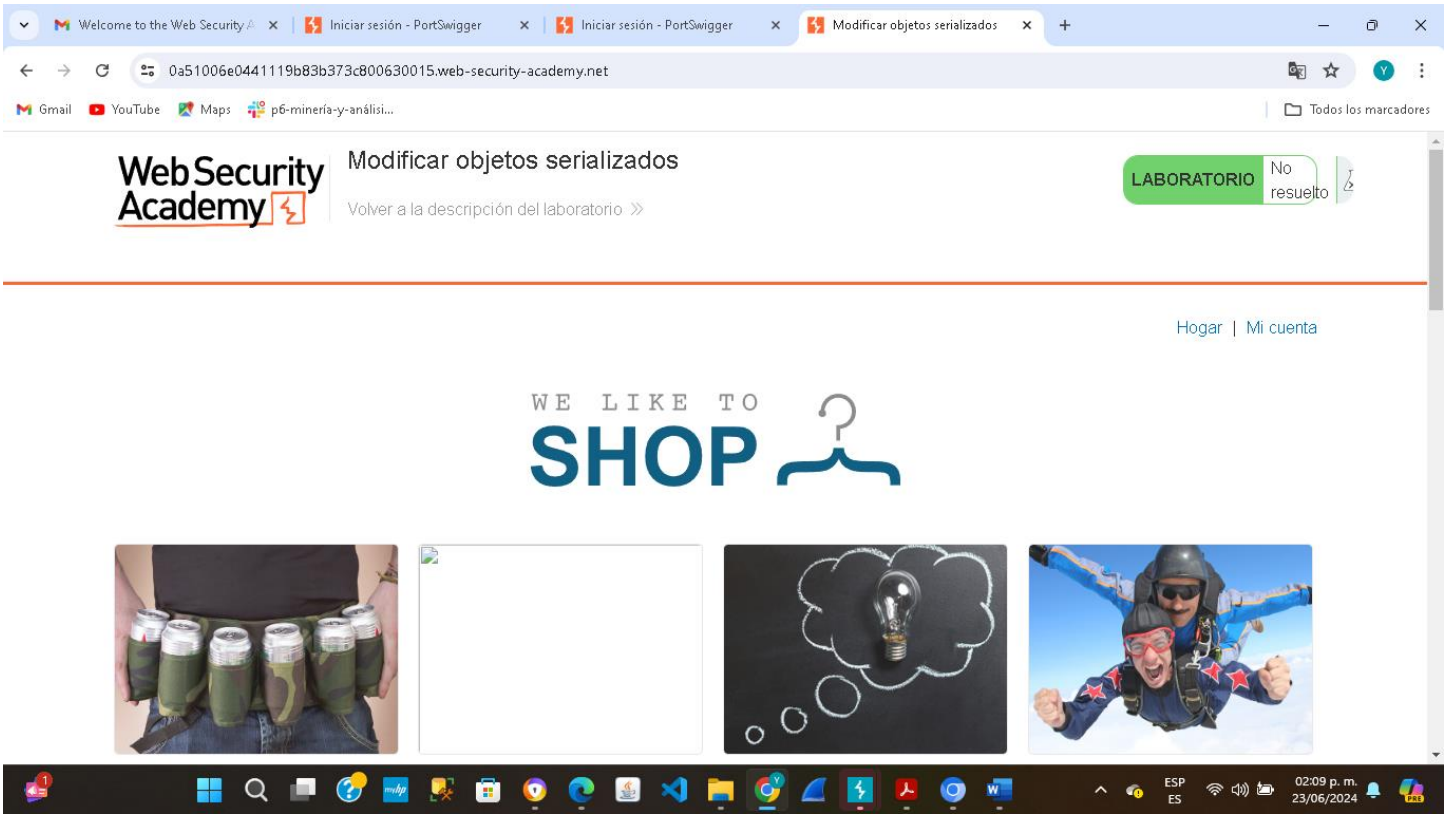
Para iniciar con la práctica, daremos clic en ***Open Browser***, lo cual abrirá un navegador que está vinculado con el programa. Una vez que se haya abierto el navegador, copiaremos el enlace de la página del laboratorio (este se encuentra en la sección *Recursos* del presente documento.



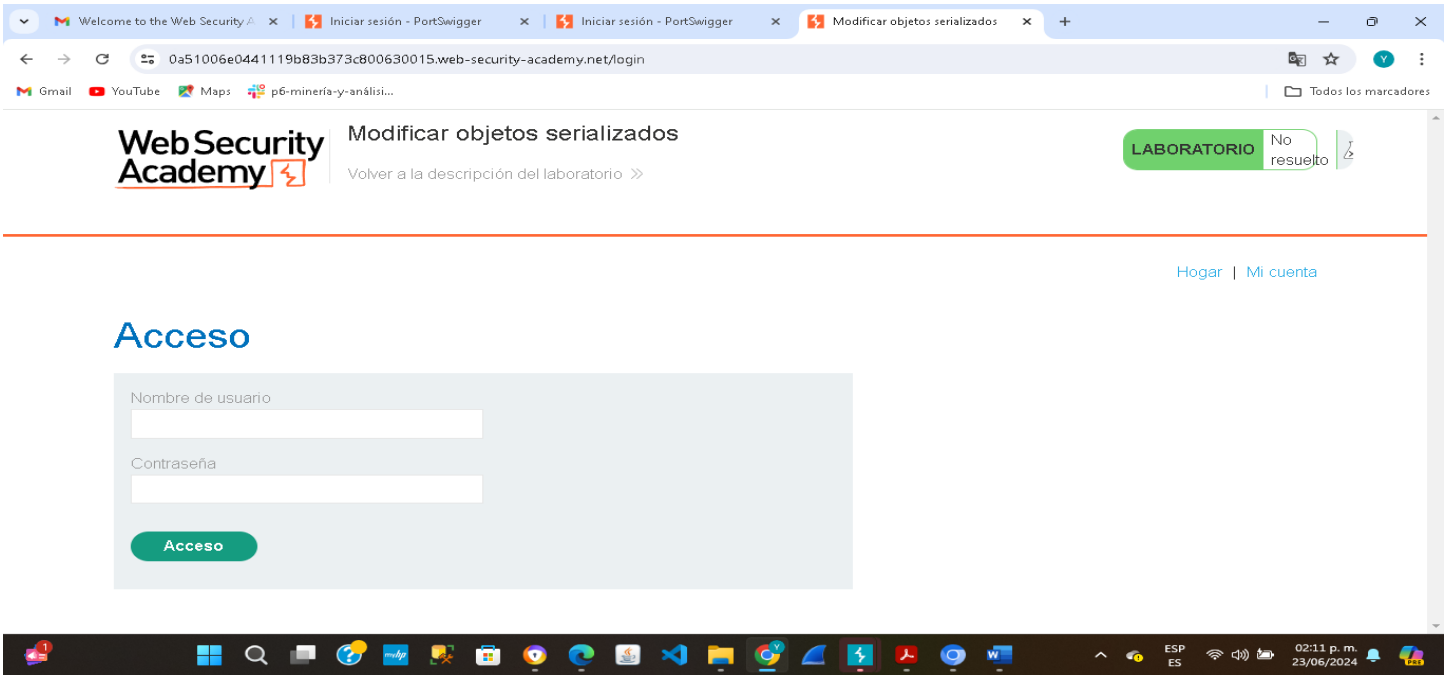
Una vez dentro de la página del laboratorio se verá la siguiente pantalla: Para poder realizar la práctica en el laboratorio, es importante generar una nueva cuenta en PortSwigger.



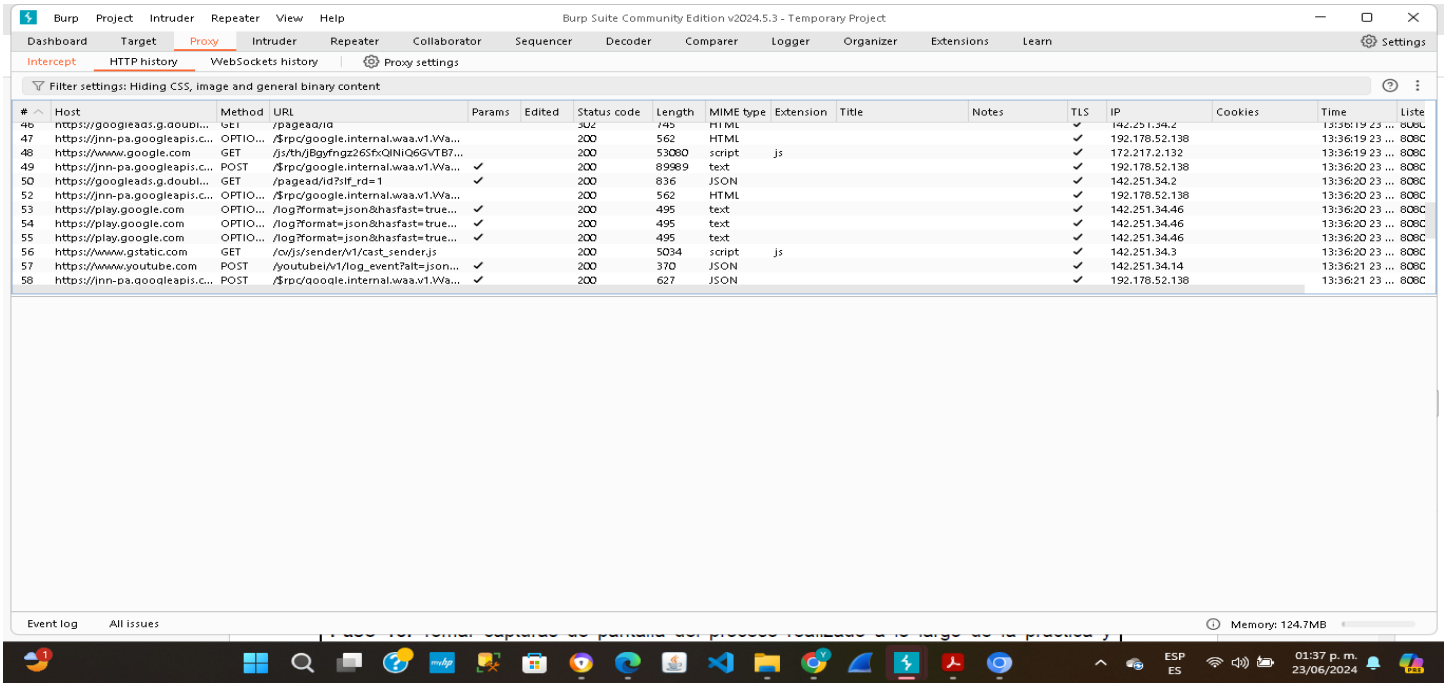
A continuación, podemos observar que, una vez creada la cuenta e iniciado sesión, entrar al laboratorio de práctica.



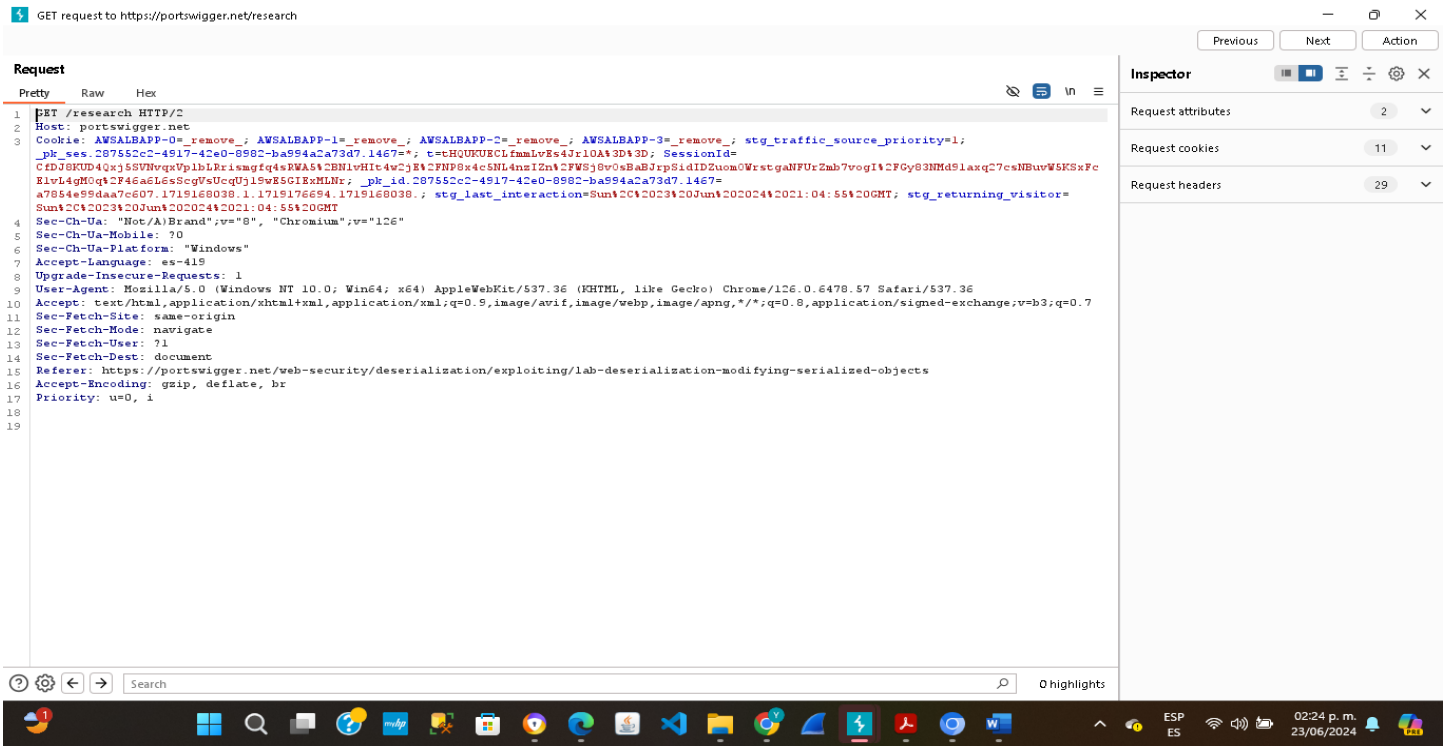
A continuación, en la siguiente imagen ingresaremos las credenciales proporcionadas en el material de la actividad.



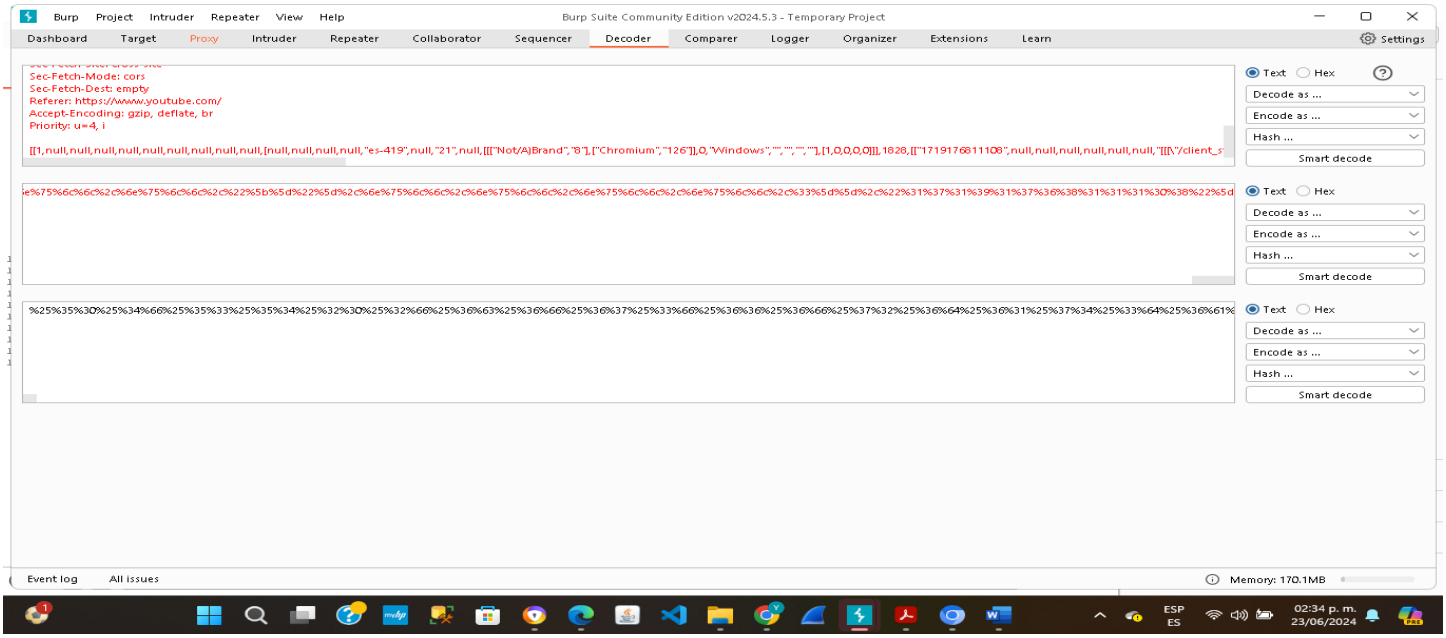
La siguiente imagen nos muestra que ingresamos al *Burp* y al dar clic en el botón *Intercept is off*. Con esto, se encenderá el interceptador para captar todas las salidas de la página como se muestran a continuación.



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



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



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

Conclusión

La realización de esta actividad ha sido fundamental para comprender y abordar una de las vulnerabilidades más críticas en el ámbito de la ciberseguridad: la deserialización insegura. En el campo laboral, este conocimiento es invaluable, ya que nos permite identificar y corregir debilidades en las aplicaciones web que desarrollamos y mantenemos. Aprender a utilizar herramientas como Burp Suite Community Edition y la plataforma PortSwigger nos capacita para proteger mejor los sistemas que manejan información sensible, garantizando la seguridad y privacidad de los datos.

Además, en nuestra vida cotidiana, este aprendizaje nos hace más conscientes de los riesgos a los que estamos expuestos al interactuar con diversas plataformas en línea. Saber cómo los atacantes pueden manipular datos para escalar privilegios nos ayuda a valorar la importancia de utilizar sitios web que implementen medidas de seguridad robustas y a ser más cautelosos con la información que compartimos.

Esta experiencia también subraya la importancia de la formación continua en ciberseguridad. En un mundo cada vez más digital, estar preparados para enfrentar nuevas amenazas es crucial. A través de actividades prácticas como esta, fortalecemos nuestras habilidades y contribuimos a crear un entorno digital más seguro y confiable para todos. La actividad no solo mejora nuestra capacidad técnica, sino que también nos empodera para protegernos y proteger a otros en el vasto mundo de internet.

Referencias

Ingeniería en desarrollo de software. Universidad México Internacional. Recuperado el día 18 de junio de 2024, 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.dq6TBS1J-S98frpn?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-0hKmItd

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