Universidad Corporativa | Programas Académicos

Ingeniería en Desarrollo de Software

Actividad 2 – Deserialización insegura.

Auditoria Informática.

Ingeniería en Desarrollo de Software.

Tutor: Jessica Hernández.

Alumno: Gerardo Rojo.

Fecha: 19/10/2024.

Contenido

Introducción.

Estamos ya en la segunda actividad correspondiente de nuestra materia Auditoria Informática. Noa hemos de posicionar en el marco de un proyecto de seguridad informática, una empresa de software ha solicitado la realización de diversas pruebas en páginas web, dichas paginas carecen de las medidas de seguridad adecuadas. Estas pruebas son esenciales parala empresa ya que requieren identificar y mitigar posibles vulnerabilidades que podrían ser explotadas por atacantes malintencionados. En esta segunda etapa del proyecto, se requiere llevar a cabo una prueba específica de deserialización insegura en una página web determinada, proporcionada dentro del contenido de la descripción de esta segunda actividad. La deserialización insegura es una vulnerabilidad que ocurre cuando datos no confiables son deserializados, permitiendo a un atacante ejecutar código malicioso o manipular la lógica de la aplicación. Siendo esto una vulnerabilidad altamente peligrosa, pues al ejecutar código malicioso sin darnos cuenta podríamos estar compartiendo nuestros datos con infinidad de personas malintencionadas. Y todo esto sin nuestra autorización, dando lugar a extorciones o suplantaciones de identidad.

Descripción.

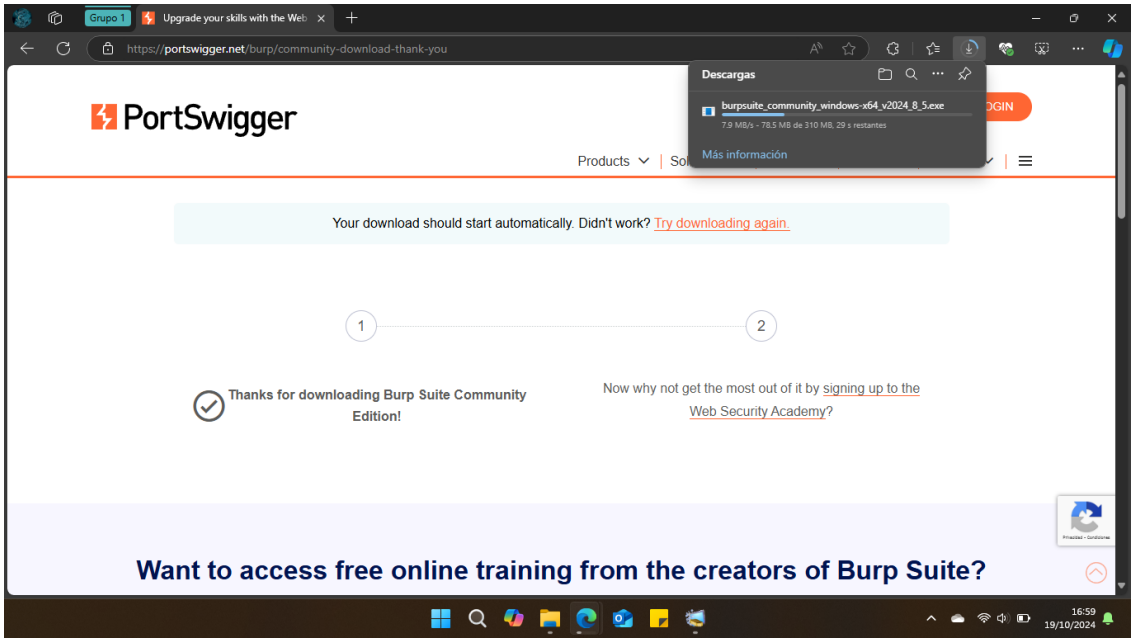
En este caso, la prueba se centrará en el uso de cookies como vector de ataque. Las cookies son pequeños fragmentos de datos que los sitios web almacenan en el navegador del usuario para mantener el estado de la sesión y otras informaciones relevantes. Para llevar a cabo esta prueba, se utilizará Burp Suite Community Edition, una herramienta ampliamente reconocida en el ámbito de la seguridad informática. Burp Suite permite a los profesionales de seguridad realizar pruebas de penetración y análisis de aplicaciones web de manera eficiente. El objetivo de esta prueba es iniciar sesión en la página web como un usuario normal y, mediante la manipulación de las cookies, escalar privilegios para acceder al modo administrador. El proceso comenzará con la identificación de las cookies relevantes que se generan al iniciar sesión como un usuario estándar. Luego, se analizarán estas cookies para detectar posibles puntos de deserialización insegura. Utilizando las funcionalidades de Burp Suite, se intentará modificar las cookies de manera que se obtengan privilegios de administrador. Este tipo de prueba es crucial para asegurar que las aplicaciones web implementen correctamente las medidas de seguridad necesarias para proteger los datos y la integridad del sistema.

Justificación.

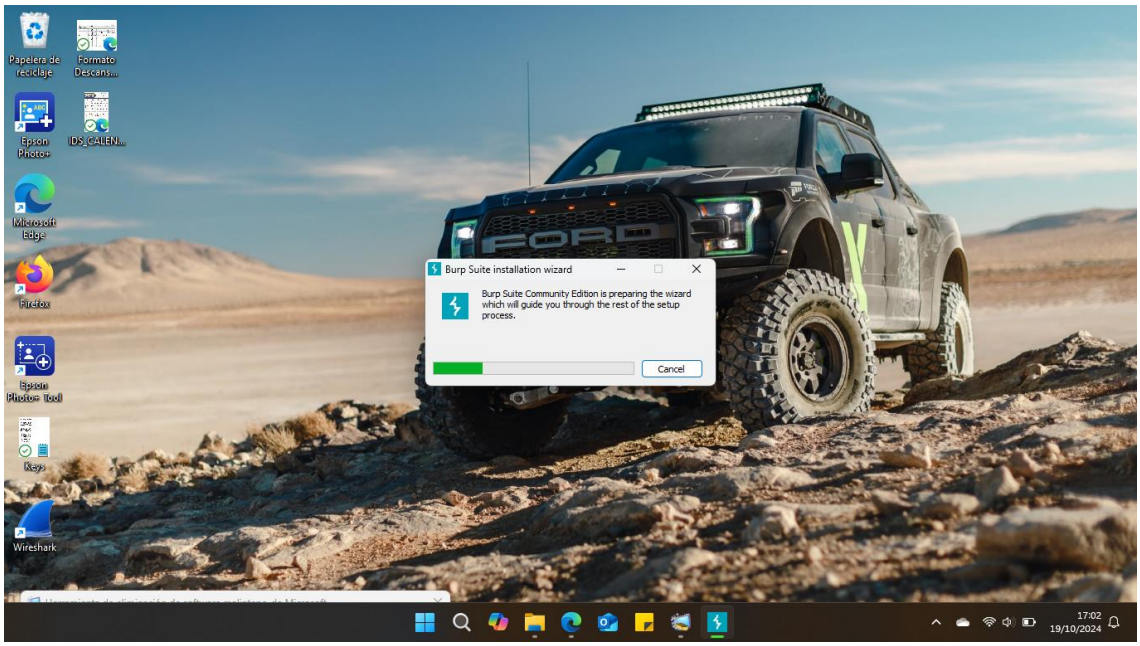
Realizar pruebas controladas de deserialización insegura en páginas web es crucial para garantizar la seguridad y la integridad de las aplicaciones. La deserialización insegura es una vulnerabilidad que ocurre cuando una aplicación deserializa datos manipulados por un atacante, lo que puede llevar a la ejecución de código malicioso, ataques de denegación de servicio (DoS) y la omisión de autenticaciones. Primero, estas pruebas permiten identificar y mitigar riesgos antes de que los atacantes puedan explotarlos. Al simular ataques controlados, los desarrolladores pueden descubrir puntos débiles en el proceso de deserialización y aplicar medidas de seguridad adecuadas, como la validación de datos y el uso de firmas digitales para verificar la integridad de los objetos serializados. Además, estas pruebas fomentan una cultura de seguridad dentro del equipo de desarrollo. Al estar conscientes de los peligros de la deserialización insegura, los desarrolladores pueden adoptar prácticas de codificación más seguras y estar mejor preparados para enfrentar posibles amenazas.

Desarrollo.

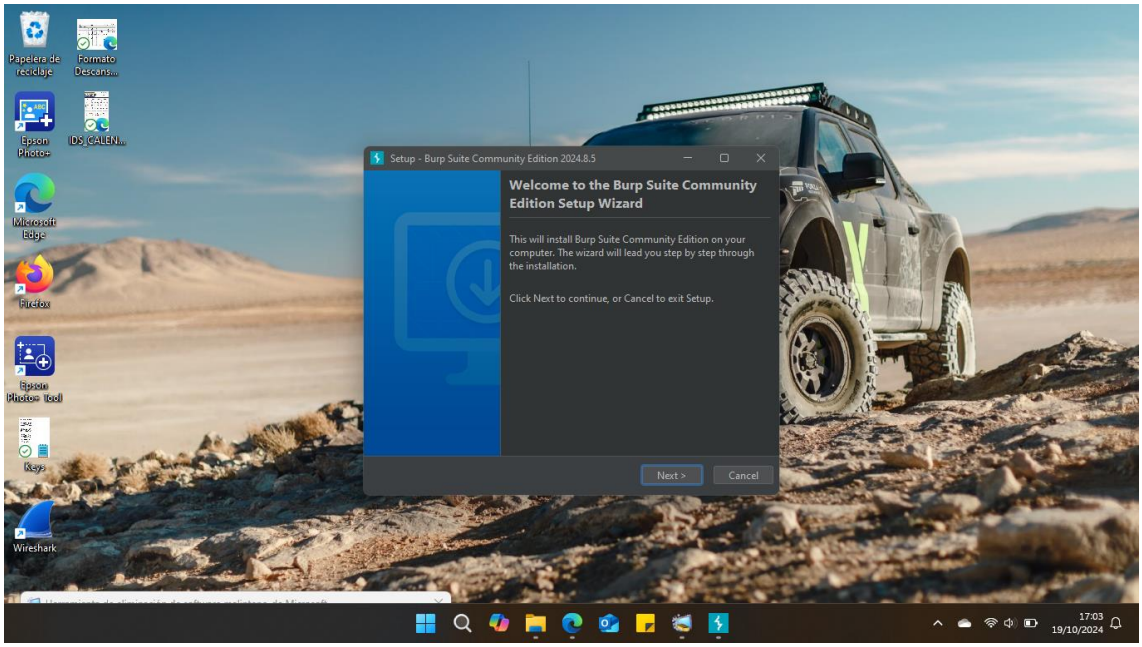
Antes que todo tenemos que instalar los programas que hemos de necesitar, en este caso Burp Suite Community Edition.



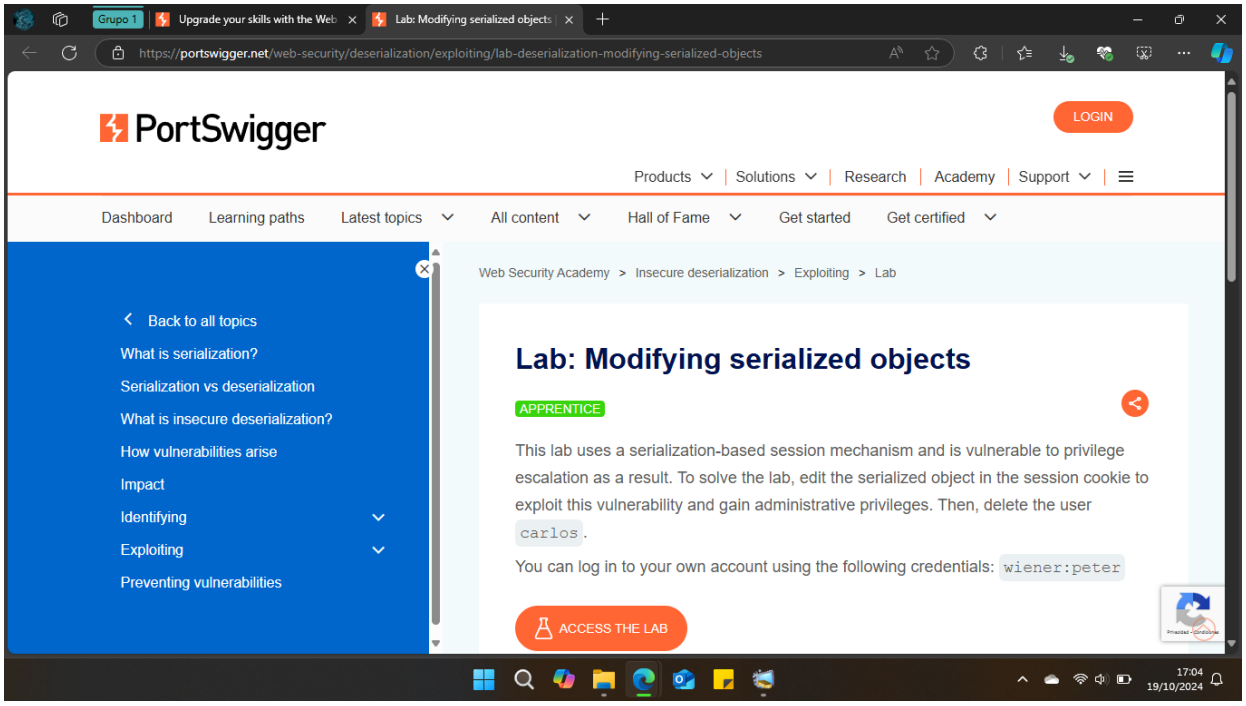
Para ello tenemos que ir al sitio oficial de la aplicación y descargar el instalador directamente en nuestro equipo.



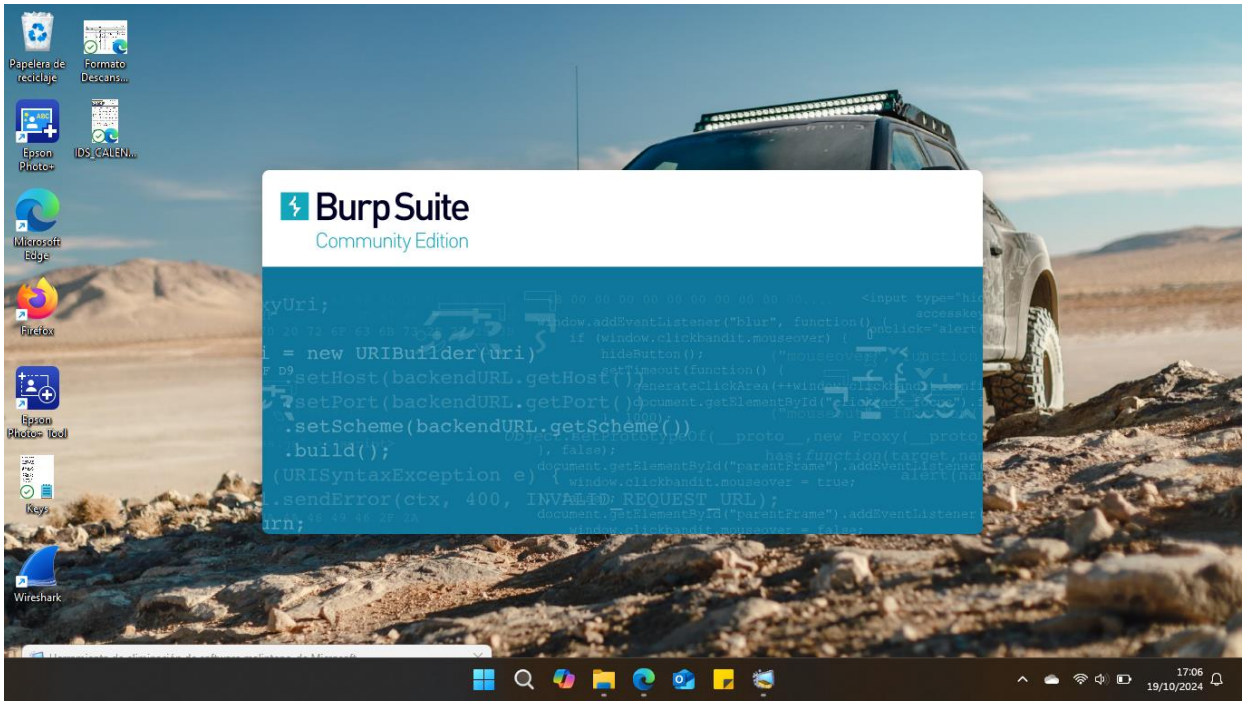
Una vez descargado el instalador procedemos a ejecutarlo, de preferencia con derechos de administrador para que no se genere ningún error por permisos para la aplicación.



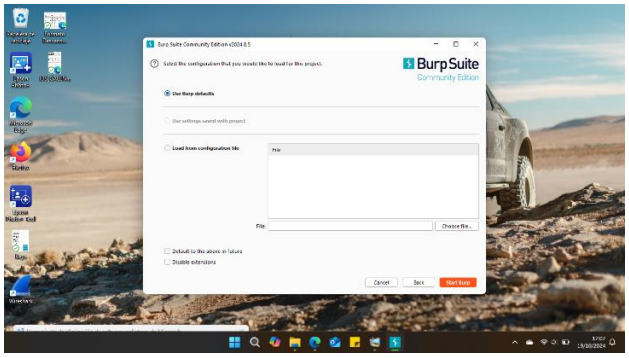
Ahora solo queda seguir los pasos del instalador para tener instalado el programa correctamente, el proceso es sumamente sencillo, realimente no hay que mover nada, solo dejarlo tal como viene por defecto.

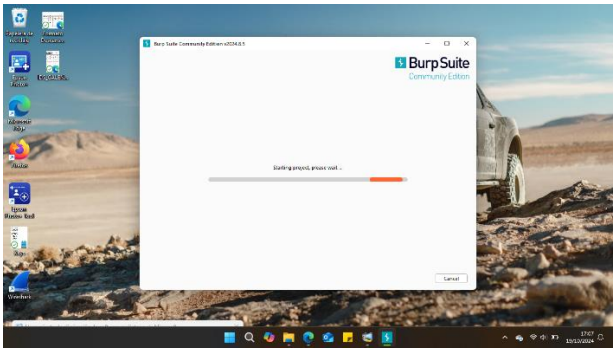


Mientras finaliza el proceso de instalación de nuestra aplicación podemos ir avanzando con el proceso de registro en la pagina de PortSwigger, esto para que nos permita realizar la prueba de deserialización que nos ofrece.



Procedemos a abrir nuestra aplicación de Burp Suite para poder crear un nuevo proyecto, tal como se muestra en las capturas de a continuación.

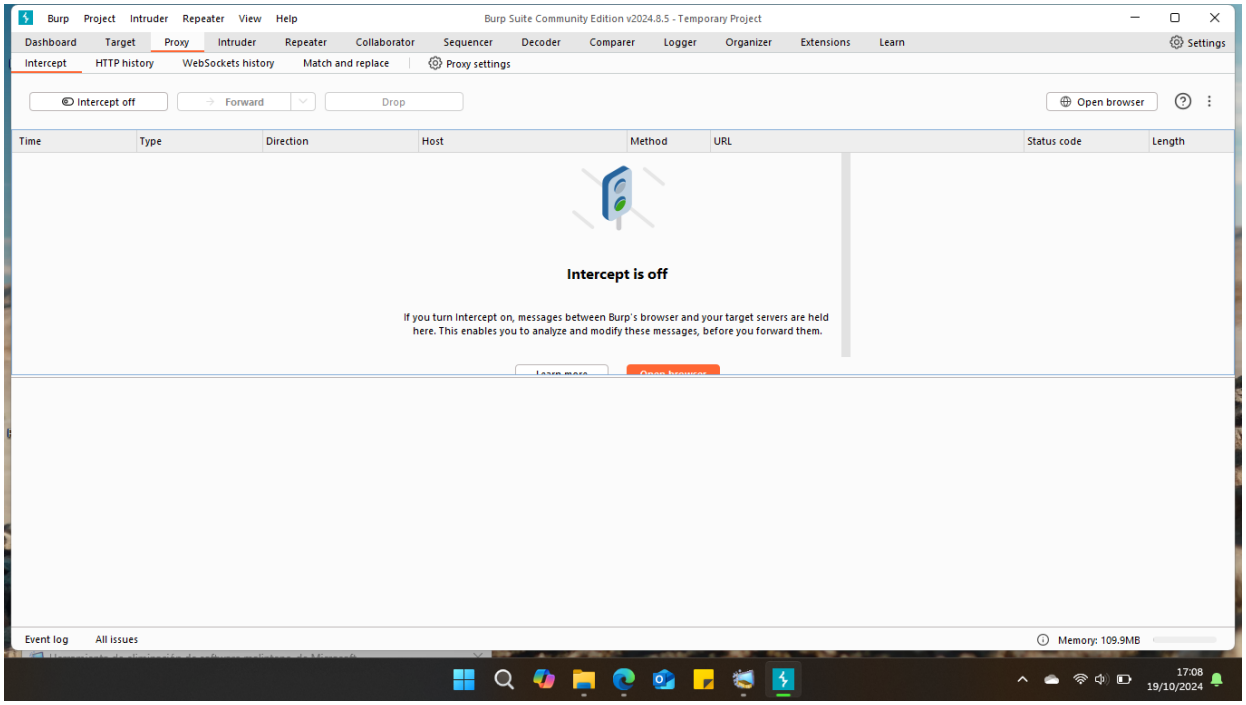




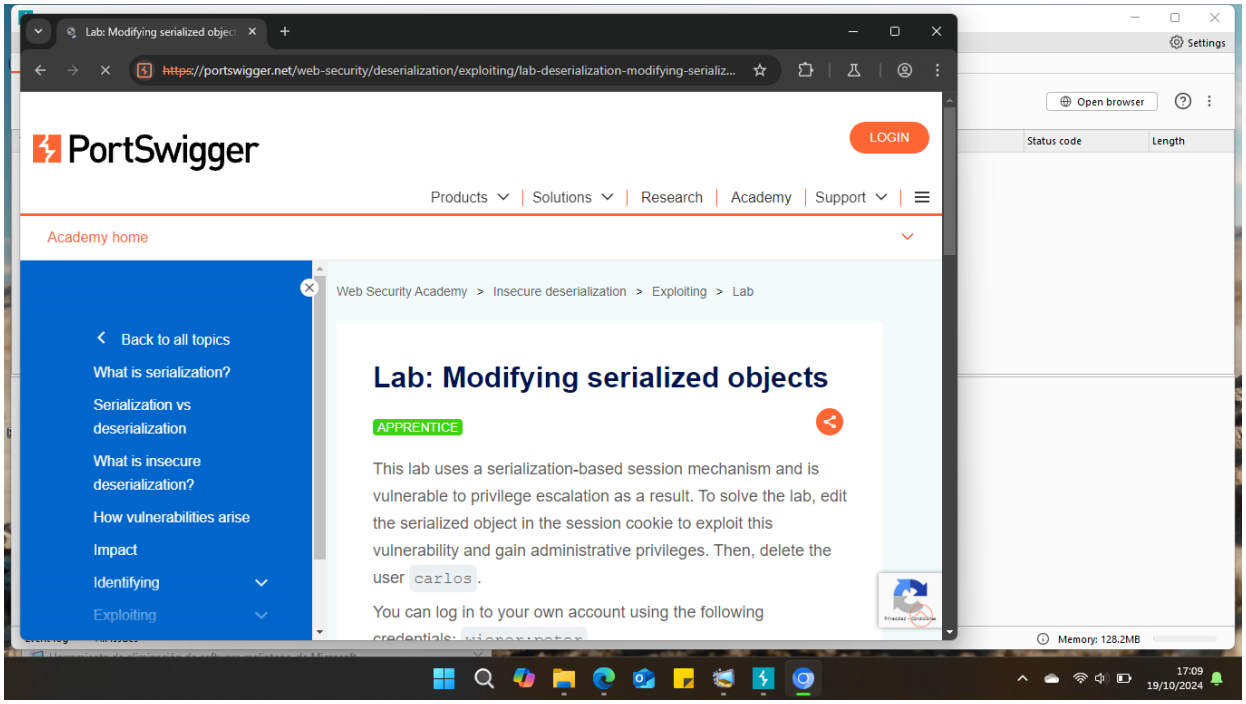
El proceso para crear un nuevo proyecto dentro de esta aplicación es sumamente sencillo, ya que de hecho solo dejaremos las opciones justo como están seleccionadas por defecto. Estas son las indicaciones que nos brinda la guía de la actividad proporcionada por la academia.

Ataque al sitio.

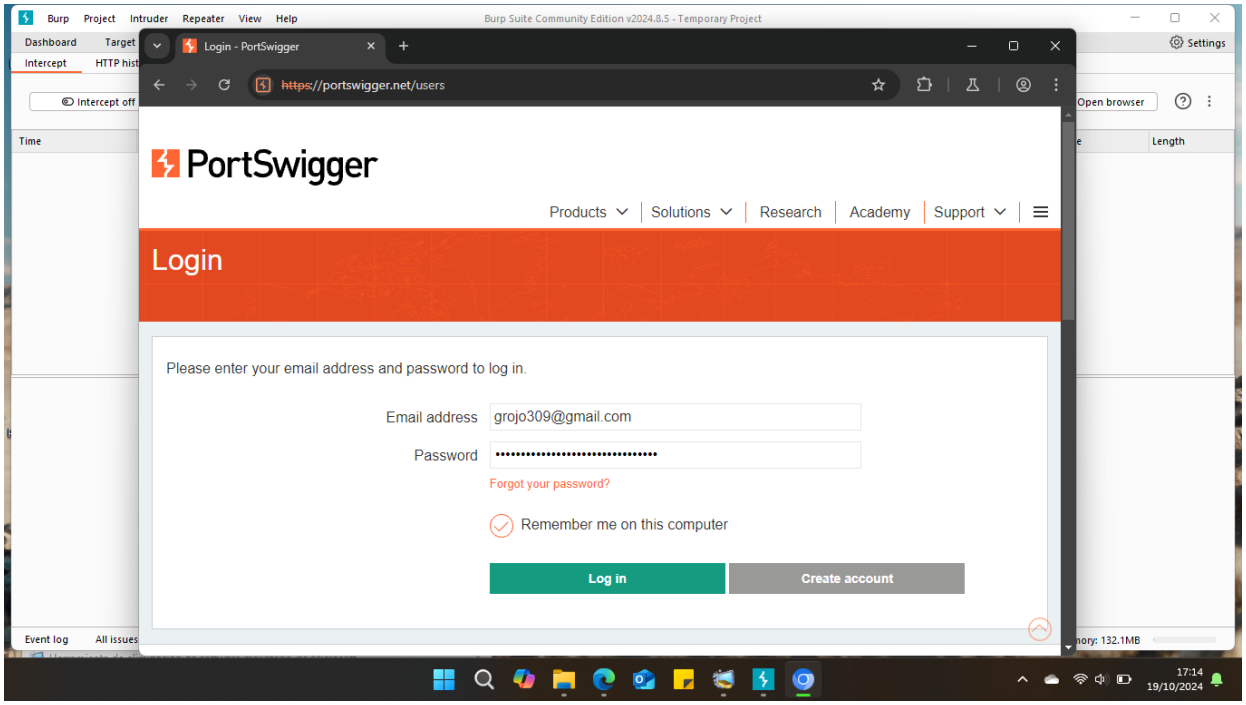
Pues bien, ha llegado el momento de comenzar con la preparación para el ataque al sitio que se nos solicita, como ya se menciono dentro de la descripción de esta actividad, ingresaremos a un sitio de pruebas con el usuario y la contraseña que la misma pagina nos proporciona, una vez registrados interceptaremos la comunicación entre la página y el servidor con ayuda de Burp con el fin de modificar la cookie que contiene nuestra información de usuario y con esto darnos los privilegios de administrador. Para poder confirmar que tenemos los derechos eliminaremos un usuario ya existente dentro de la base de datos de la página.



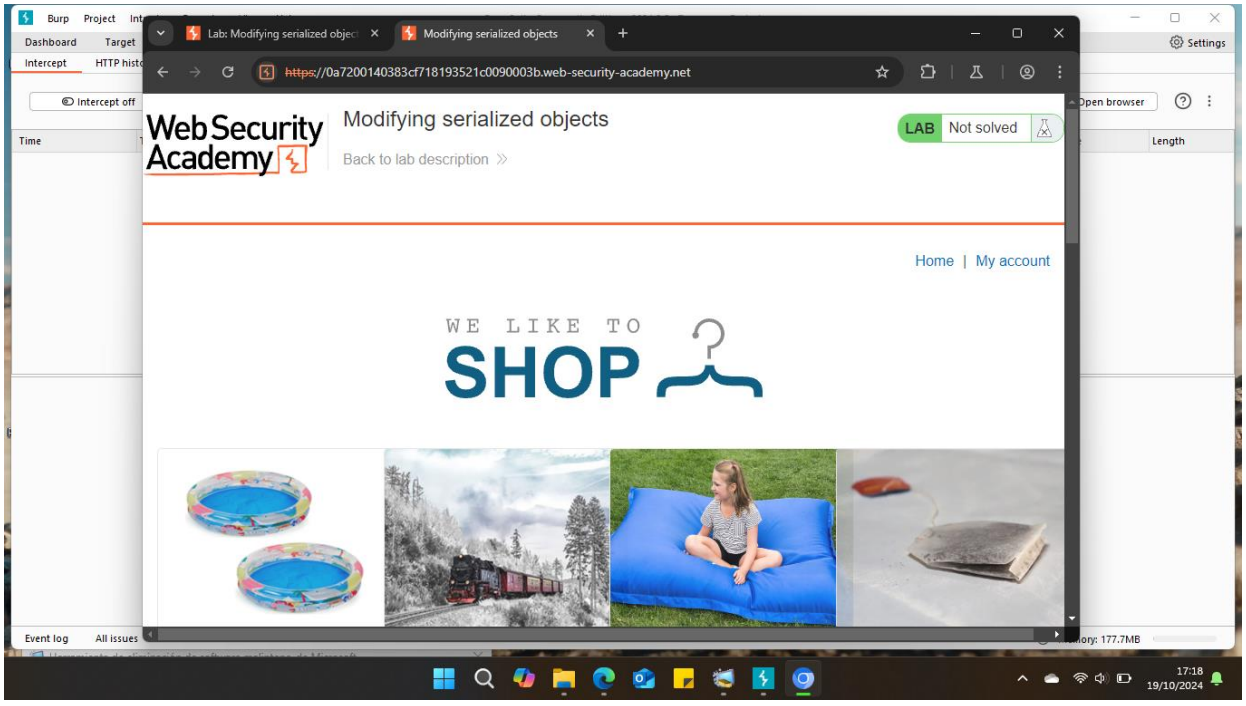
Noa dirigimos a la pestaña de “Proxi” y desde aquí daremos clic en el botón resaltado en color naranja, lo que abrirá una pestaña del navegador integrado de la aplicación,



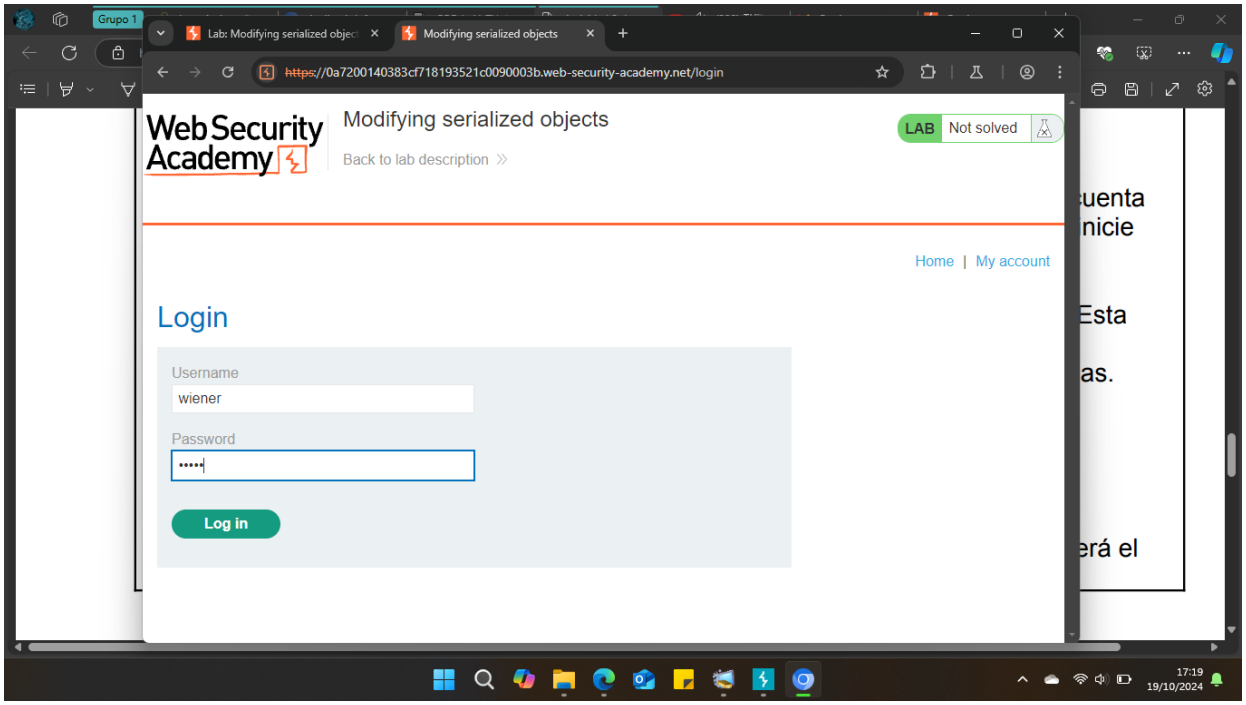
Dentro de esta nueva pestaña colocaremos la dirección URL del proyecto de deserialización, esta dirección es la que obtuvimos después de nuestro registro en la página de PortSwigger.



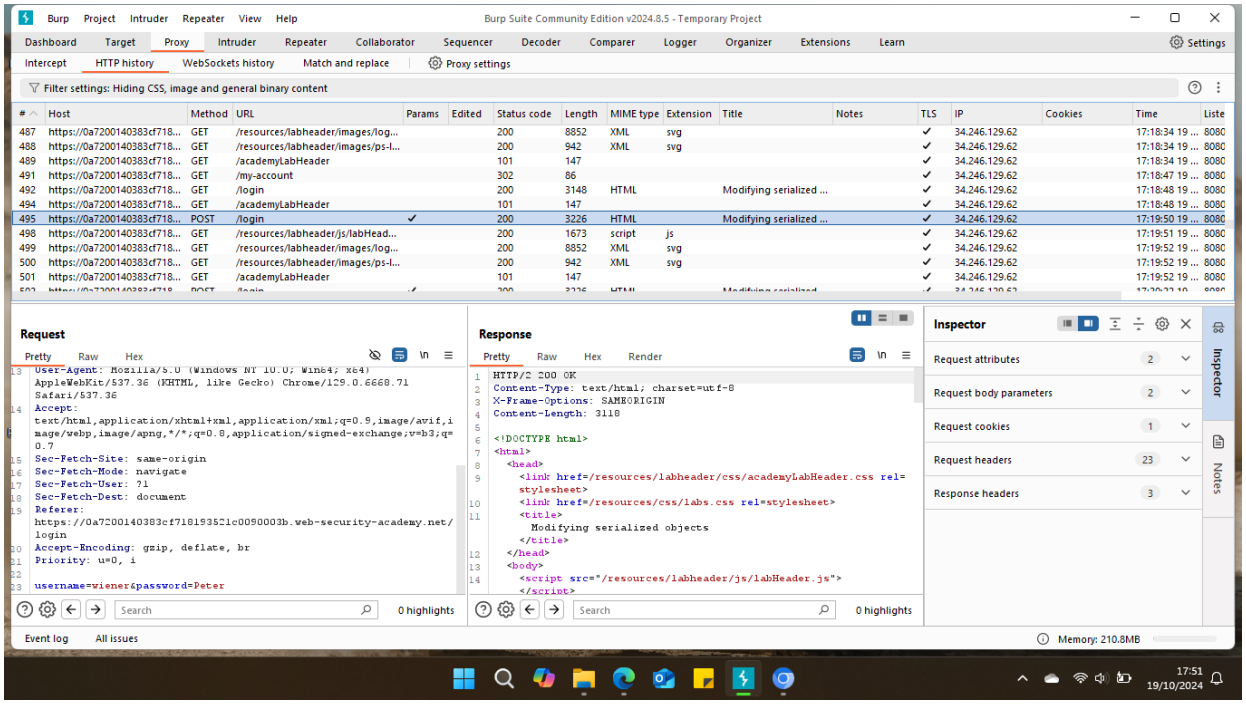
Entonces procedemos a iniciar sesión con nuestras credenciales que obtuvimos en el registro, esto para que nos permita realizar el proyecto de deserialización, ya que, si no nos registramos dentro de este nuevo navegador, simplemente no nos permitirá realizar la prueba.



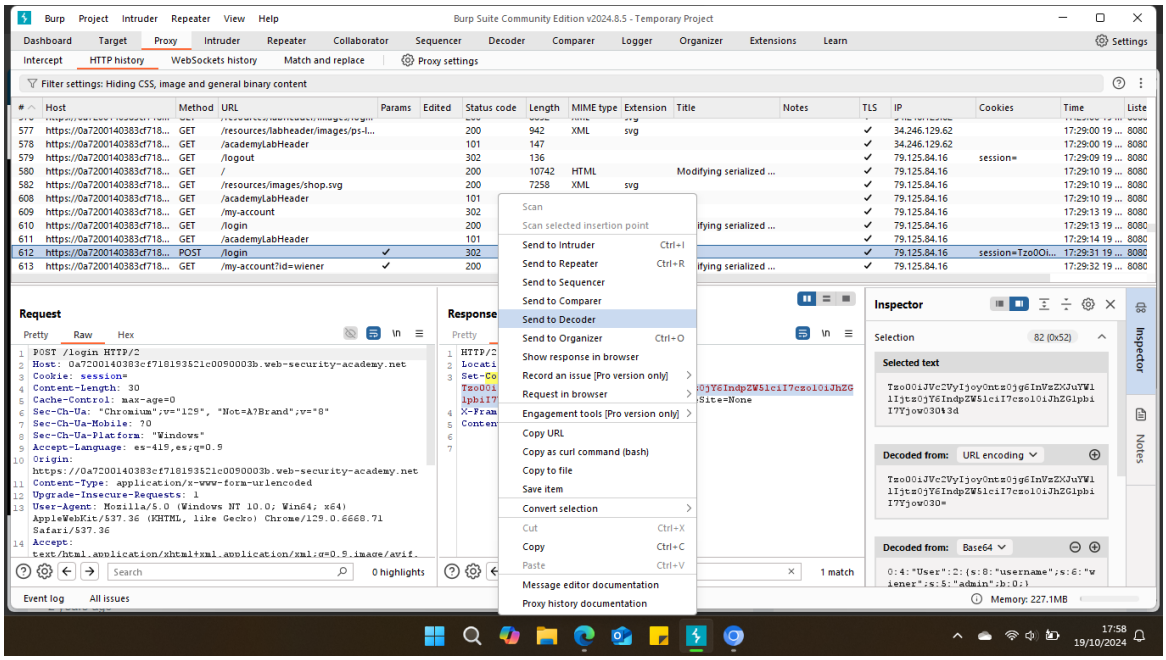
Ahora tenemos esta nueva pantalla, es qui donde hemos de comenzar con nuestro proceso de ataque, lo que debemos hacer en esta nueva pestaña es registrarnos con los datos que nos proporciona la descripción de la práctica, para esto damos clic en “my Account”.



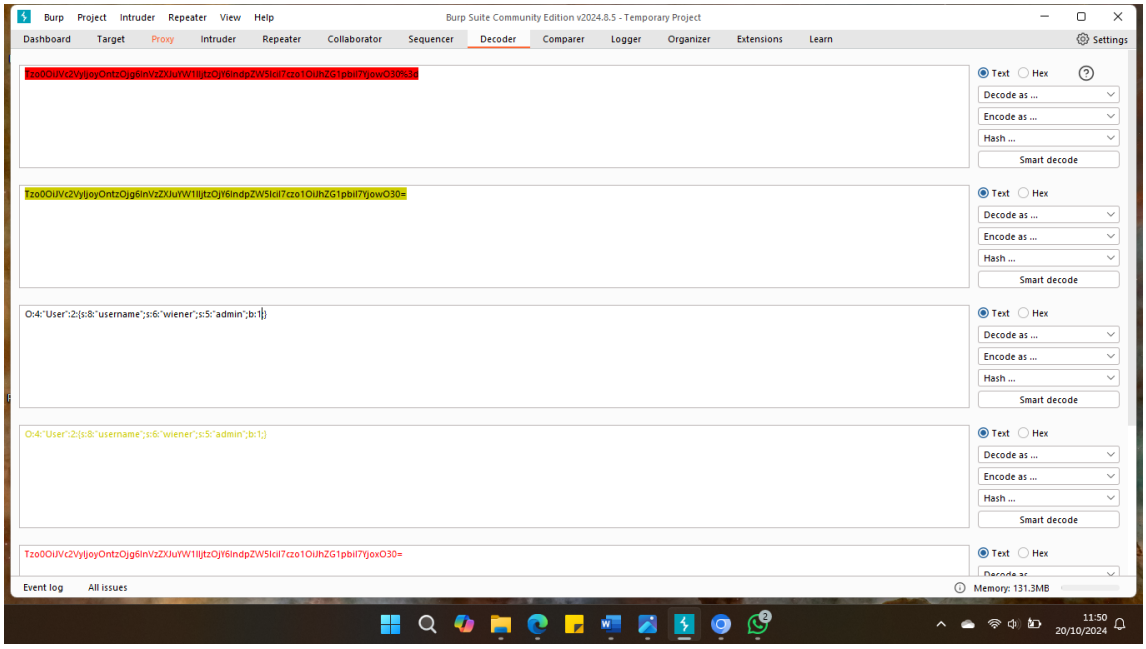
Nos envía a esta nueva pestaña en donde colocamos el usuario y la contraseña que se nos proporcionan en la descripción de la actividad. Usuario: Wiener, Contraseña: Peter.



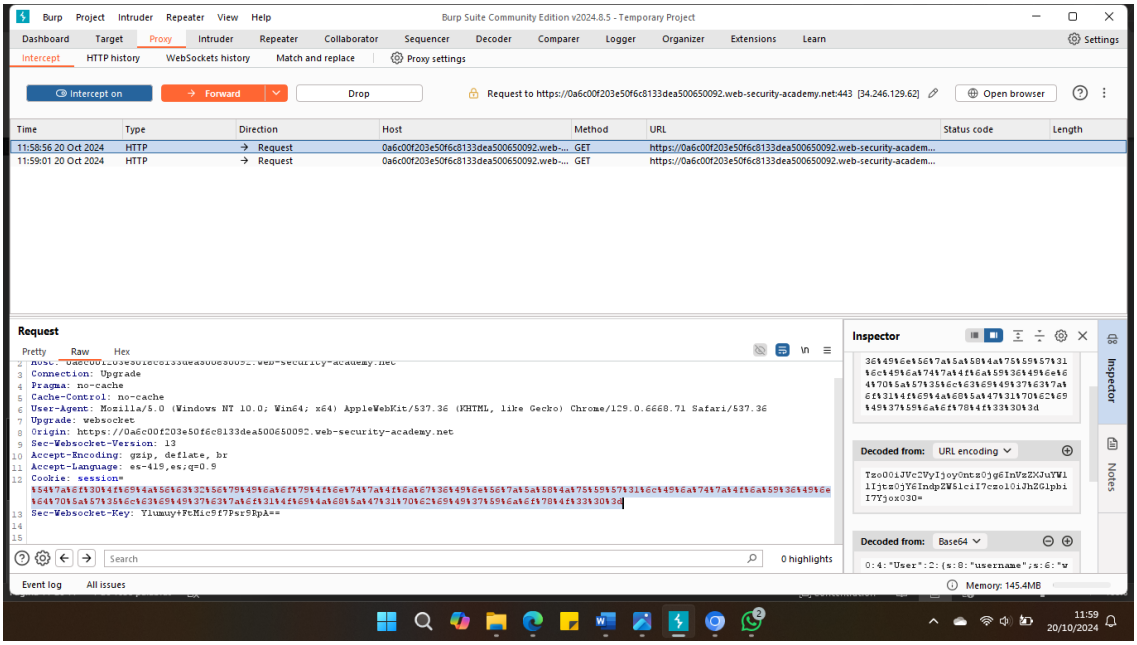
Una vez que damos clic a log in se genera un evento que se registra dentro del historial de HTTP, esto dentro de nuestra aplicación de Burp. Es aquí donde buscaremos el evento que contiene la cookie de nuestro inicio de sesión, entonces la seleccionaremos y editaremos con el fin de obtener permisos de administrados con la cuenta básica que hemos ingresado.



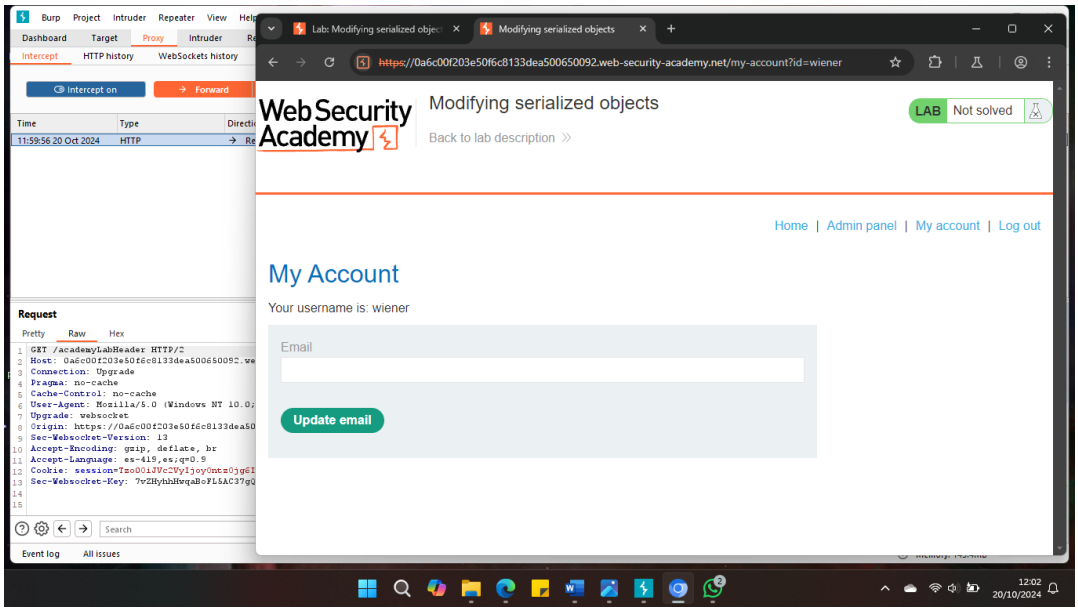
Seleccionamos la cookie que contiene la información de nuestro inicio de sesión, evento que ha quedado registrado justo después de iniciar sesión dentro de la página de la prueba. Compartimos la cookie con el decodificador que viene integrado dentro de la misma herramienta de Burp.



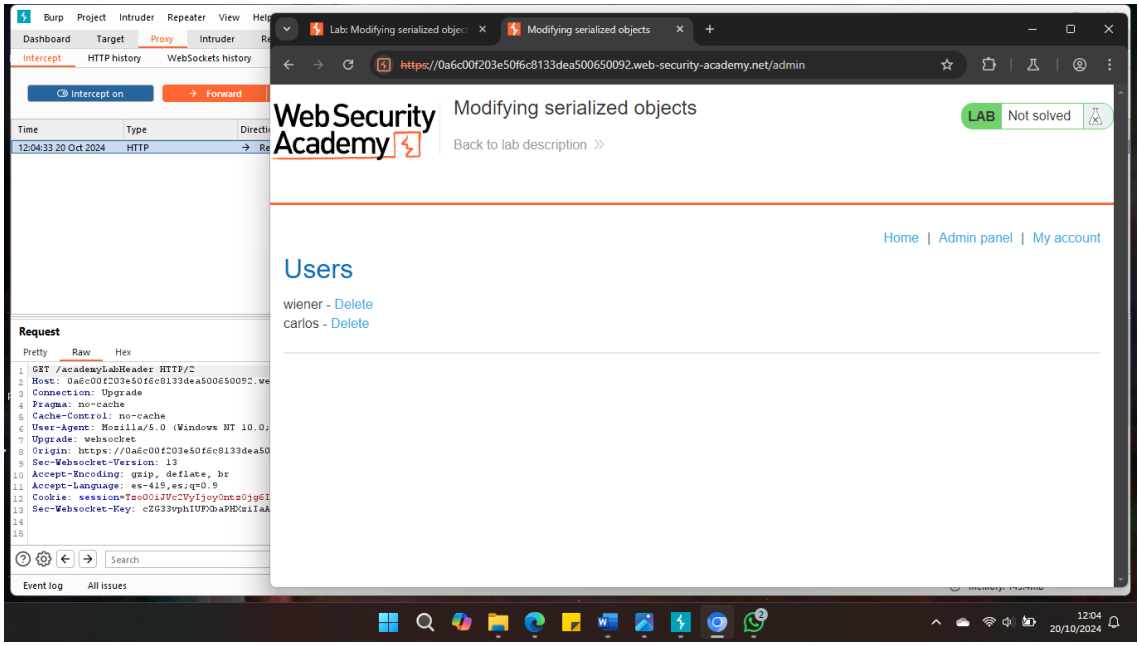
Dentro de esta nueva pestaña lo que haremos es decodificar la cookie que acabamos de copiar, primeramente, la decodificaremos en URL, posterior a esto se decodifica en base 64 y se modificara a manera de obtener los permisos de administrador. Una vez modificada codificaremos nuevamente a la inversa, es decir, primero la codificamos en base 64 y de ahí la codificamos en URL.



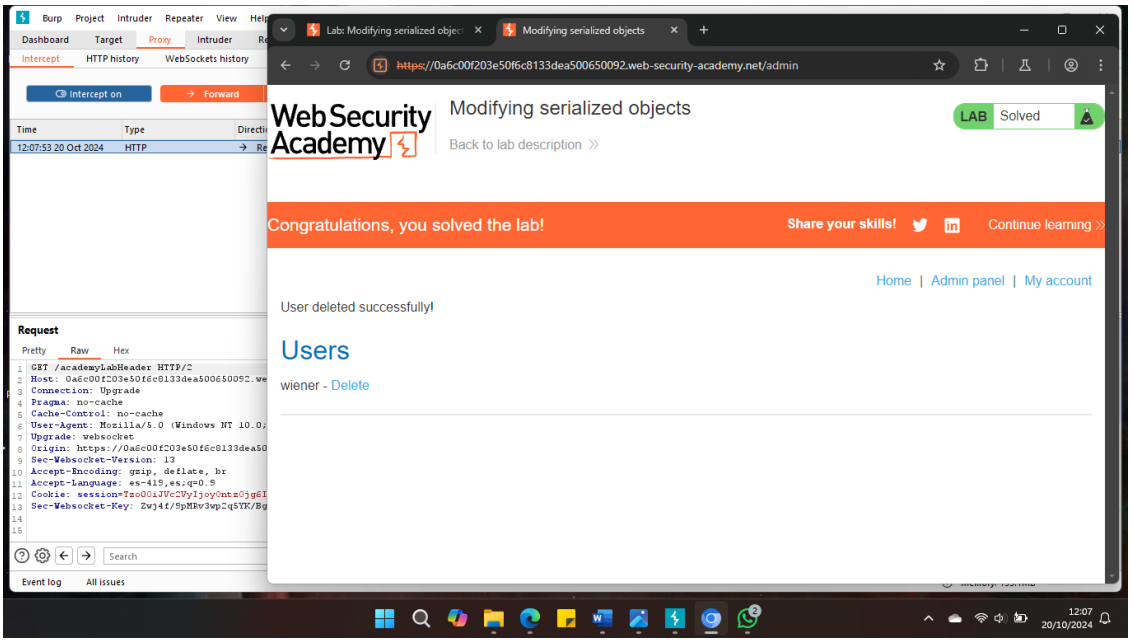
Lo que sigue es encender el interruptor de interceptor, seguido de esto recargamos la pagina del navegador para que se vuelva a generar un evento que nos proporcione la cookie, es aquí donde reemplazaremos la cookie original por la que hemos editado en el decodificador.



Ahora dentro de nuestro navegador las opciones han cambiado, pues ahora tenemos permisos de administrador, entraremos a este nuevo menú para poder eliminar al usuario que se nos solicita.



Cada que demos un clic dentro de las opciones del navegador tendremos que repetir el proceso de reemplazar la cookie que se genera, pues recordemos que el usuario con el que ingresamos no tiene permisos administrativos, y es ahí donde entra el papel del Interceptor.



Eliminamos entonces al usuario que se nos solicita, y como se menciona, cada que seleccionemos una de las opciones dentro del navegador que necesite permisos de administrador tendremos que sustituir la cookie que se genera por la que hemos editado en el Decoder para otorgarnos los permisos correspondientes. Y como lo muestra la captura anterior, hemos eliminado correctamente el usuario que se nos solicita y ahora el indicador en la parte superior derecha ha cambiado a “Solved”. Lo que significa que la practica ha finalizado exitosamente.

Conclusión.

La realización de pruebas de deserialización insegura utilizando Burp Suite Community Edition es una práctica esencial para identificar y mitigar vulnerabilidades en aplicaciones web. Burp Suite, una herramienta ampliamente utilizada en la seguridad informática, permite a los evaluadores de penetración y profesionales de la seguridad realizar pruebas exhaustivas de deserialización insegura mediante su conjunto de herramientas manuales. Estas pruebas son cruciales para garantizar la seguridad de las aplicaciones web. Esta herramienta permite a los profesionales de la seguridad identificar y explotar posibles vulnerabilidades de deserialización, que pueden ser utilizadas por atacantes para ejecutar código malicioso o acceder a datos sensibles. A través de la configuración adecuada y el uso de herramientas como el Repeater y el Intruder, los evaluadores pueden simular ataques y analizar las respuestas del servidor para detectar comportamientos anómalos. La capacidad de Burp Suite para personalizar y automatizar ciertos aspectos del proceso de prueba también mejora la eficiencia y efectividad de las evaluaciones de seguridad.

Referencias.

Cantelli, F., & Cantelli, F. (2024, 14 agosto). Qué es Insecure Deserialization y cómo prevenirla. Hackmetrix Blog. https://blog.hackmetrix.com/insecure-deserialization/

Rivera, D. (2021, 5 diciembre). Riesgo A8 en OWASP - Deserialización insegura. pleets. https://blog.pleets.org/article/es/owasp-a8-insecure-deserialization

Deserialization | HackTricks