Universidad Corporativa Coppel | Programas Académicos

Ingeniería en Desarrollo de Software

Actividad 3 – Cross site scripting (XSS)

Auditoria informática

Ingeniería en Desarrollo de Software

Tutor:

Jessica Hernández Romero

Alumno:

Alejandro Abarca Gerónimo

Fecha:

24 de febrero de 2025

Indice

Introducción

Cuando se trata de violación de datos, las consecuencias son grandes y profundamente impactantes. Estas violaciones se han convertido en problemas de seguridad cibernética, así como pérdidas financieras, daños de reputación, problemas legales, multa regulatoria y la prevención de una profunda confianza del consumidor. A pesar del mayor peso dado a la seguridad de los datos, las personas dedicadas a la información encuentran nuevas formas de dividir para acceder a datos valiosos y datos de acreditación para las empresas. La pérdida de datos puede afectar a los usuarios de Internet de varias maneras, como el robo de identidad, la compensación de identidad y la pérdida financiera.

Robo de identidad

- Los atacantes pueden usar los datos personales robados para realizar compras, abrir cuentas bancarias, o acceder a redes sociales.
- Esto puede causar pérdidas económicas y estrés emocional.

Suplantación de identidad

- Los atacantes pueden crear cuentas en nombre de la víctima para realizar ciberacoso o ciberbullying.
- También pueden generar contenido negativo en nombre de la víctima.

Pérdidas financieras

- Los usuarios pueden sufrir pérdidas económicas si sus datos personales son robados.
- Los usuarios pueden tener que pagar compensaciones a los clientes afectados, investigar la violación, y pagar honorarios legales.

Descripción

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). Para lo cual 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.

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.

Justificación

El ataque de pérdida de autenticación de datos genera graves consecuencias para los usuarios de Internet. Este tipo de ataque se refiere a la situación en la que un atacante gana acceso no autorizado a las credenciales de un usuario (como contraseñas, tokens de sesión, o datos biométricos), lo que puede permitirle acceder a servicios, cuentas y recursos personales.

Las auditorías informáticas son eficaces porque ayudan a evaluar el estado de los sistemas de información de una organización, identificando áreas de mejora y asegurando que los recursos tecnológicos se utilicen de manera eficiente y segura.

Estas son algunas de las principales tareas a realizar en una auditoría informática:

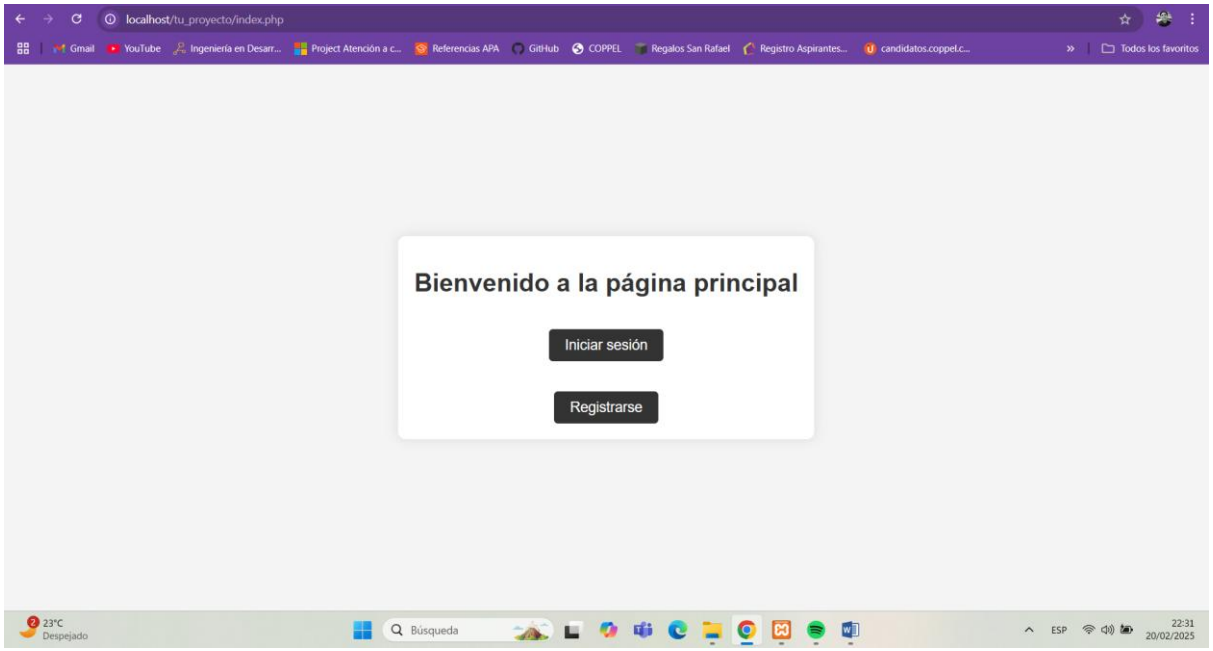
- Seguridad de la información.
- Cumplimiento normativo.
- Riesgos tecnológicos.

- Eficiencia operativa.
- Gestión de cambios.
- Controles internos y procedimientos.
- Planes de contingencia y recuperación.
- Responsabilidades y roles.

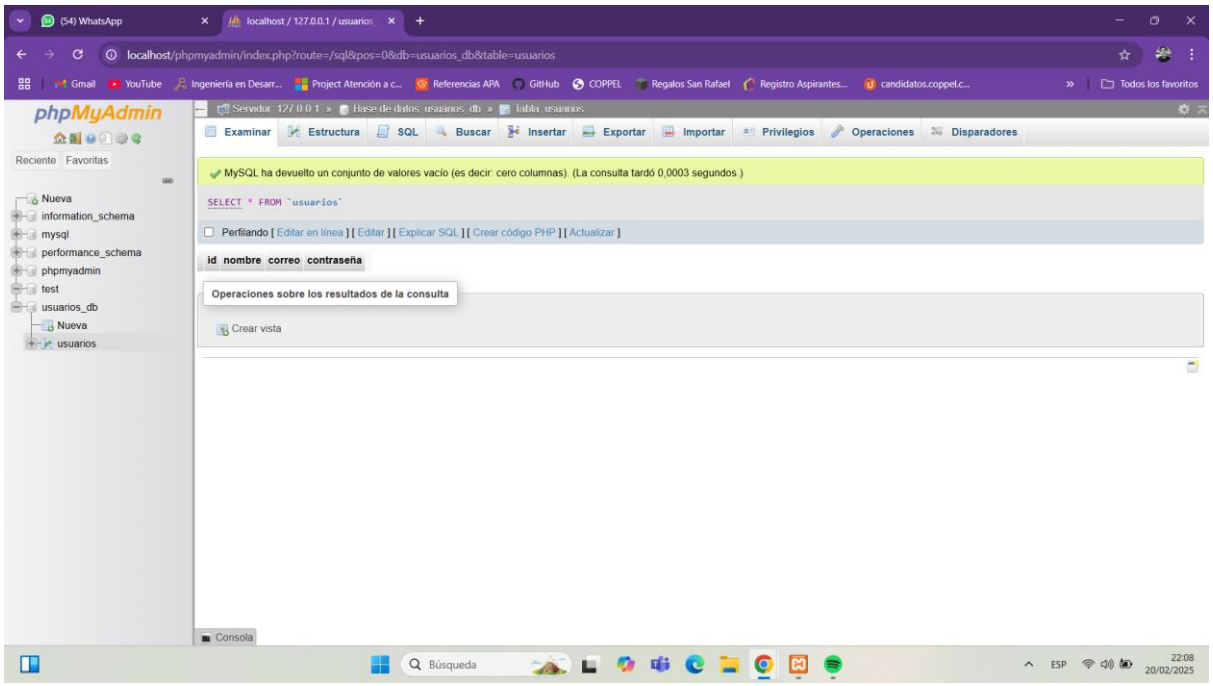
Etapa 1:

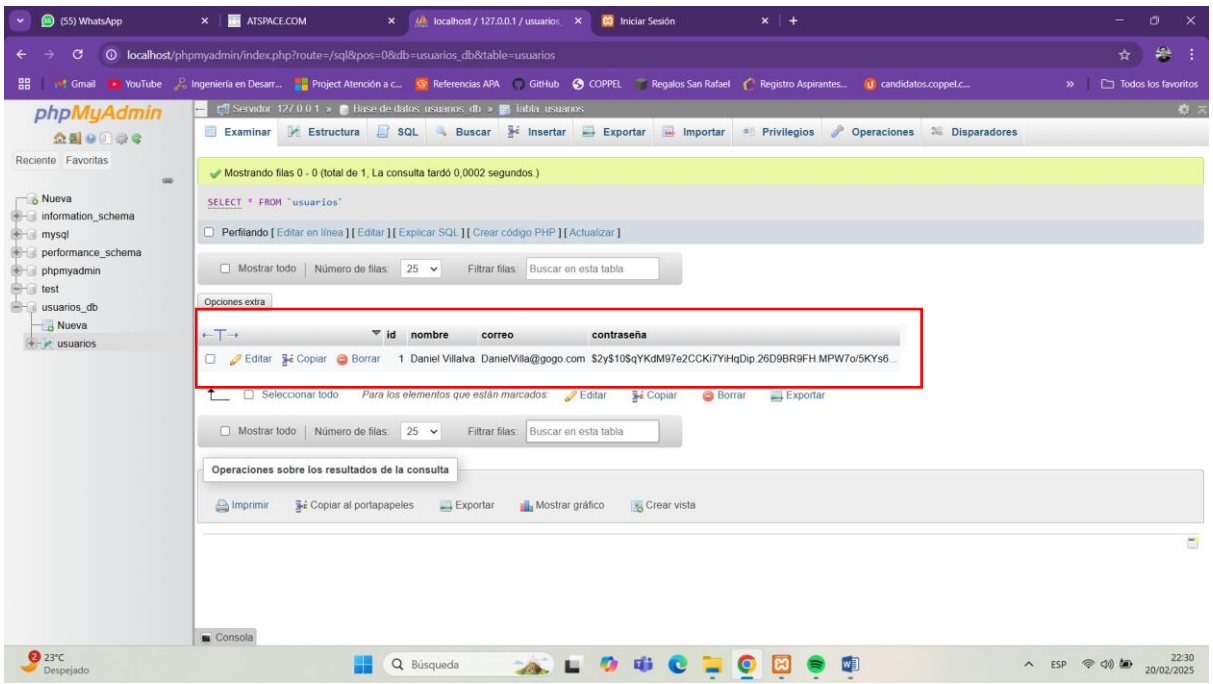
Descripción del sitio web

Desarrollamos una página de acceso para poder realizar registros e ingresar a una plataforma determinada. Con ayuda de herramientas como Xampp para ejecutar una página de forma local y la creación de la BD mediante phpMyAdmin.



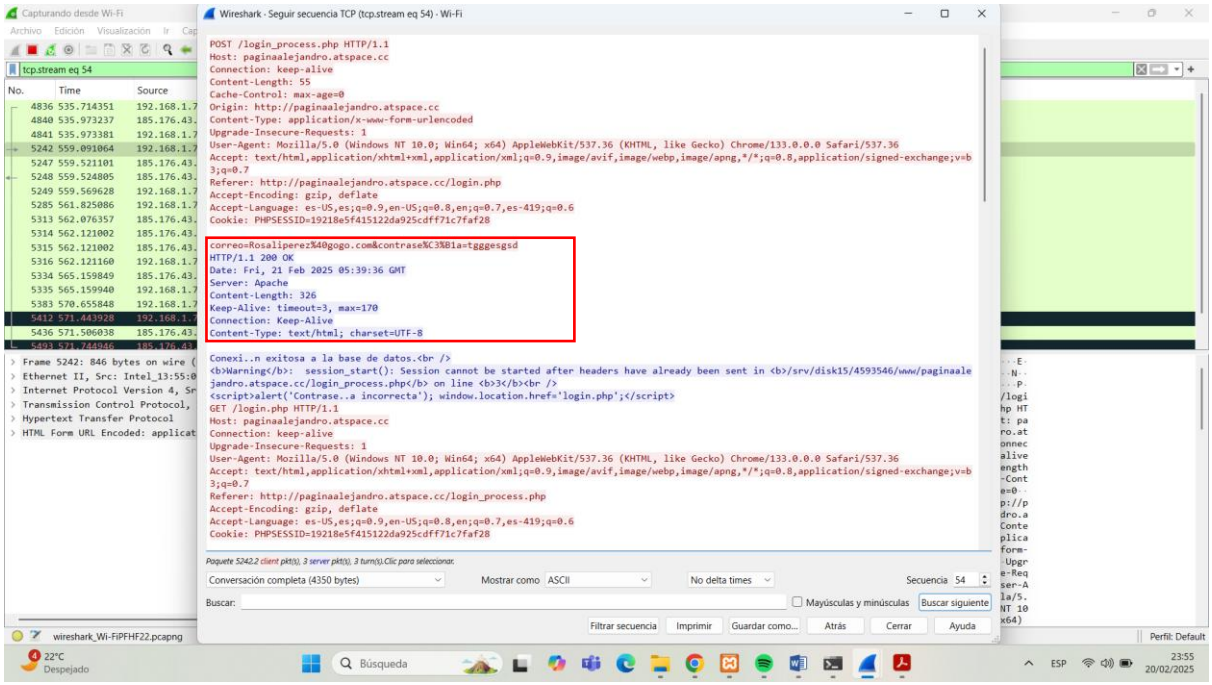
Posterior a esto vinculamos por medio de phpMyAndmin la BD que almacena todas las credenciales de los usuarios una vez que hemos desarrollado dicha BD.





Ataque al sitio

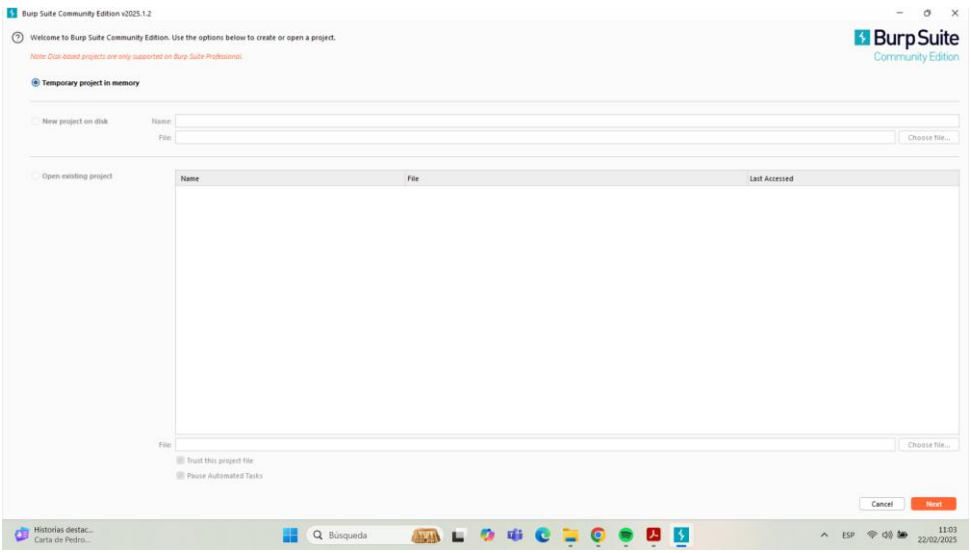
De esta manera realizamos el ataque a dicha página web para extraer las credenciales de los usuarios las cuales se muestran a continuación. Para ello utilizamos **ip.addr == 192.168.1.78 and http**



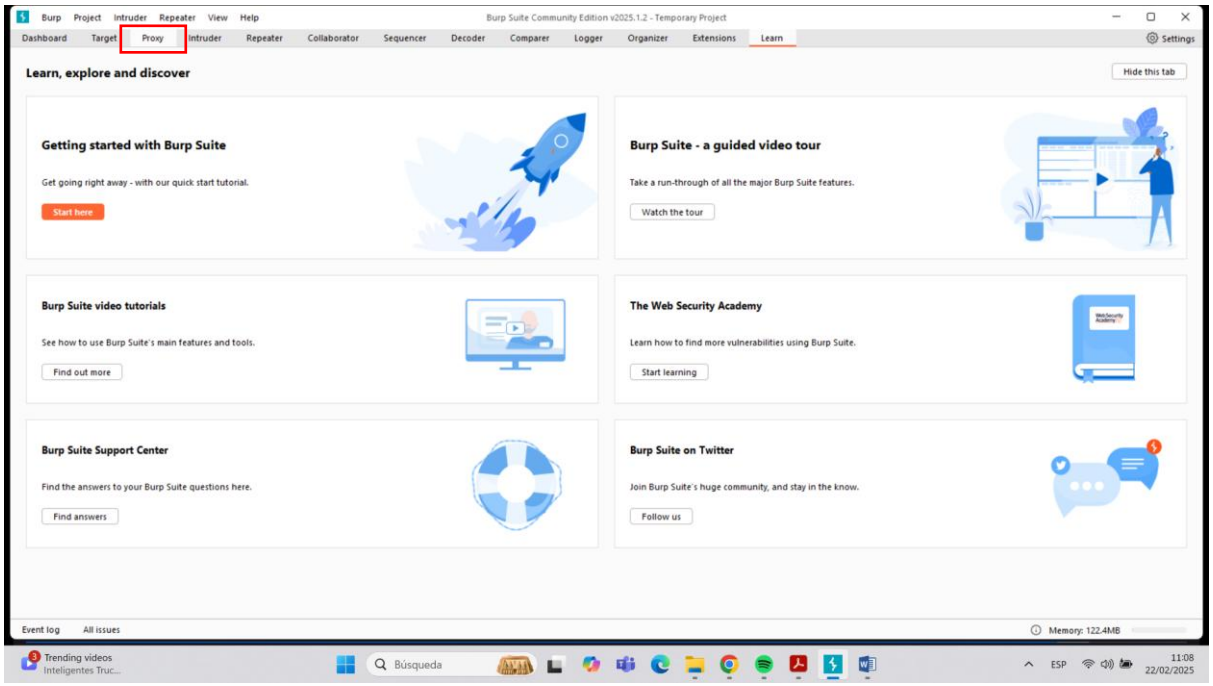
Etapa 2:

Ataque al sitio

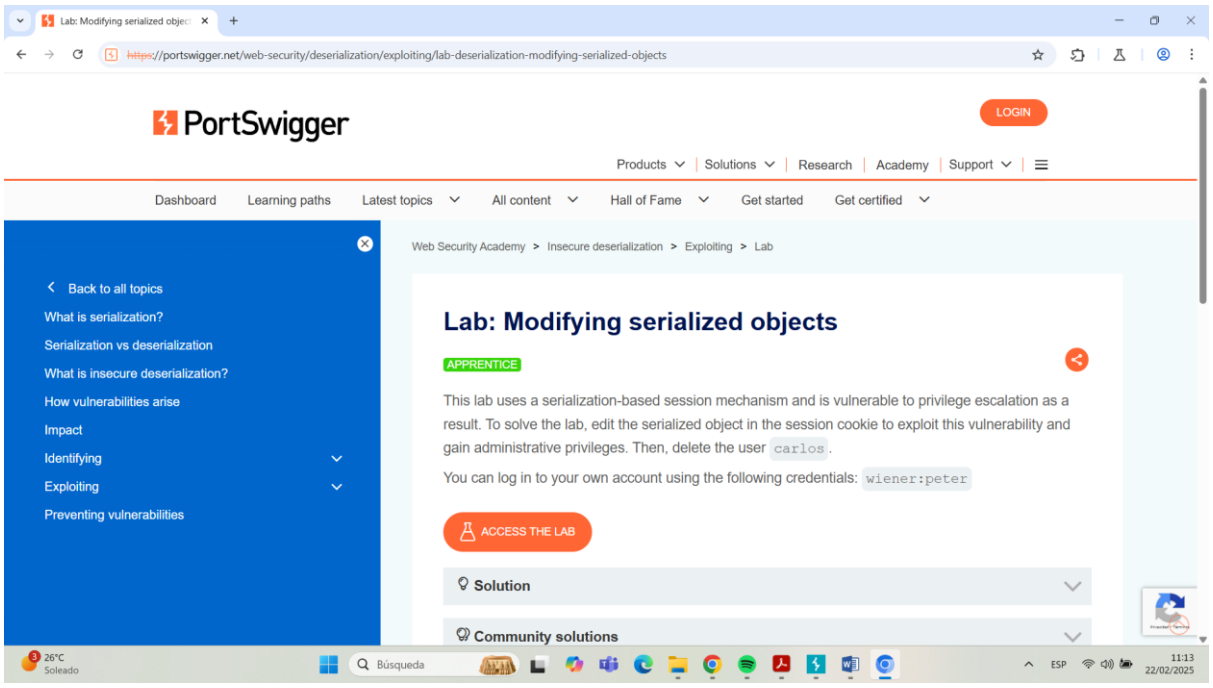
Como primer paso ingresamos al link de descarga proporcionado en el documento de la actividad para descargar la herramienta solicitada y procedimos a realizar la instalación.



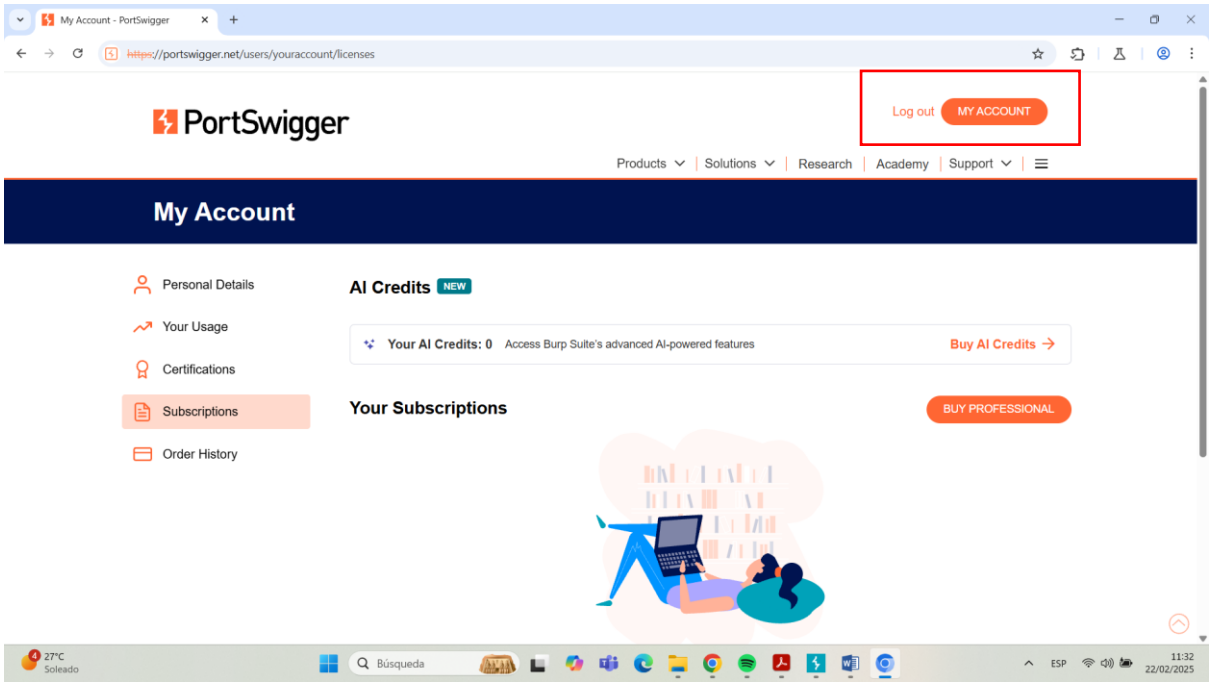
Una vez creado el proyecto y realizar las configuraciones correspondientes se procede a realizar el proceso que se solicita en la actividad ingresando a la pestaña PROXY.



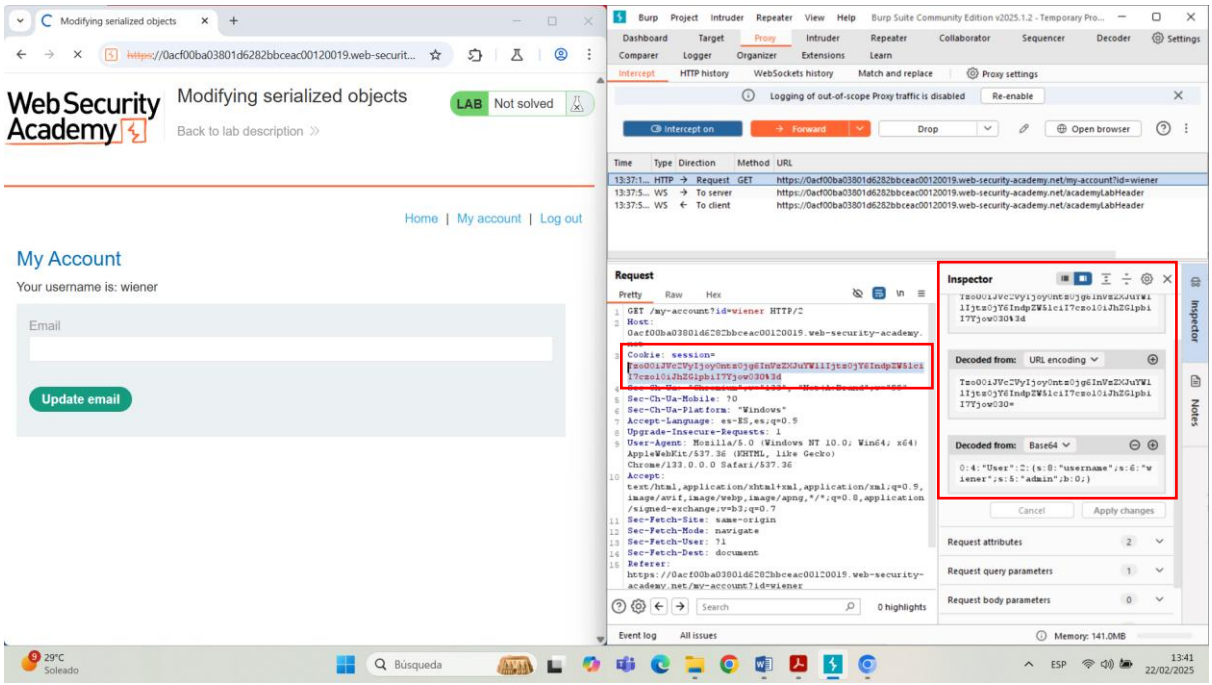
Después de haber ingresado a la pestaña antes mencionada, procedemos a abrir el Browser el cual es el navegador de la herramienta a utilizar y colocamos el link del laboratorio para trabajar dentro de este navegador.



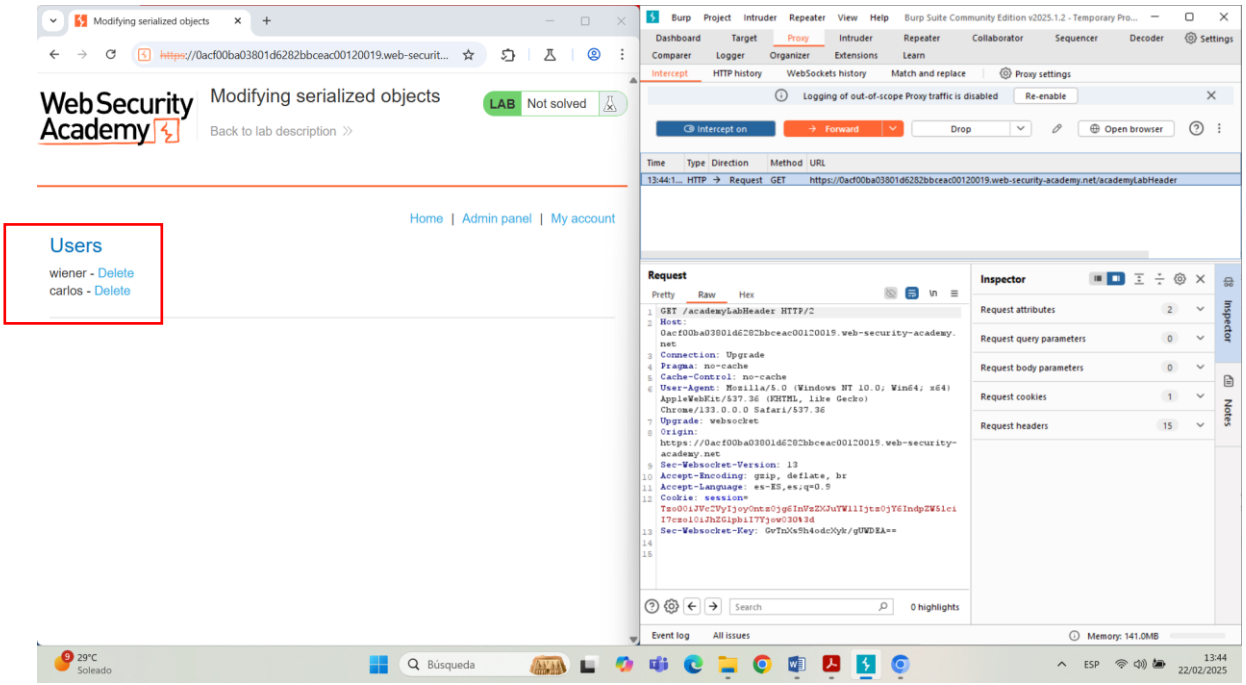
Una vez que ingresamos a la cuenta creada con anterioridad durante la descarga de Burp Suite, ingresamos al apartado MY ACCOUNT para ingresar las credenciales proporcionadas en el archivo de la actividad.



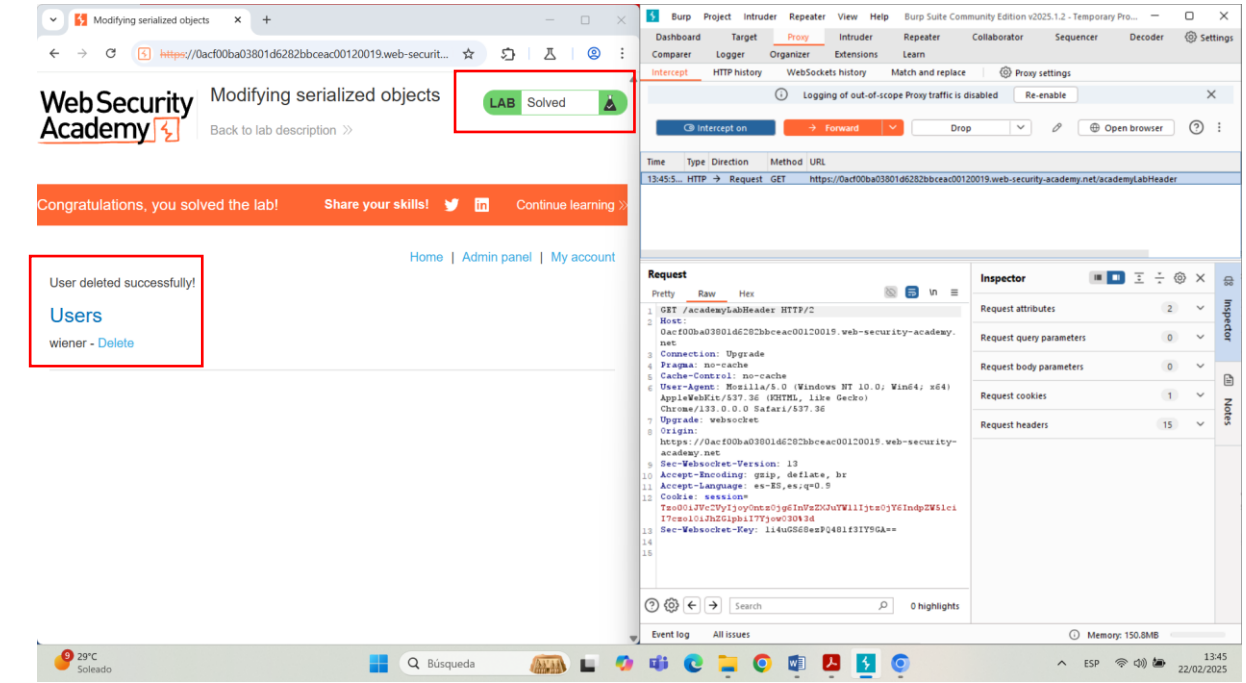
Una vez que ingresamos a la cuenta proporcionada encendemos el **Intercept on** para poder visualizar la cookie, seleccionamos y visualizamos en el apartado inspector para poder habilitar el modo admin. con valor de 1.



Una vez realizado dicho cambio de valor y pasar a tener derechos de administrador podemos visualizar los usuarios, en este caso el que tenemos que borrar es el usuario **Carlos.** Damos clic en **Delete** y nuevamente seleccionamos la cookie para modificar el valor de 0 a 1 y demostrar que somos **admin.**



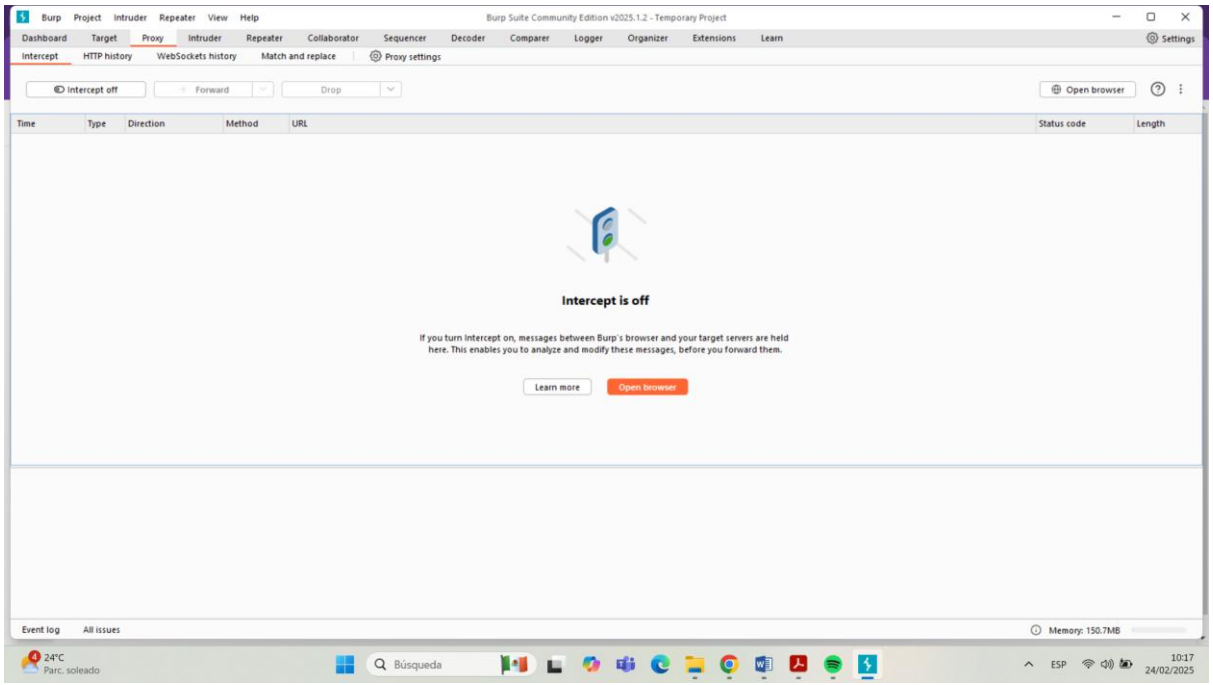
En la siguiente pantalla se muestra el ejercicio resuelto con la cuenta de **Carlos** eliminada, sólo queda el usuario **wiener**, usuario del cual se nos proporcionaron las credenciales.



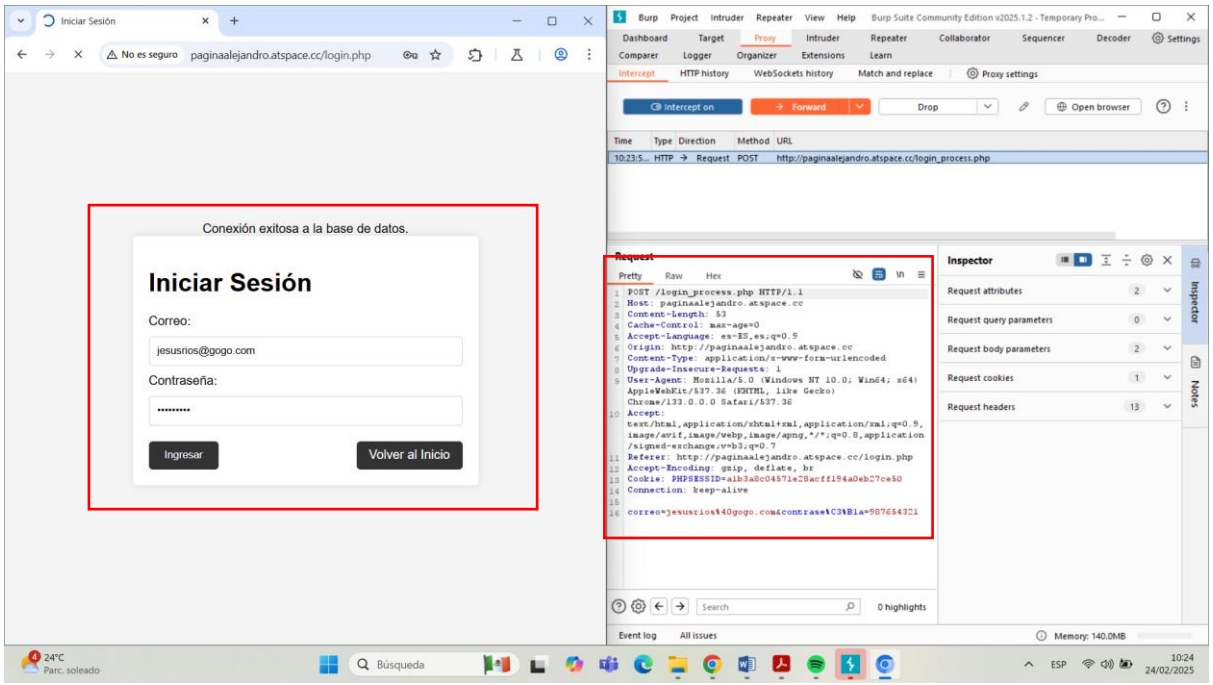
Etapa 3:

Ataque al sitio

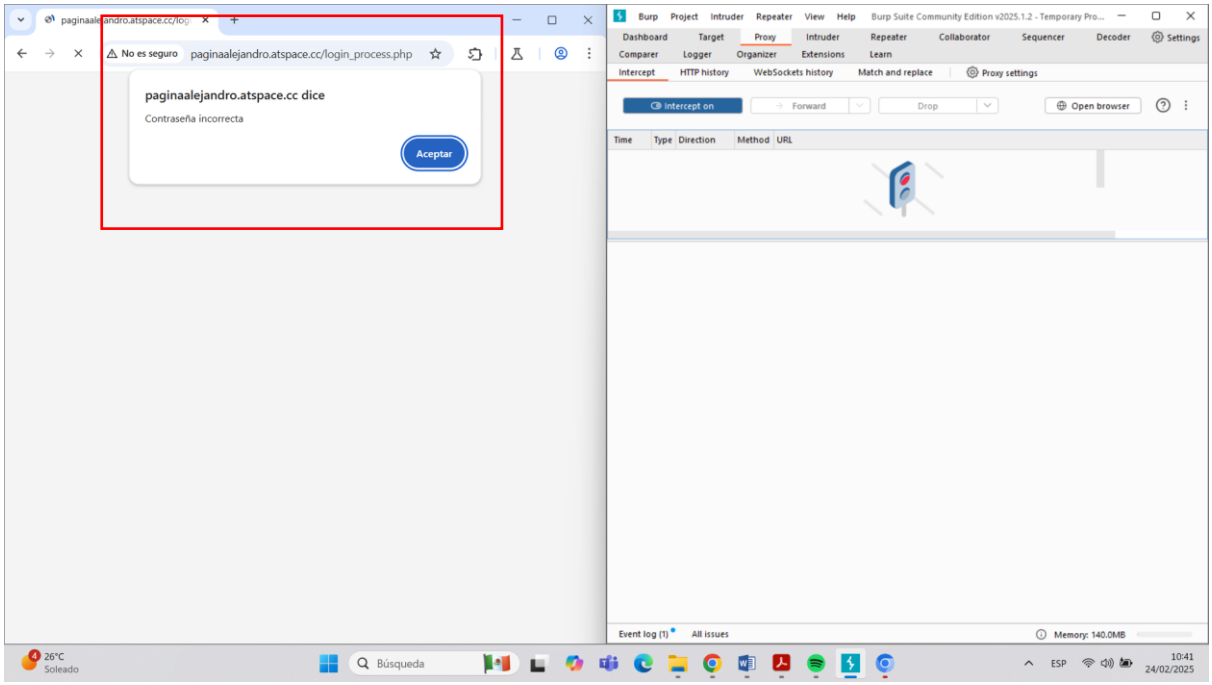
Abrimos Burp Suit y creamos un nuevo proyecto, después ingresamos a la pestaña PROXY y abrimos el navegador, pegamos el link de acceso del sitio web que utilizamos en la primera actividad.



Una vez abierta la página web introducimos las credenciales de acceso correcto y con el uso de Burp suite realizamos la captación de la información como se muestra a continuación.



Hemos realizado la alteracion dela contraseña del usuario y al momento de ingresar nos aparece el mensaje de contraseña incorrecta como se muestra a continuacion.



Conclusión

Como parte final de la materia de auditoria informática en esta última actividad realizamos el ataque a un sitio web sin protocolos de seguridad mediante Cross Site Scripting (XSS) la cual es una vulnerabilidad de seguridad común en aplicaciones web que permite a los atacantes inyectar scripts maliciosos en las páginas vistas por otros usuarios. Los atacantes pueden utilizar esta técnica para robar información sensible, como credenciales de usuario o cookies, secuestrar sesiones, redirigir a los usuarios a sitios maliciosos, o realizar otras acciones maliciosas.

El XSS representa una amenaza seria para la seguridad web. Para prevenir el uso y robo de información en las empresas y sus sitios, las mejores prácticas a realizar seria la validación y escape de los datos de entrada, el uso de cabeceras de seguridad como Content Security Policy y la implementación de medidas de

protección como el uso de frameworks que manejen correctamente la sanitización de datos. La concienciación sobre esta vulnerabilidad y la adopción de medidas preventivas pueden mitigar significativamente el riesgo que representa para los usuarios y la integridad de las aplicaciones.

Referencias

1. *Insecure deserialization | Web Security Academy*. (s. f.). https://portswigger.net/web-security/deserialization
2. Strawbridge, G. (2024, 2 septiembre). Data breach: 5 graves consecuencias de la violación de datos. *MetaCompliance*. https://www.metacompliance.com/es/blog/data-breaches/5-damaging-consequences-of-a-data-breach
3. Ponce, J. L. (2023, 9 agosto). *Auditoría informática: ¿Qué es y cómo hacer una con éxito?* Ikusi MX. https://www.ikusi.com/mx/blog/auditoria-informatica/