
# Actividad

# 2

## Deserialización Insegura

## Auditoria Informática

# Ingeniería en Desarrollo de Software

**Tutor:** Jessica Hernández Romero

**Alumno:** Darío Ismael Núñez Manrriquez

**Fecha:** 13/06/2023

**Auditoria Informática**

Nombre del Autor

Darío Ismael Núñez Manrriquez

Actividad

Deserialización Insegura

Unidad

2

Fecha de entrega

13/06/2023

# índice

## Contenido

# Introducción

¿cómo afecta el ataque de pérdida de autenticación de datos a los usuarios de internet?

La seguridad es uno de los aspectos mas interesantes que debemos tener en cuenta cuando realizamos el desarrollo de alguna aplicación. Cuando se toman riesgos estos sirven para orientar al desarrollador o profesionales de la seguridad sobre las vulnerabilidades mas criticas que se encuentran las aplicaciones web.

A continuación, mostrare algunos ejemplos de riesgos de aplicaciones web.

1. Inyección

Es una vulnerabilidad de las aplicaciones WEB, que afecta directamente a las bases de datos de la aplicación.

2. Pérdida de autenticación

Las vulnerabilidades relacionadas con la pérdida de autenticación son críticas en la seguridad de las aplicaciones y en especial de las aplicaciones WEB

3. Exposición a datos sensibles

Las aplicaciones WEB que no protegen adecuadamente los datos confidenciales,

4. Entradas XML

Este es un ataque contra una aplicación web que analiza la entrada XML *. Esta entrada puede hacer referencia a una entidad externa,

Esto es solo 4 de 10 ejemplos de riesgos de aplicaciones web

## Descripción

En la siguiente actividad la plataforma me brinda una especifica selección de pagina en la cual implementare un ataque para revisar su vulnerabilidad en su seguridad, para realizar la actividad la plataforma me brinda la siguiente instrucción. Las instrucciones son las siguientes.

**Contextualización:**

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

Para esta segunda etapa, pide realizar una prueba de deserialización insegura en una página específica. Esta debe ser mediante las cookies. Para lograrlo, utilizar el programa Burp Suite Community Edition. El objetivo de esta prueba es que se inicie sesión como un usuario normal y luego pasar a modo administrador a través de las cookies.

**Actividad:**

Con la ayuda de la plataforma PortSwigger, realizar el ataque a una página proporcionada por ellos. En ella, iniciar sesión con las credenciales que se proporcionan, las cuales son para usuarios normales; no obstante, a través de las cookies, entrar al modo administrador.

Cabe mencionar que este laboratorio utiliza un mecanismo de sesión basado en serialización. Por ende, es vulnerable a la escalada de privilegios. En consecuencia, hay editar el objeto serializado en la cookie de sesión para aprovechar esta vulnerabilidad y obtener privilegios administrativos. Finalmente, el objetivo es eliminar la cuenta de Carlos.

Hay que iniciar sesión en la propia cuenta con las siguientes credenciales:

- Usuario: wiener
- Contraseña: peter

## Justificación

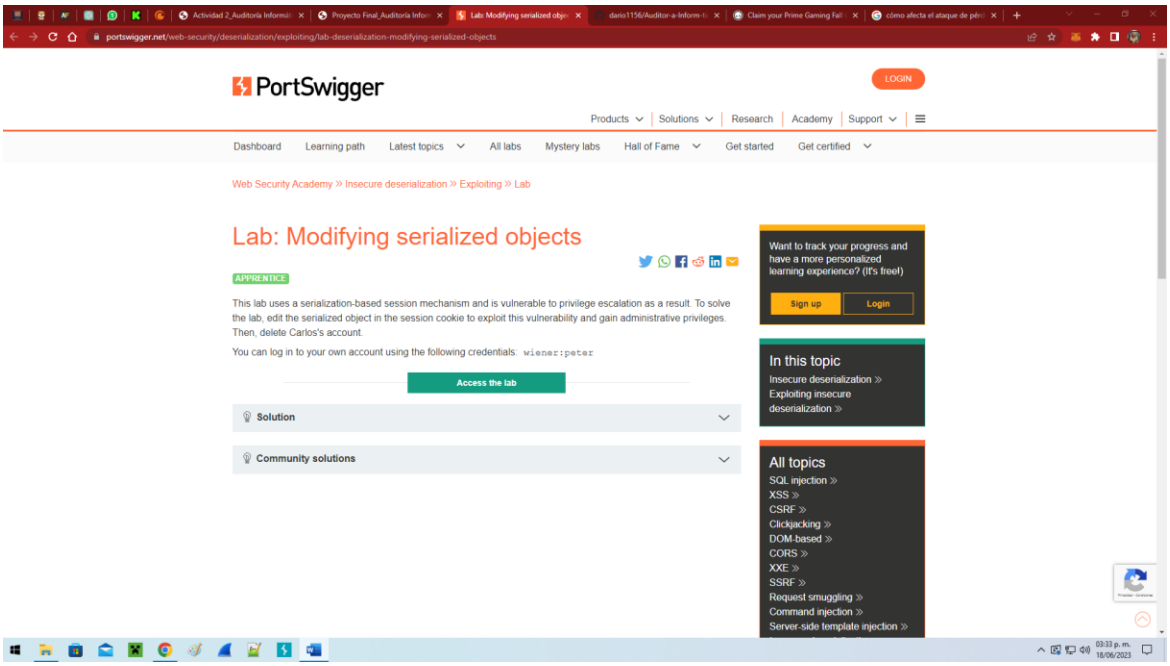
El detalle de realizar esta actividad es para poder aprender sobre la Deserialización Insegura este tipo de ataque se realiza mediante las cookies, para lograrlo se utilizará la aplicación Burp Suite Community Edition, El objetivo de esta prueba es que se inicie sesión como un usuario normal y luego pasar a modo administrador a través de las cookies.

Realizando esta actividad con la ayuda de la plataforma portswigger se realiza el ataque a la página proporcionado por la plataforma de la escuela yo pienso que al realizar esta aplicación será tema para considerar al tener que asegurar alguna pagina web

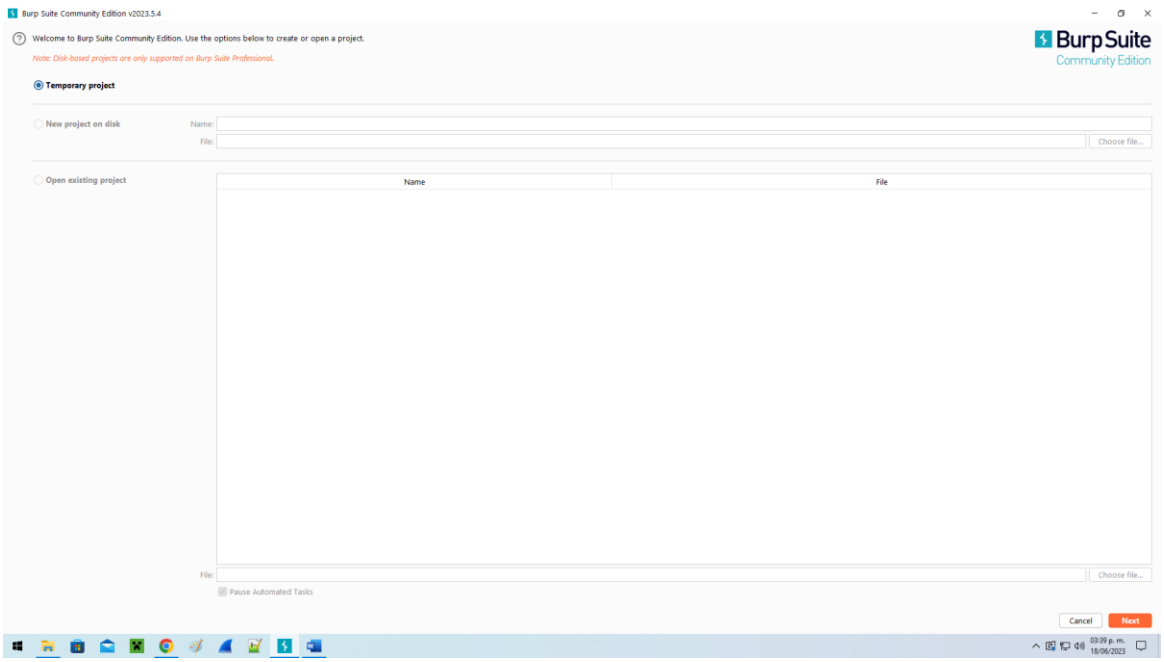
Se plantea desarrollar este proyecto con el propósito de identificar estas vulnerabilidades de seguridad y describir los riesgos a los que se expone dicha entidad. Asimismo, se pretende brindar unas acciones en pro de mitigar las falencias de seguridad con la aplicación de técnicas basadas en OWASP Top 10.

## Ataque al sitio

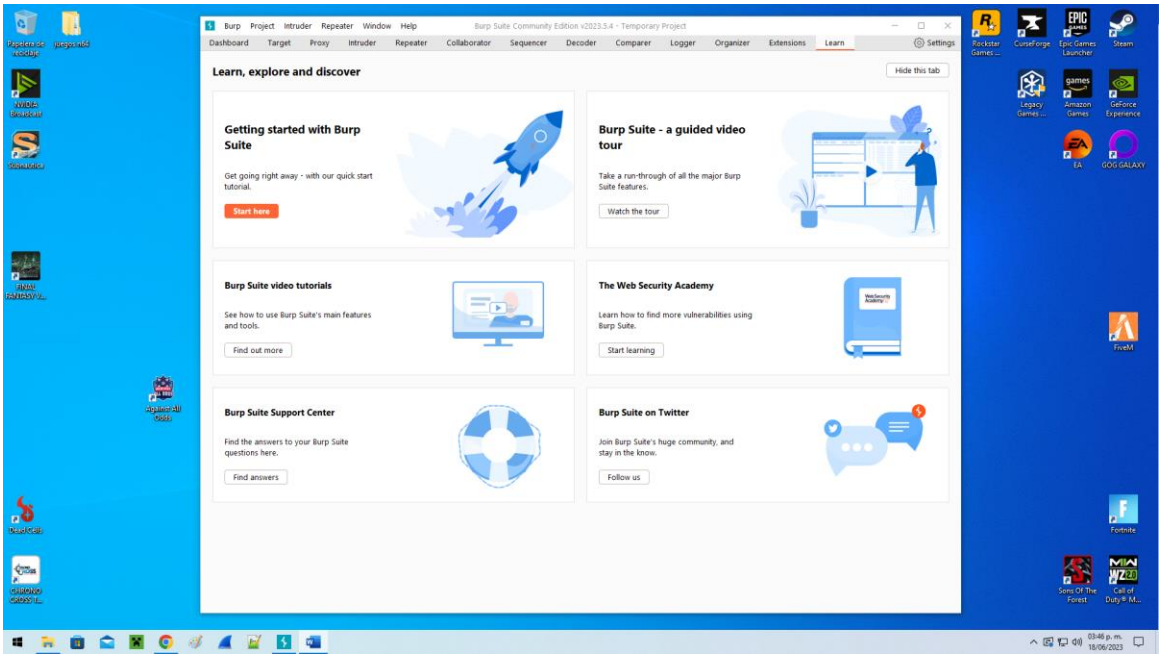
Entrando al laboratorio de practica primer captura,



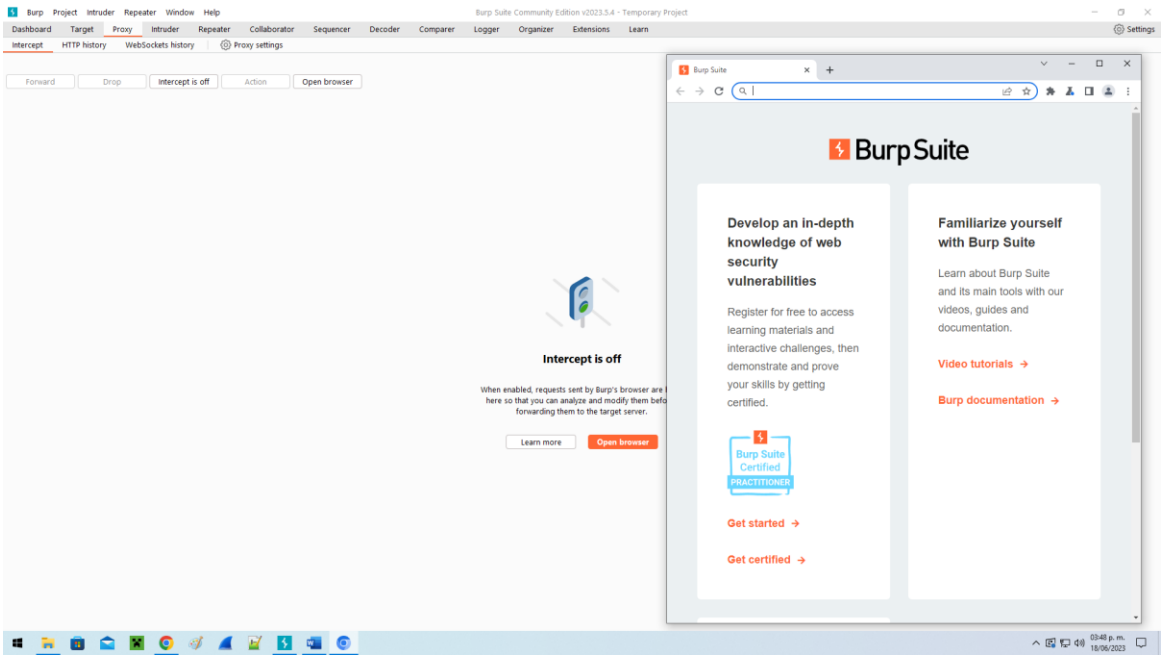

Iniciando la aplicación Burp Suite Community Edition.



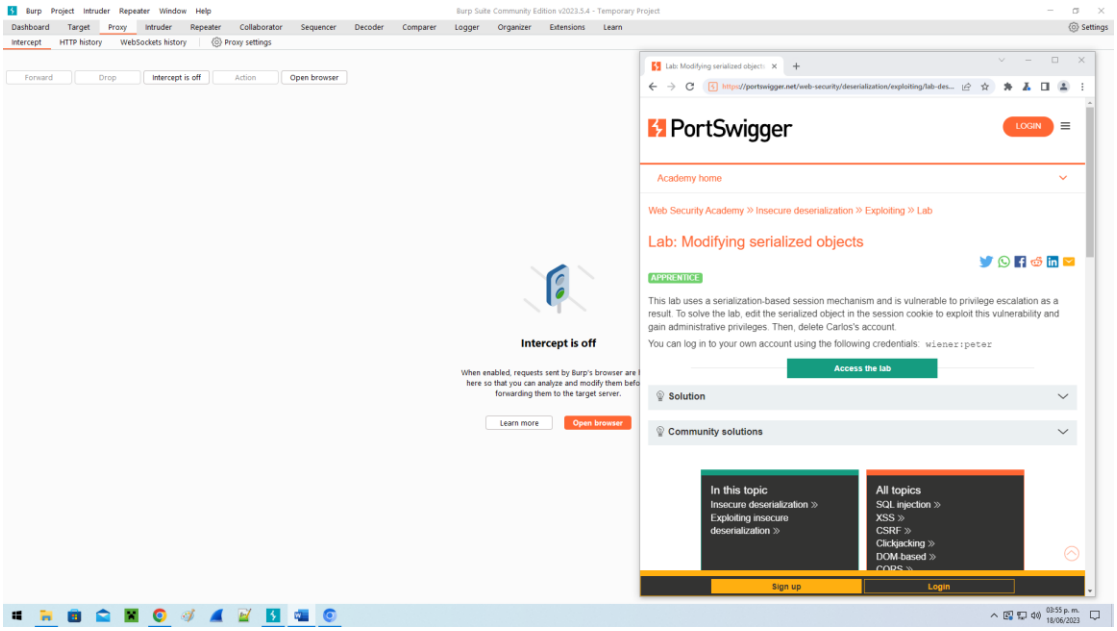
Alistando la aplicación para realizar el ataque.




Siguiendo las indicaciones

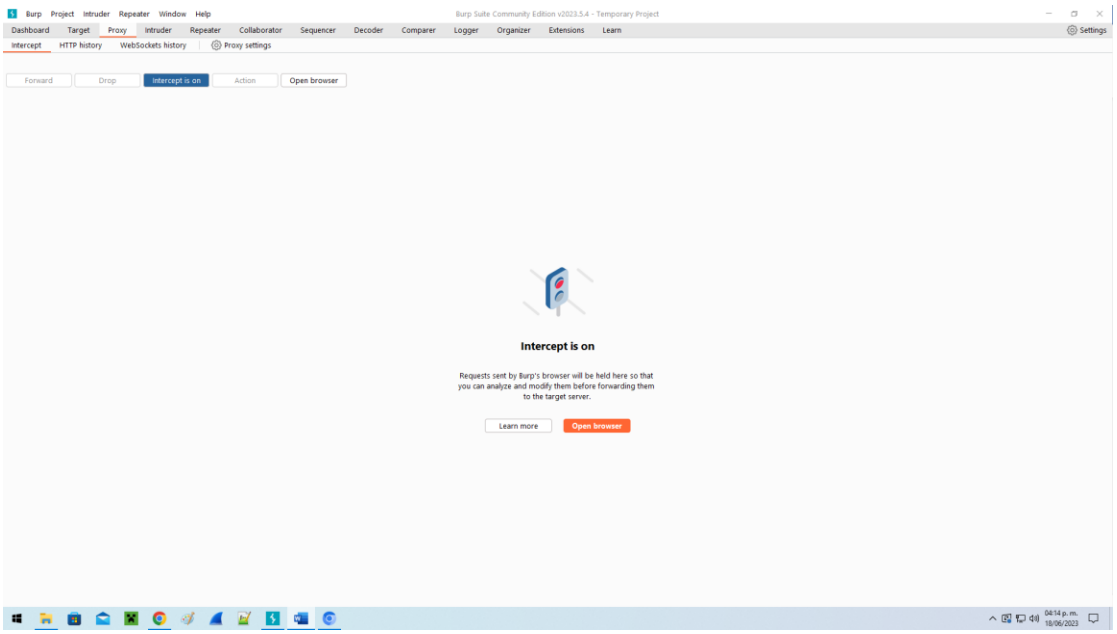


Ingresando ala pagina de laboratorio proporcionada por la escuela



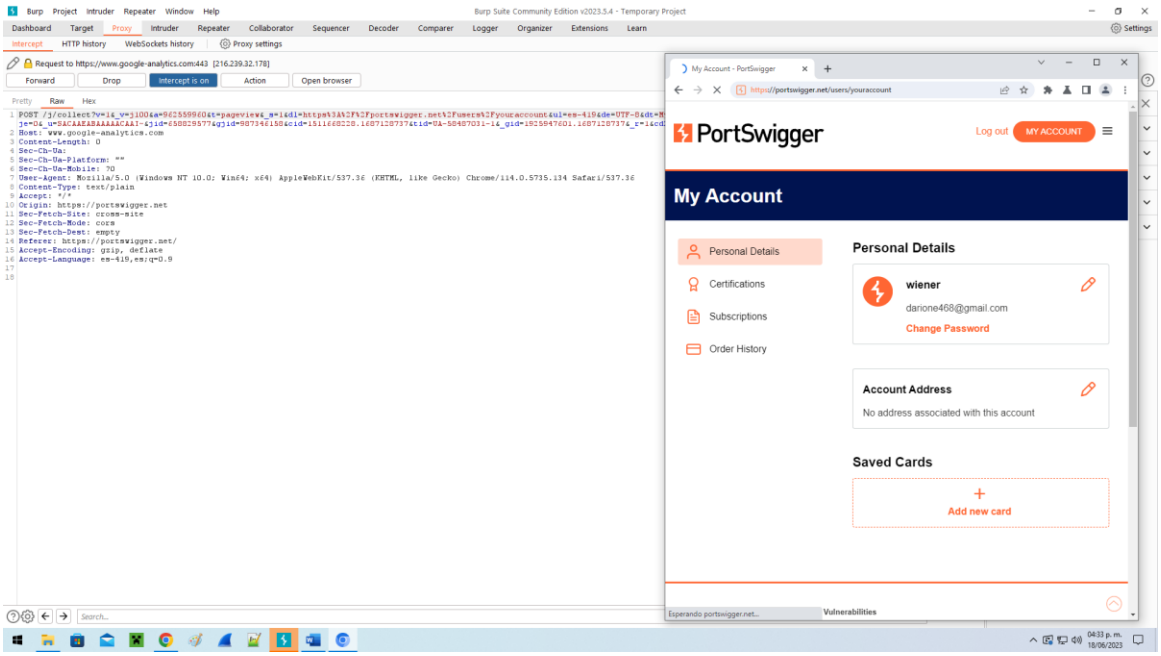

Terminando registro en la página de laboratorio

Contraseña de pagina: \AP6+#8jtdaj\JM2w'{\GeHi\d984394

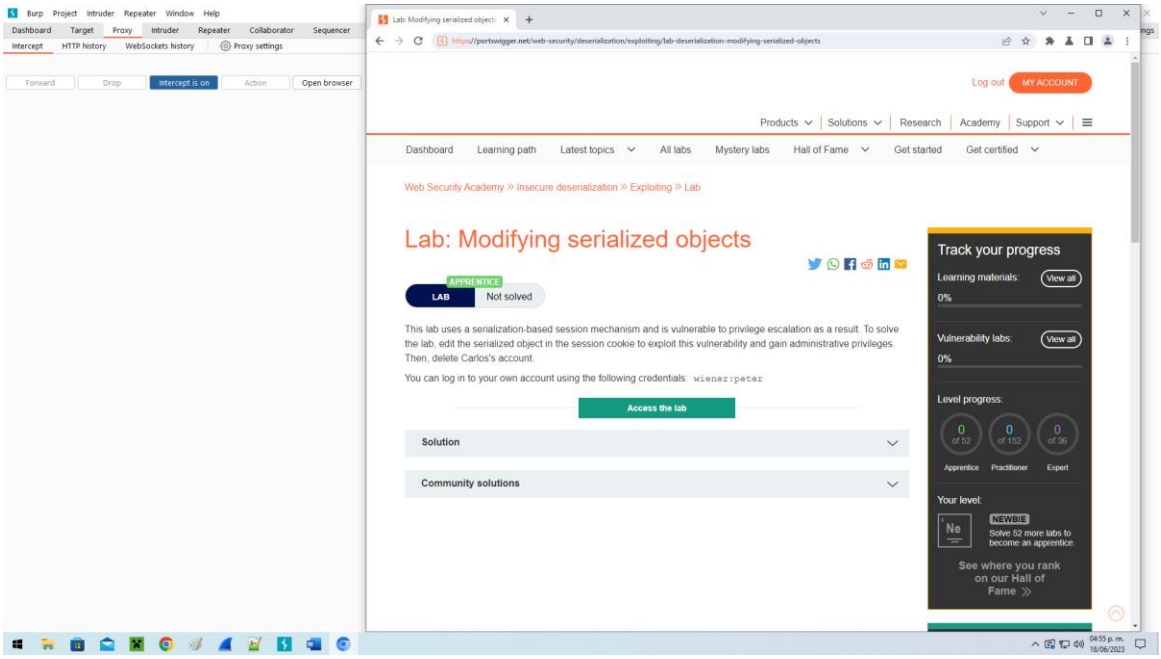



Activando intercept is on

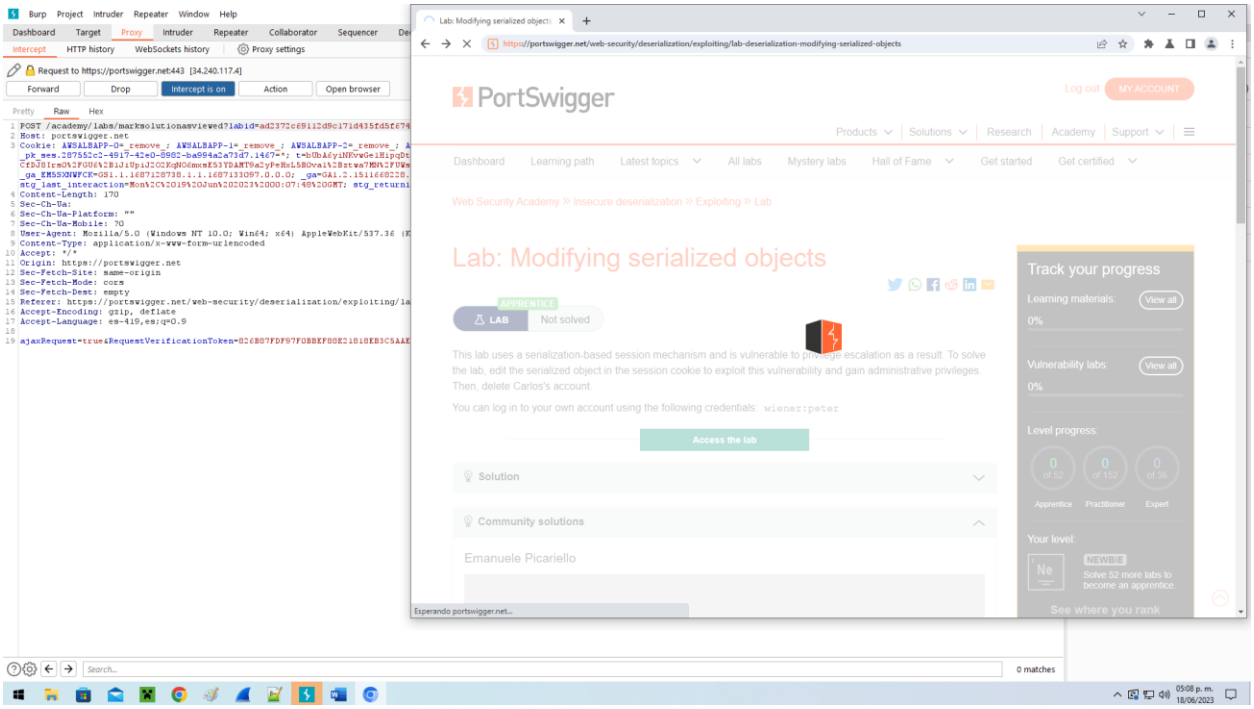
Captura mostrando que ya estoy dentro del usuario creado




Dentro de laboratorio



Rezlizando practoica laboratorio




Después de esto la pagina se quedaba colgada y en blanco ya no aparecía nada mas

Soy del fuerte Sinaloa y tengo un pésimo internet y le atribuyó esta falla al internet

Para todo me falla,

## Conclusión

Al realizar esta actividad me dio inseguridad, que creo no superare porque en realidad me mostro lo fácil que puede ser vulnerar una pagina web aun que esta este diseñado para realizar este tipo de actividades.

Pero el fin de esta actividad no es para causarme inseguridad es para demostrarme que las páginas web tienen vulnerabilidades y debemos de buscar la manera para poder reforzar esas vulnerabilidades de tal manera que sea cada vez más difícil el poder penetrar la seguridad implementada por el equipo de desarrollo.

## Bibliografía

En si la información que tome la tome del archivo PDF que la escuela patrocina y no tengo la necesidad de bibliografía alguna ´parte de este proyecto

Link de github:

https://github.com/dario1156/Auditor-a-Inform-tica