Actividad [#2] – [Deserialización Insegura]

[Auditoría Informática]

Ingeniería en Desarrollo de Software

Tutor: Lic. Jessica Hernández Romero

Alumno: Alan David López Rojas

Fecha:28/09/2023

Índice

Introducción

La pérdida de autenticación de datos representa una seria amenaza en el mundo digital y afecta considerablemente a los usuarios de internet. Esta vulnerabilidad permite que los atacantes obtengan acceso no autorizado a cuentas y servicios en línea, lo que puede tener una serie de impactos negativos en la vida de las personas.

Uno de los efectos más evidentes de la pérdida de autenticación es el acceso no autorizado a cuentas y servicios en línea. Los atacantes pueden aprovechar vulnerabilidades en los sistemas de autenticación débiles o explotar la falta de medidas de seguridad para entrar en cuentas ajenas. Esto puede resultar en la suplantación de identidad, donde los atacantes se hacen pasar por el usuario legítimo, lo que puede llevar al acceso no autorizado a información confidencial y servicios privados.

Además, la pérdida de autenticación puede dar lugar al robo de información personal, como contraseñas, números de teléfono, direcciones de correo electrónico y datos financieros. Esta información robada se puede utilizar para cometer fraudes, robo de identidad y otros delitos cibernéticos, lo que puede causar pérdidas financieras y problemas legales para las víctimas.

La vulnerabilidad también puede dañar la reputación en línea de los usuarios, ya que los atacantes pueden publicar contenido malicioso en nombre del usuario. Esto puede afectar tanto a nivel personal como profesional, socavando la confianza en línea y la imagen de una persona.

Descripción

En esta actividad, espero aprender sobre las vulnerabilidades de seguridad en línea, específicamente la pérdida de autenticación de datos. Me gustaría comprender en detalle cómo los atacantes pueden explotar esta vulnerabilidad para obtener acceso no autorizado a cuentas y servicios en línea, así como las posibles consecuencias negativas que esto puede tener para los usuarios.

Espero obtener una comprensión más profunda de cómo funciona la pérdida de autenticación, incluyendo los métodos que los atacantes pueden utilizar para comprometer la seguridad de las cuentas en línea. Además, me gustaría aprender sobre las mejores prácticas y medidas de seguridad que los usuarios pueden tomar para proteger sus cuentas y datos personales contra esta amenaza.

En particular, estoy interesado en aprender cómo se pueden detectar y prevenir ataques de pérdida de autenticación y qué herramientas o técnicas pueden utilizarse para mitigar los riesgos asociados. Además, me gustaría entender cómo las organizaciones y las empresas pueden mejorar la seguridad en línea para proteger a sus usuarios contra esta vulnerabilidad.

Justificación

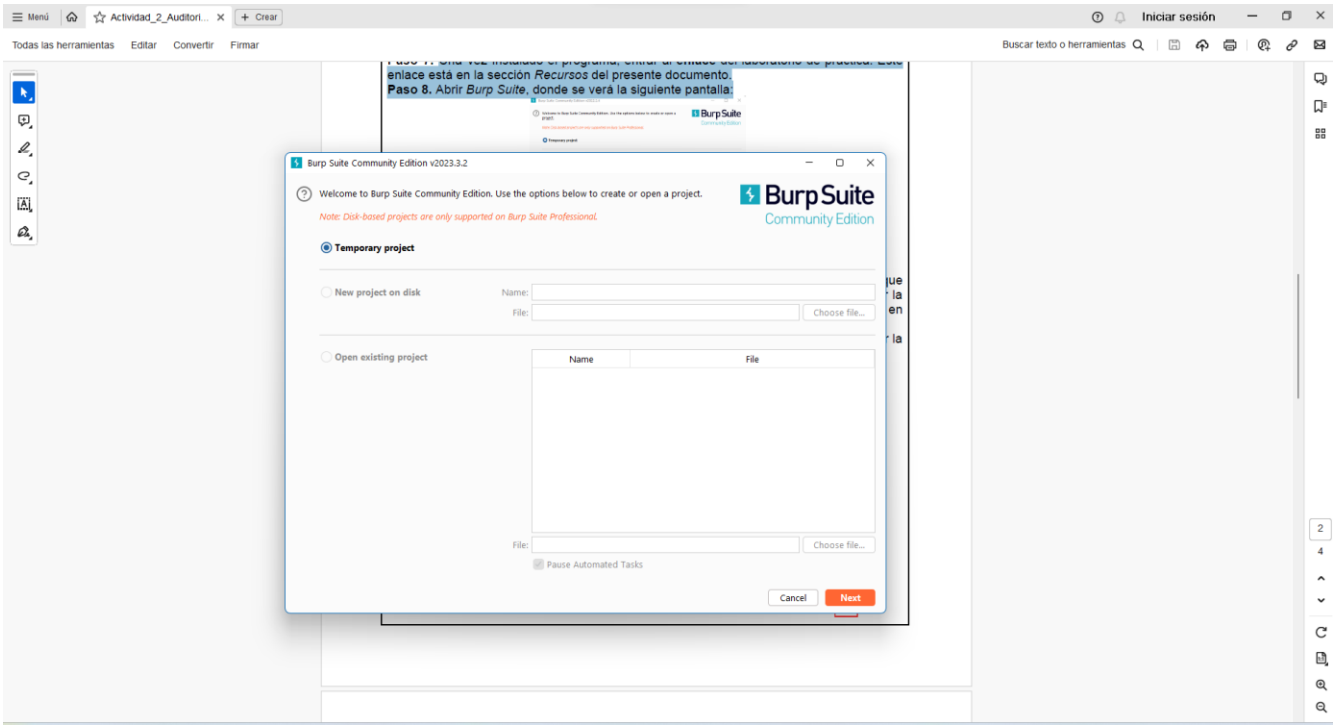
La realización de pruebas de este tipo de ataque, conocido como pérdida de autenticación de datos, se justifica por su importancia crítica en la evaluación y mejora de la seguridad en línea. Estas pruebas son esenciales debido a que ayudan a identificar y mitigar vulnerabilidades de seguridad en sistemas y aplicaciones web, incluida la explotación de debilidades en la autenticación. Esta identificación temprana es crucial para prevenir posibles ataques cibernéticos y proteger la confidencialidad de los datos sensibles, garantizando que solo personas autorizadas tengan acceso a ellos.

Además, las pruebas de pérdida de autenticación permiten a las organizaciones cumplir con regulaciones y normativas de seguridad cibernética que requieren la evaluación y protección de datos de usuarios, como GDPR o HIPAA. También ayudan a las empresas a mejorar su preparación para enfrentar amenazas del mundo real, lo que puede evitar incidentes costosos y dañinos, así como preservar la reputación de la organización al evitar incidentes de seguridad que podrían socavar la confianza de clientes y socios.

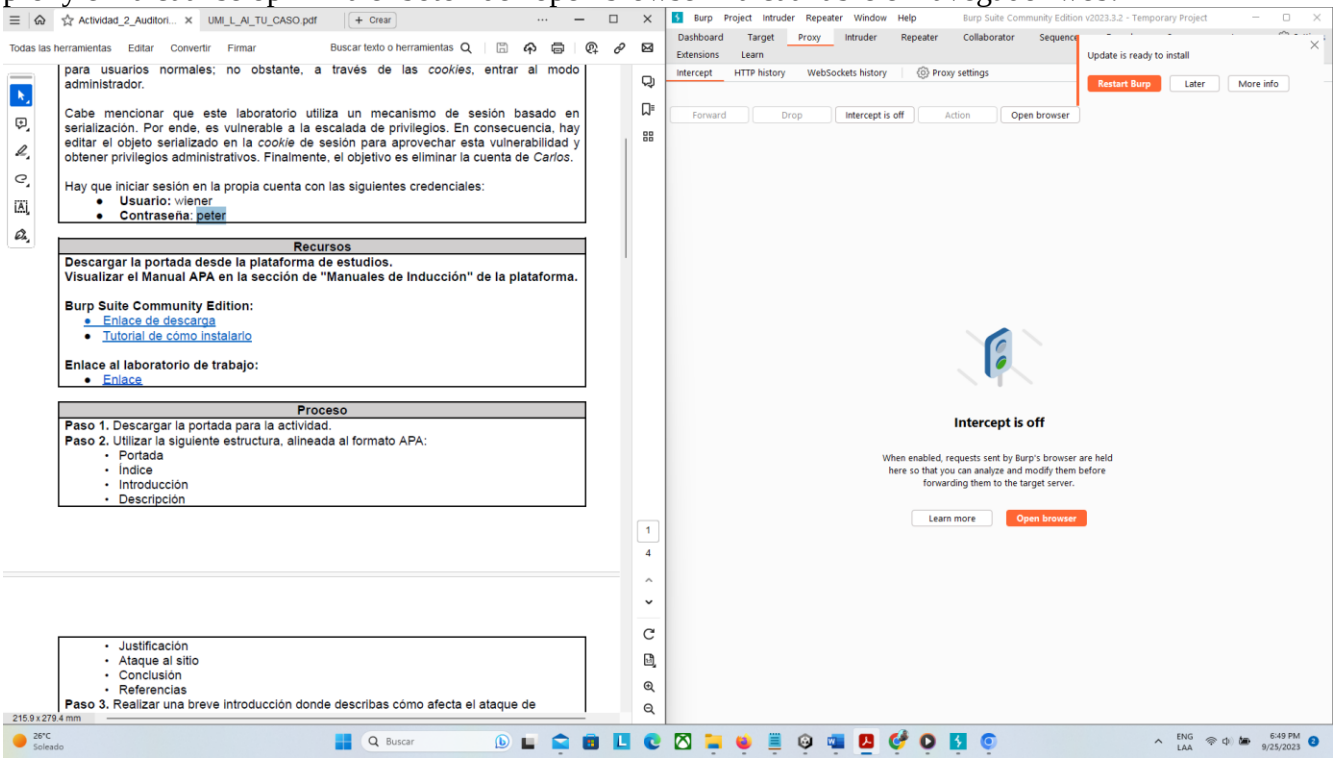
Las pruebas de pérdida de autenticación son esenciales para proteger la información confidencial, cumplir con regulaciones, mejorar la seguridad y preservar la confianza en línea en un mundo digital cada vez más interconectado y vulnerable a ataques cibernéticos.

Ataque al sitio

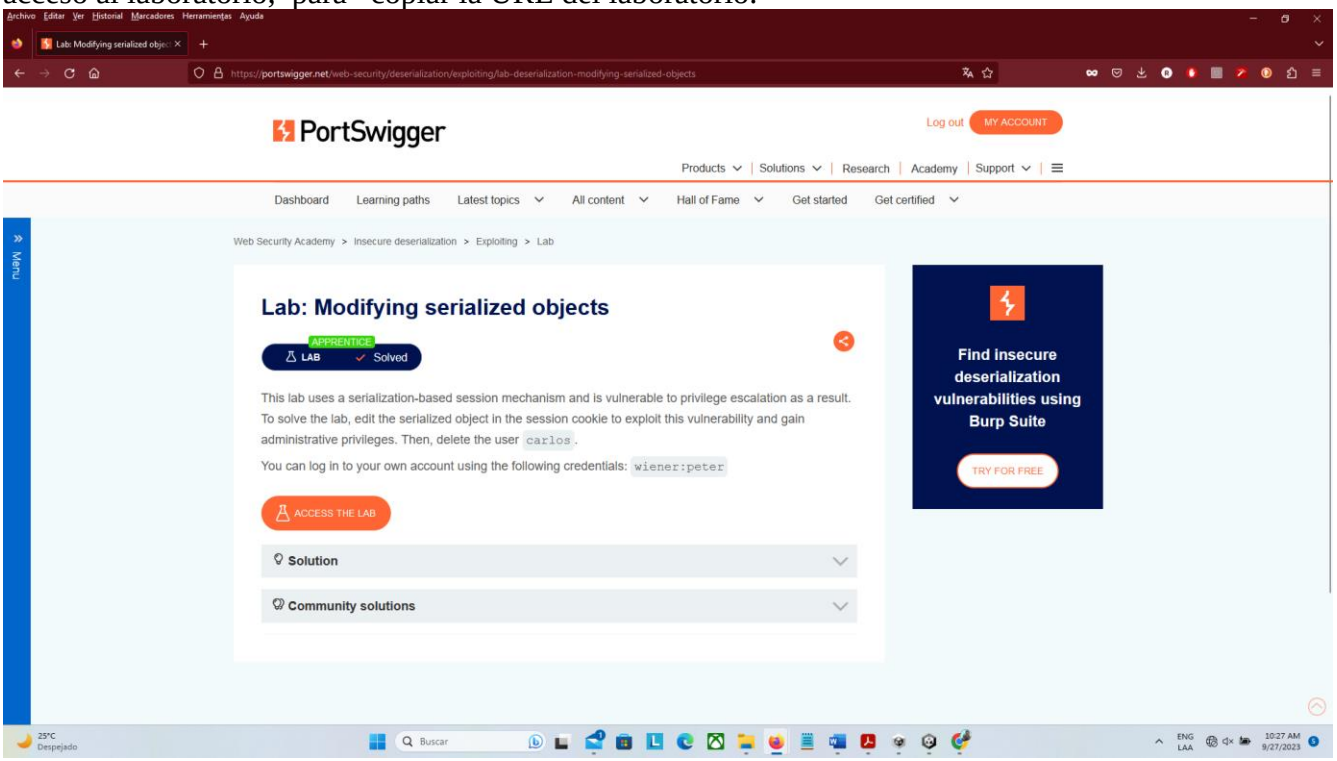
Primeramente para la práctica de esta actividad descargue el programa Burp Suite Community Edition, y luego en la página web Portswigger cree mi cuenta para poder realizar el ataque.



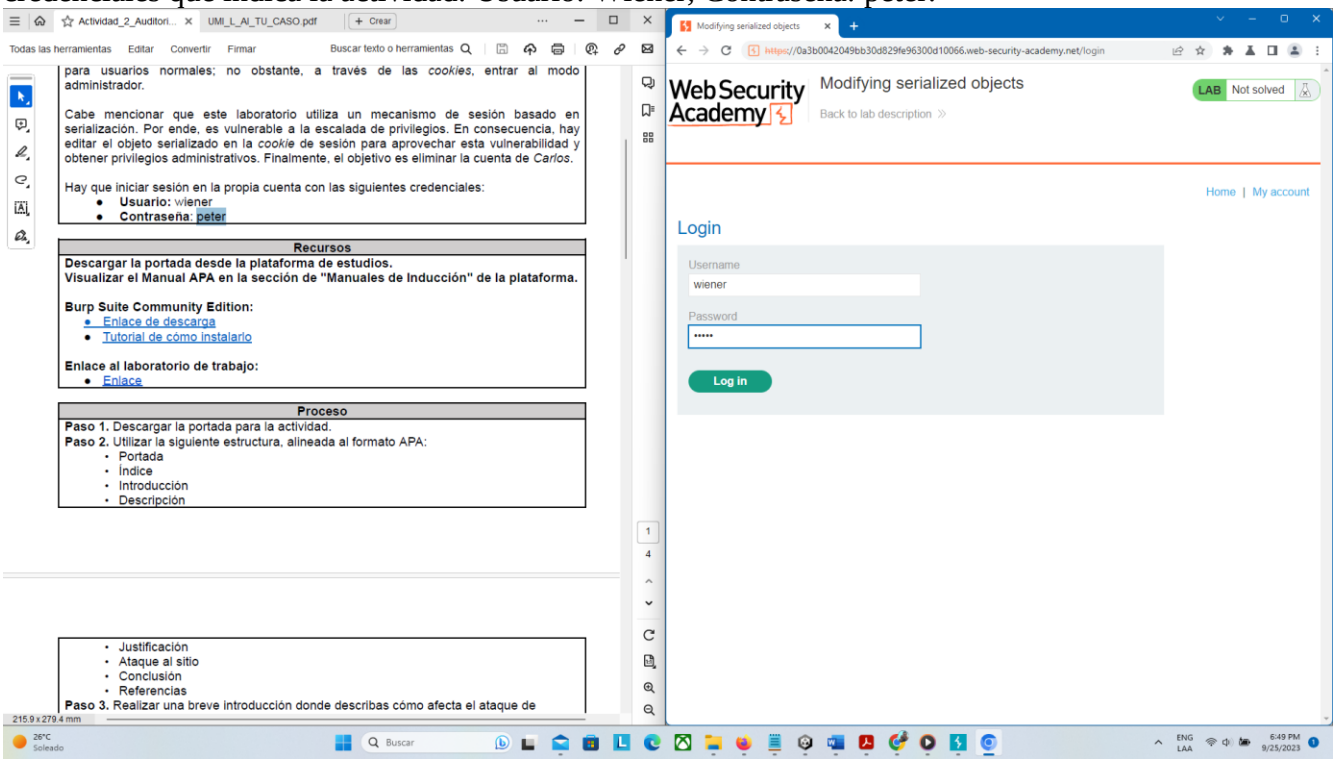
Posteriormente se ingresó al programa Burp suite con la configuración de default en la pestaña de proxy en la cual se oprimirá el botón de “open browser” la cual abre el navegador web.



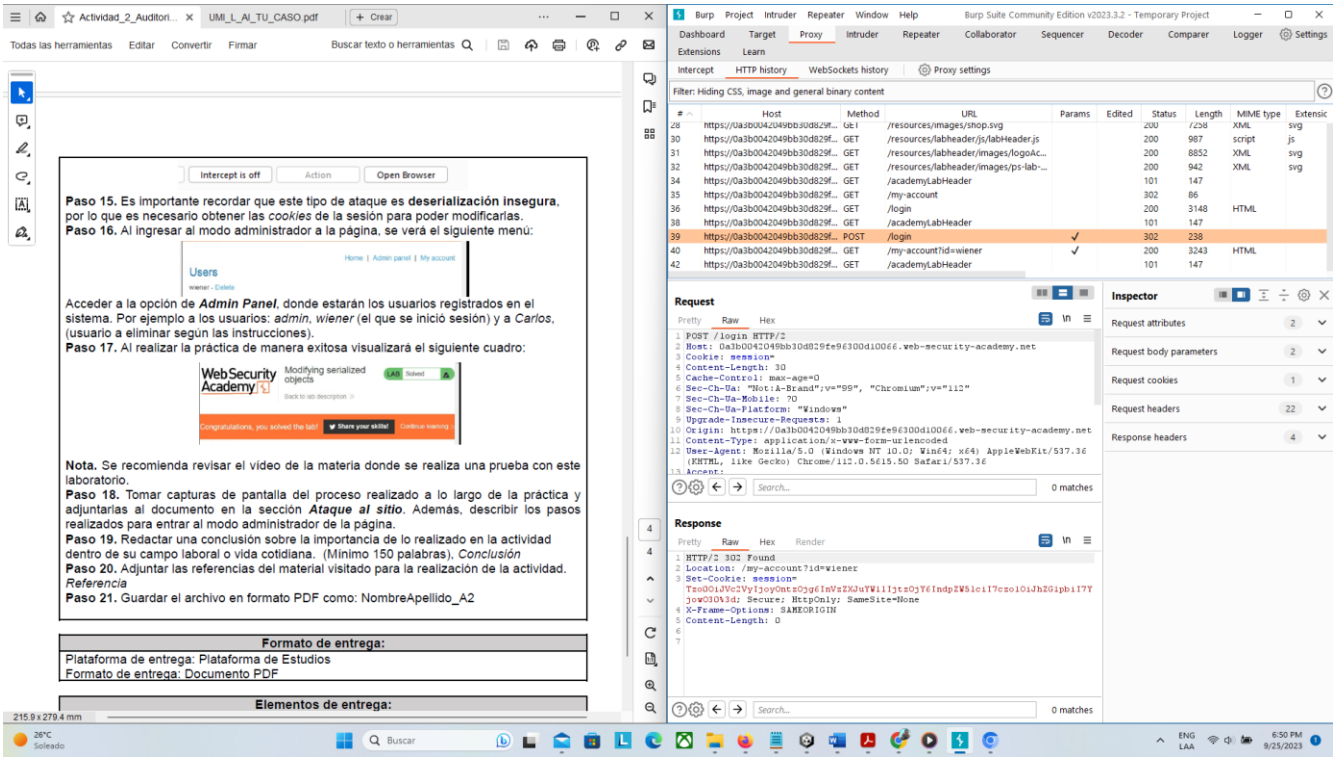
En este punto ya en mi navegador predeterminado, había creado mi cuenta en PortSwigger, y hecho el acceso al laboratorio, para copiar la URL del laboratorio.



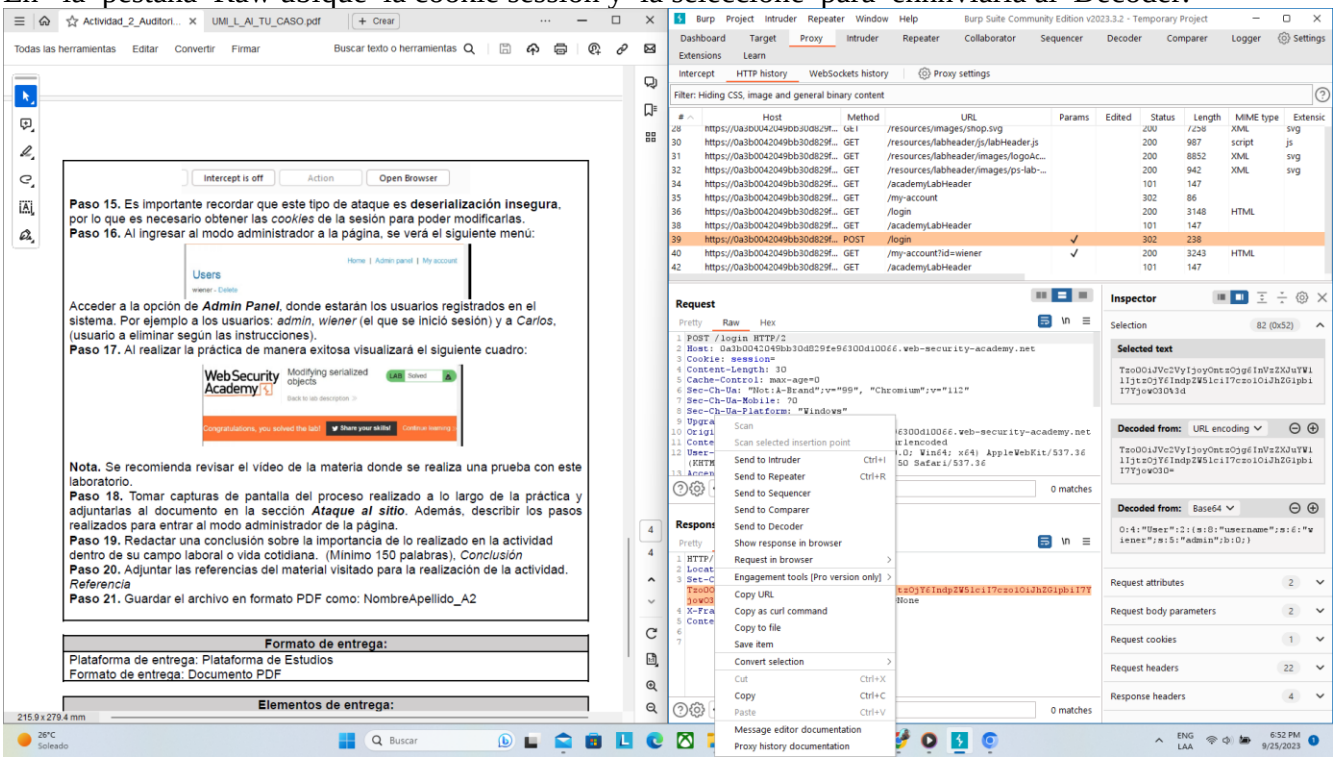
Ya en el navegador se pegará y abrirá la URL del sitio de PortSwigger, en esta se accedió con las credenciales que indica la actividad: Usuario: Wiener, Contraseña: peter.



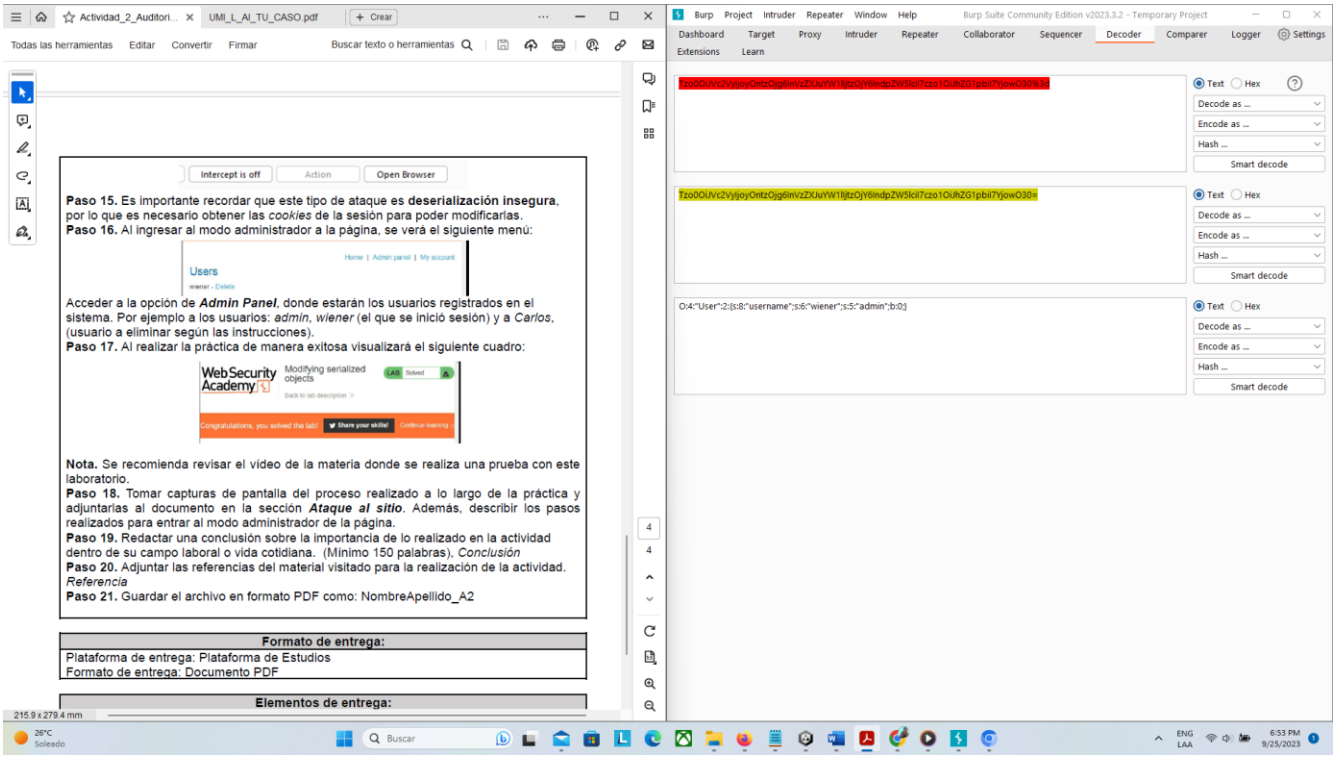
Una vez se ingresaron las credenciales, me regrese al programa Burp Suite, en el apartado de proxy y en la pestaña de HTTP history, ubique el método POST y la URL /login que es la acción que hice al iniciar sesión con las credenciales.



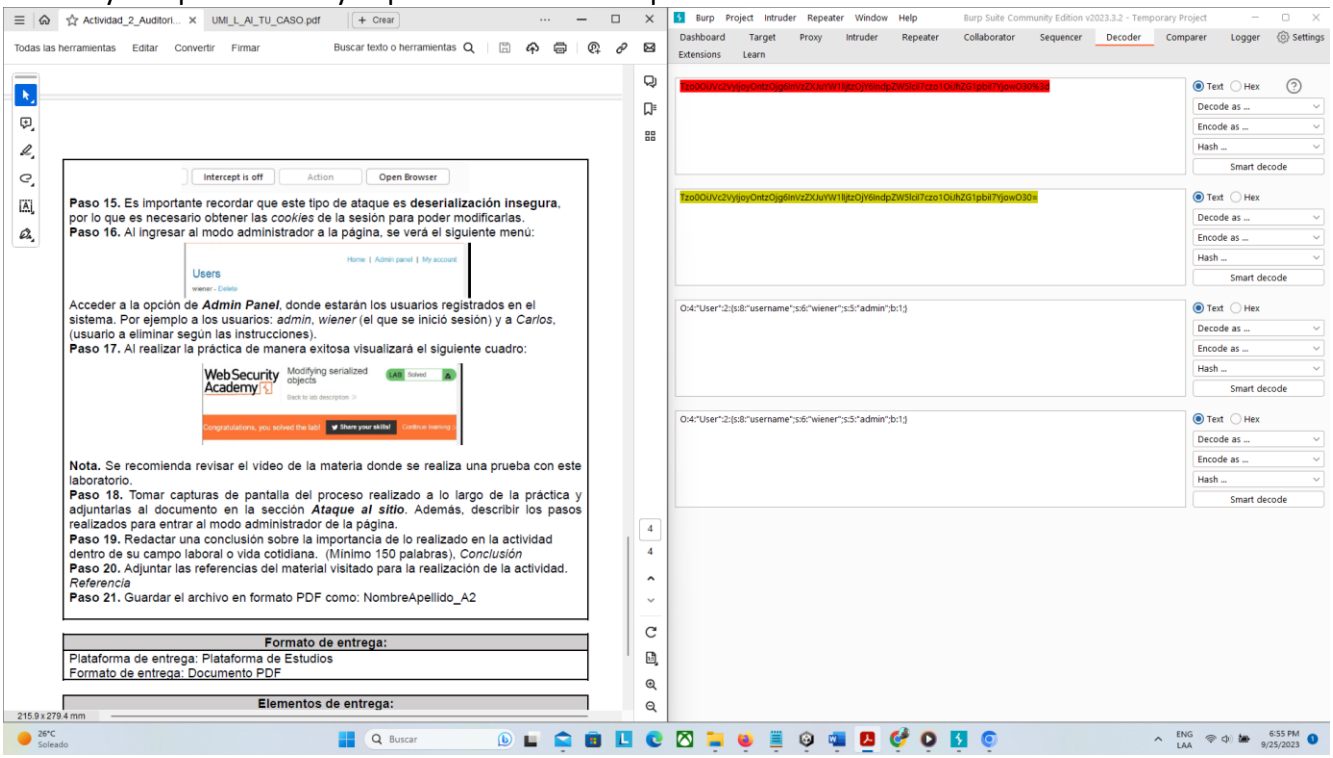
En la pestaña Raw ubique la cookie session y la seleccione para ennnviarla al Decoder.

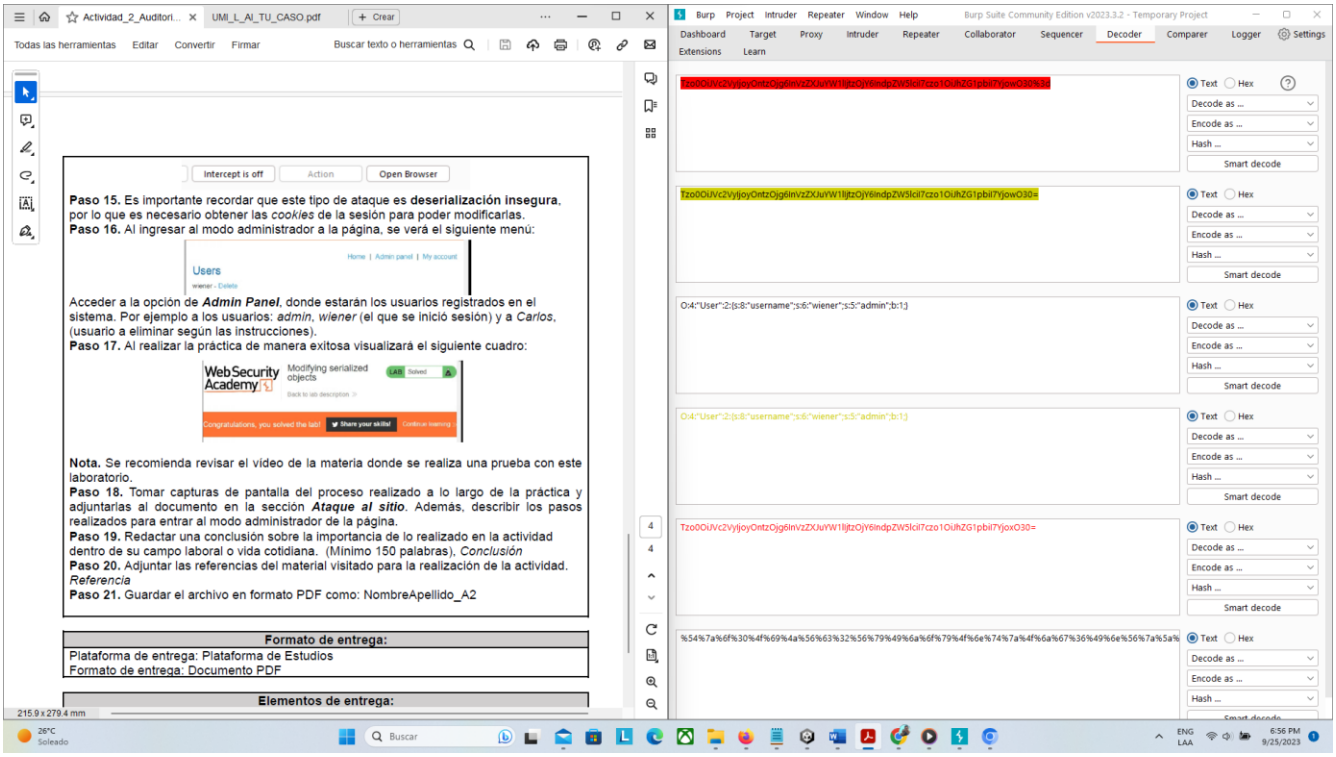


Ya una vez enn el codificador primero lo decodifique a URL y despes a base64, me envio la informacion serializada y al final de esta hay un cero que representna que el usuario no es administrador.

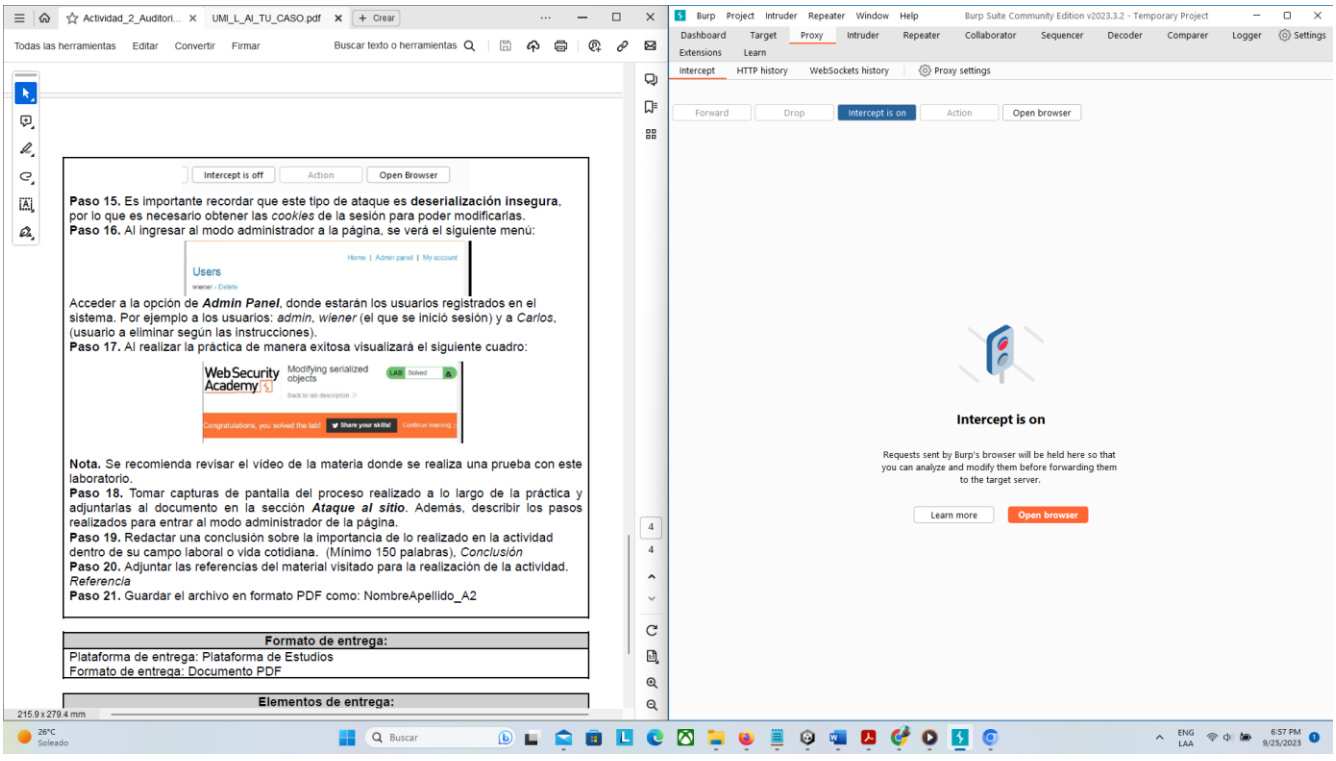


Cambie el 0 por un 1 que representa que el usuario es administrador, luego codifique a base64 y despues a URL y copie el resultado con permisos de admionistrador.

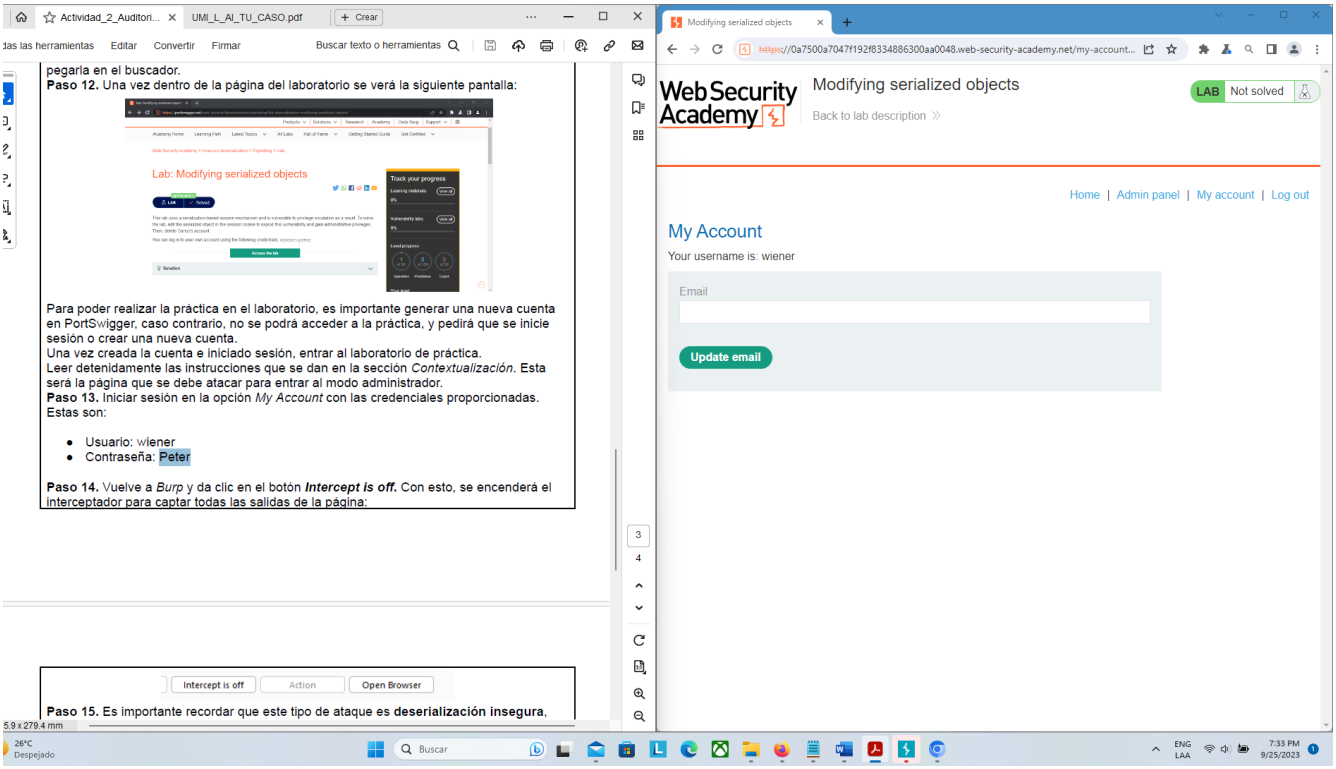




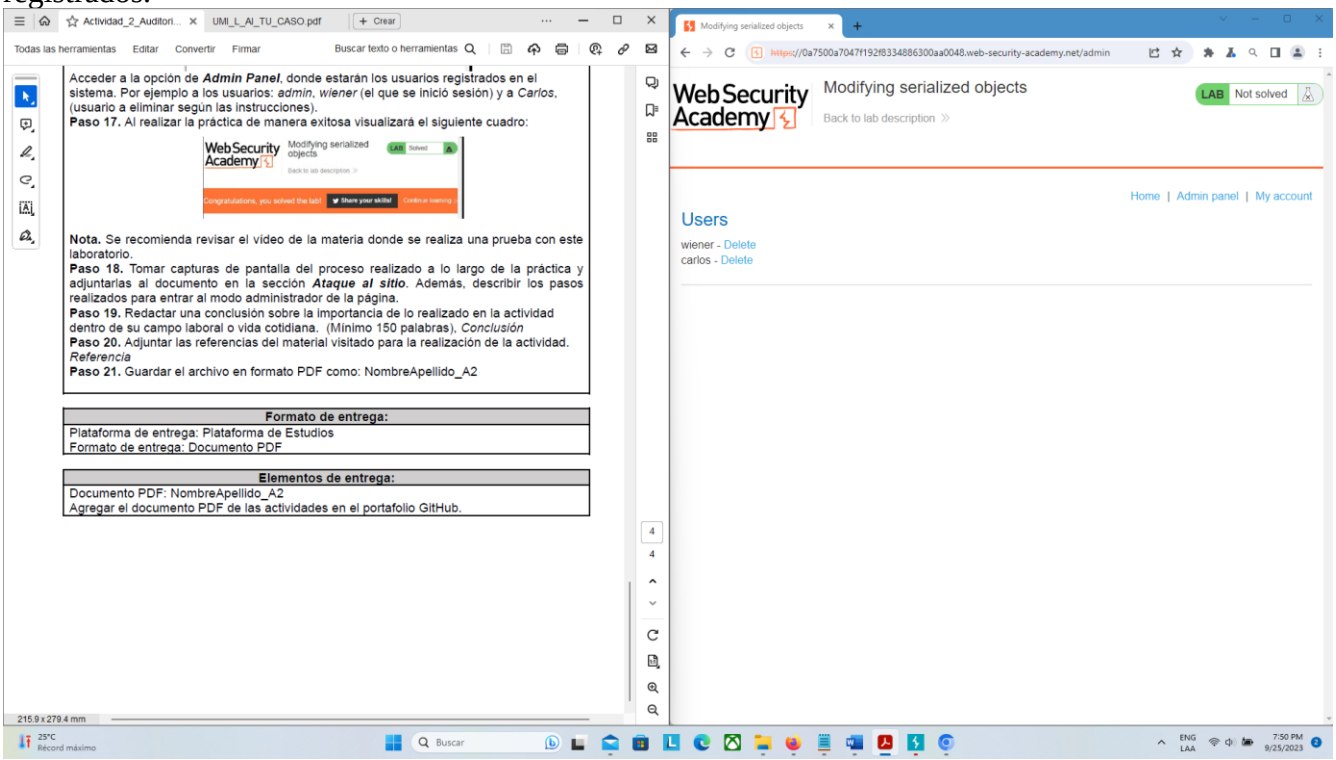
Despues encendi el interseptor y recargue la pagina del buscador y abrio la informacion de sesion del usuario.



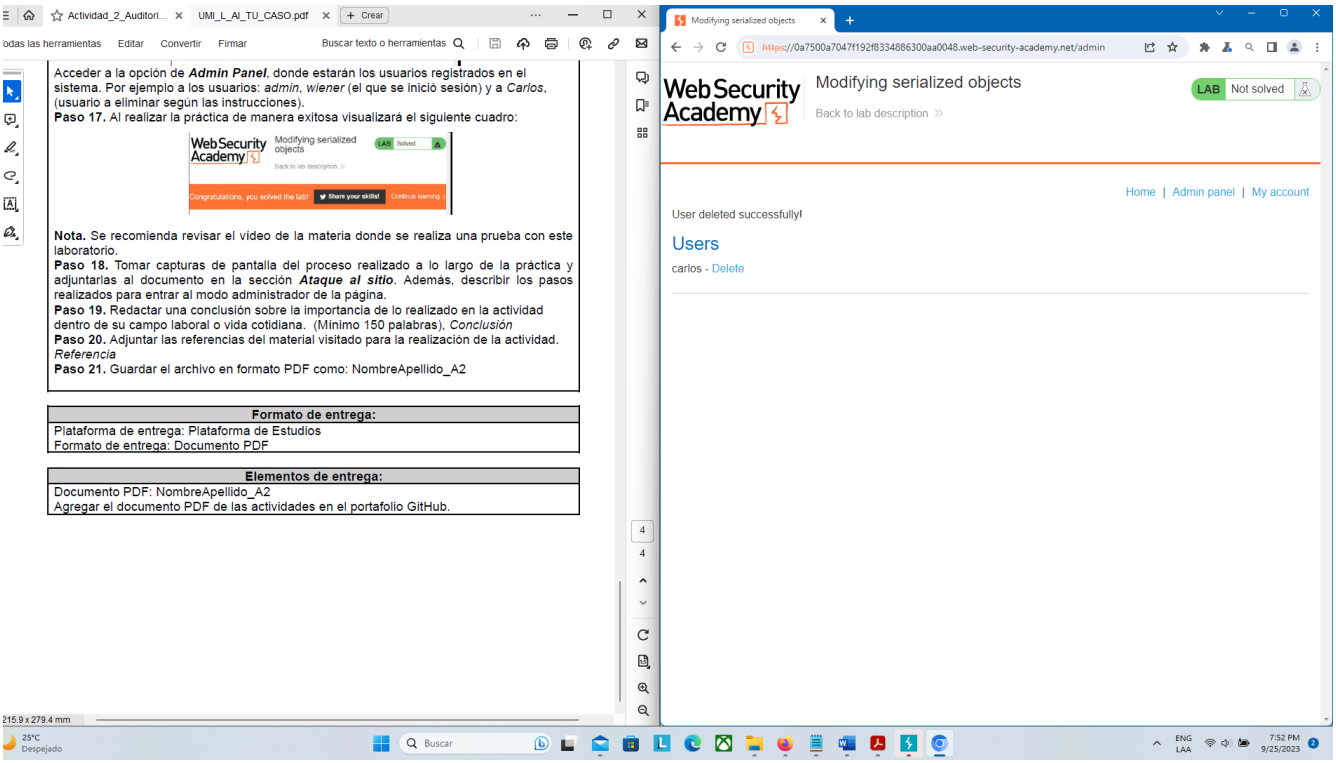
Despues cambie la informacion de cookie sessionn y la cambie por la que acabo de obtener con credenciales de administrador y me arrojo una nueva opcion que es panel de administrador.



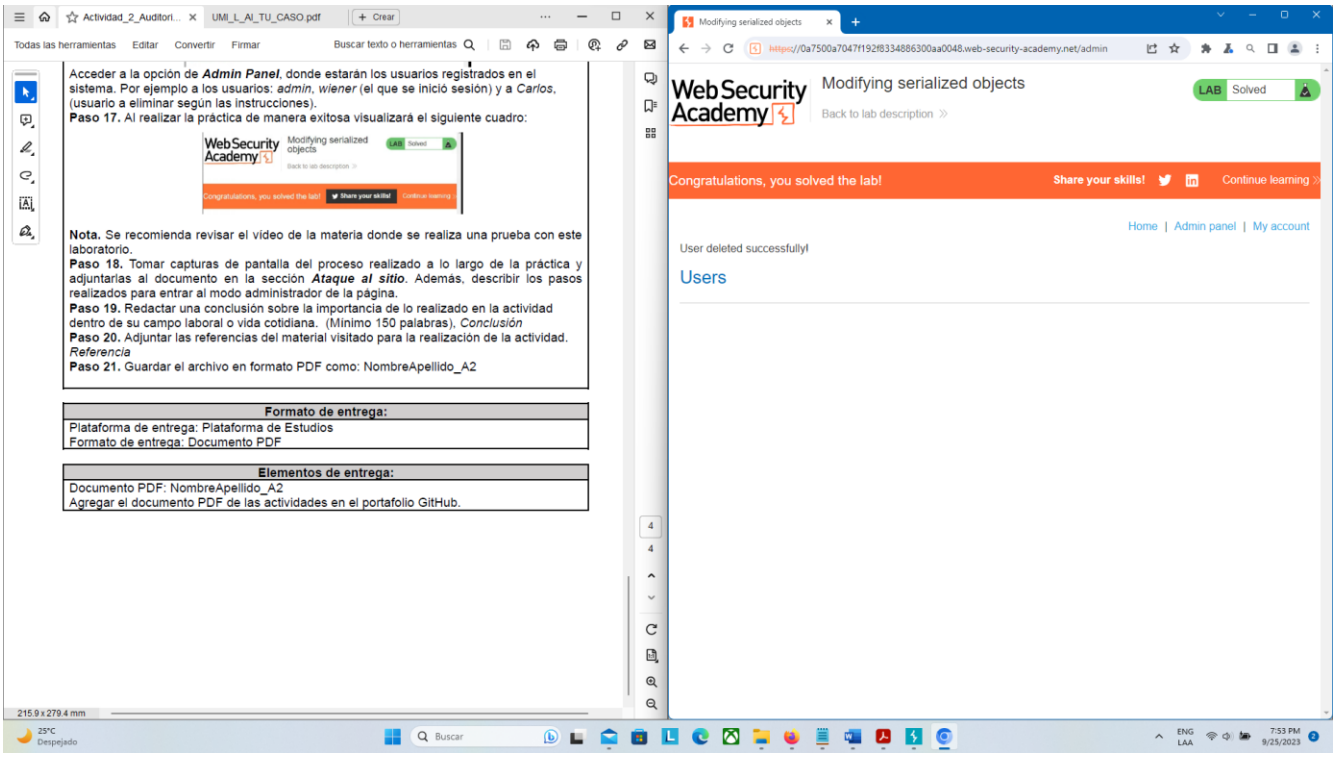
Se dio clic en esa opción y luego en la pestaña de raw se cambió nuevamente la información de cookie session y me dio un nuevo cambio en la página, a una interfaz de administrador con los usuarios registrados.



Se le dio a eliminar a un usuario y sustituimos nuevamente las credenciales, de esta manera se eliminó al usuario.



Con esto se comprueba como se puede acceder a credenciales de administrador y hacer modificaciones, finalmente la pagina me arrojo el mensaje que se había completado el laboratorio.



https://github.com/AlanDavidLR/AuditoriaInformatica.git

Conclusión

La actividad realizada, que involucró la prueba de pérdida de autenticación de datos, ha demostrado ser de suma importancia tanto en mi campo laboral como en mi vida cotidiana. Esta experiencia ha arrojado luz sobre la crítica necesidad de comprender y abordar las vulnerabilidades de seguridad en línea en un mundo cada vez más digitalizado y conectado.

En mi campo laboral, donde la gestión de datos y la seguridad de la información son cruciales, esta actividad ha subrayado la importancia de contar con protocolos de seguridad sólidos y de estar alerta ante posibles amenazas cibernéticas. La identificación de vulnerabilidades, como la pérdida de autenticación, es esencial para proteger la confidencialidad y la integridad de los datos de los clientes y de la empresa en sí. Además, la comprensión de cómo se pueden explotar estas vulnerabilidades me ha proporcionado una visión valiosa para desarrollar estrategias de mitigación y mejorar nuestras prácticas de seguridad en línea.

En mi vida cotidiana, esta actividad me ha hecho más consciente de los riesgos a los que todos estamos expuestos en línea. Desde el robo de información personal hasta la suplantación de identidad, esta experiencia me ha recordado la importancia de mantener prácticas de seguridad sólidas, como el uso de contraseñas seguras y la autenticación de dos factores. Además, me ha motivado a educar a mis amigos y familiares sobre la importancia de la seguridad cibernética y cómo pueden protegerse en línea.

Bibliografía

OWASP, Top 10 – 2017 Los diez riesgos más críticos en Aplicaciones Web, creative commons, En línea: https://wiki.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf