



# **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.....	pág. 3
Descripción.....	pág. 4
Justificación.....	pág. 5
Ataque al sitio.....	pág. 6
Conclusión.....	pág. 13
Bibliografía.....	pág. 14

## **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**

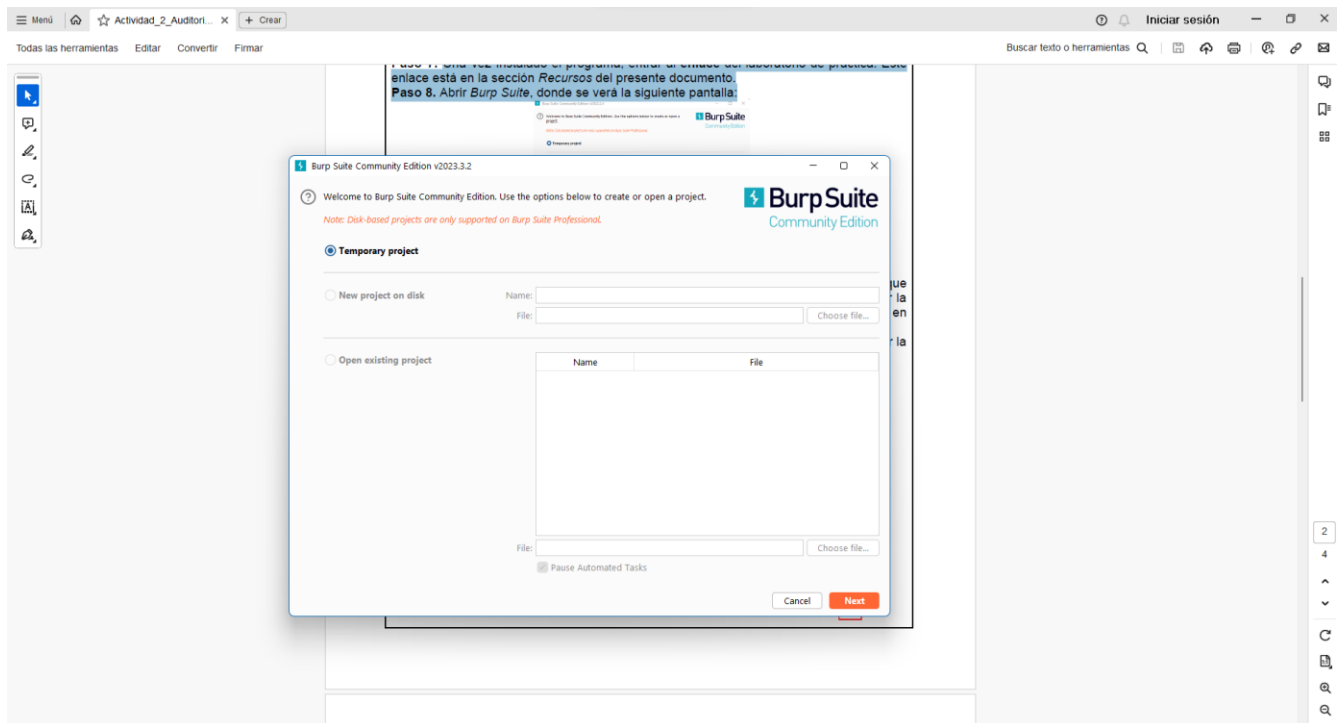
La realización de pruebas de este tipo de ataque, conocido como pérdida de autenticación de datos, se justifica por su importancia crítica en la evaluación y mejora de la seguridad en línea. Estas pruebas son esenciales debido a que ayudan a identificar y mitigar vulnerabilidades de seguridad en sistemas 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.

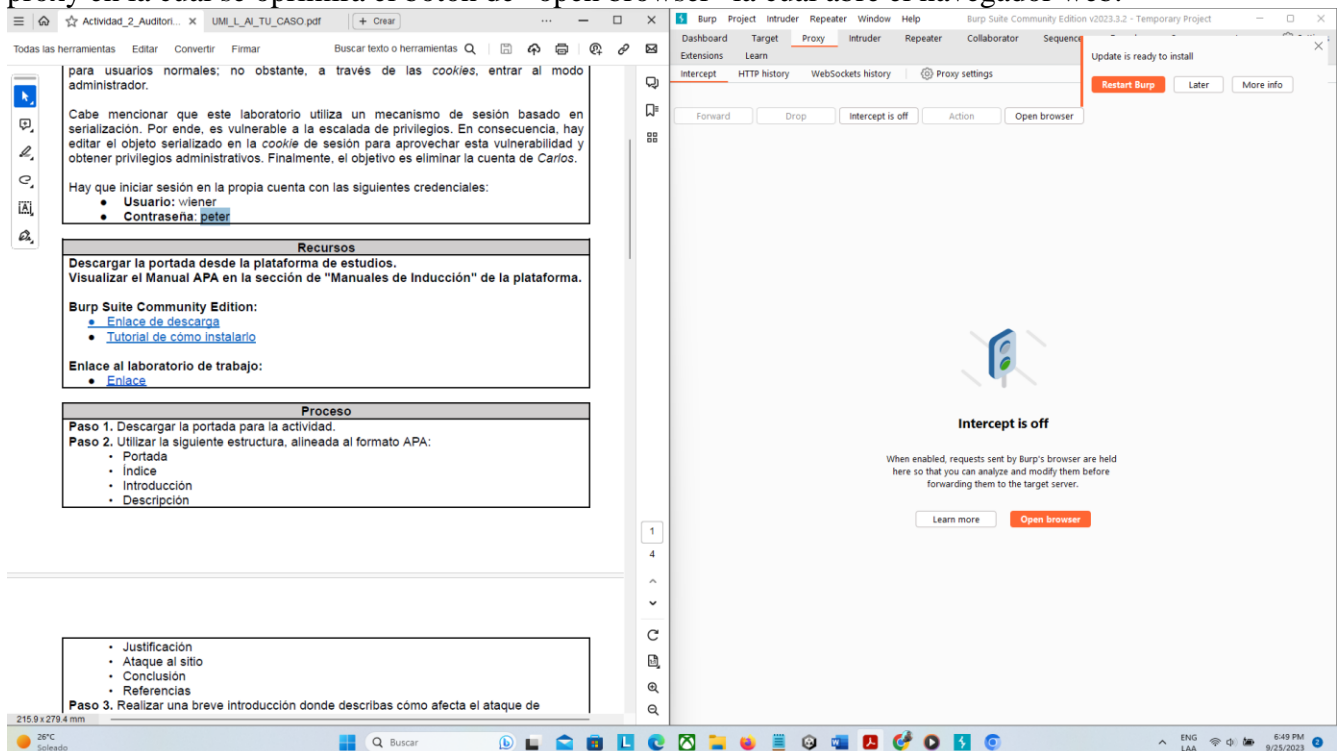
Las pruebas de pérdida de autenticación son esenciales para proteger la información confidencial, cumplir con regulaciones, mejorar la seguridad y preservar la confianza en línea en un mundo digital cada vez más interconectado y vulnerable a ataques cibernéticos.

## Ataque al sitio

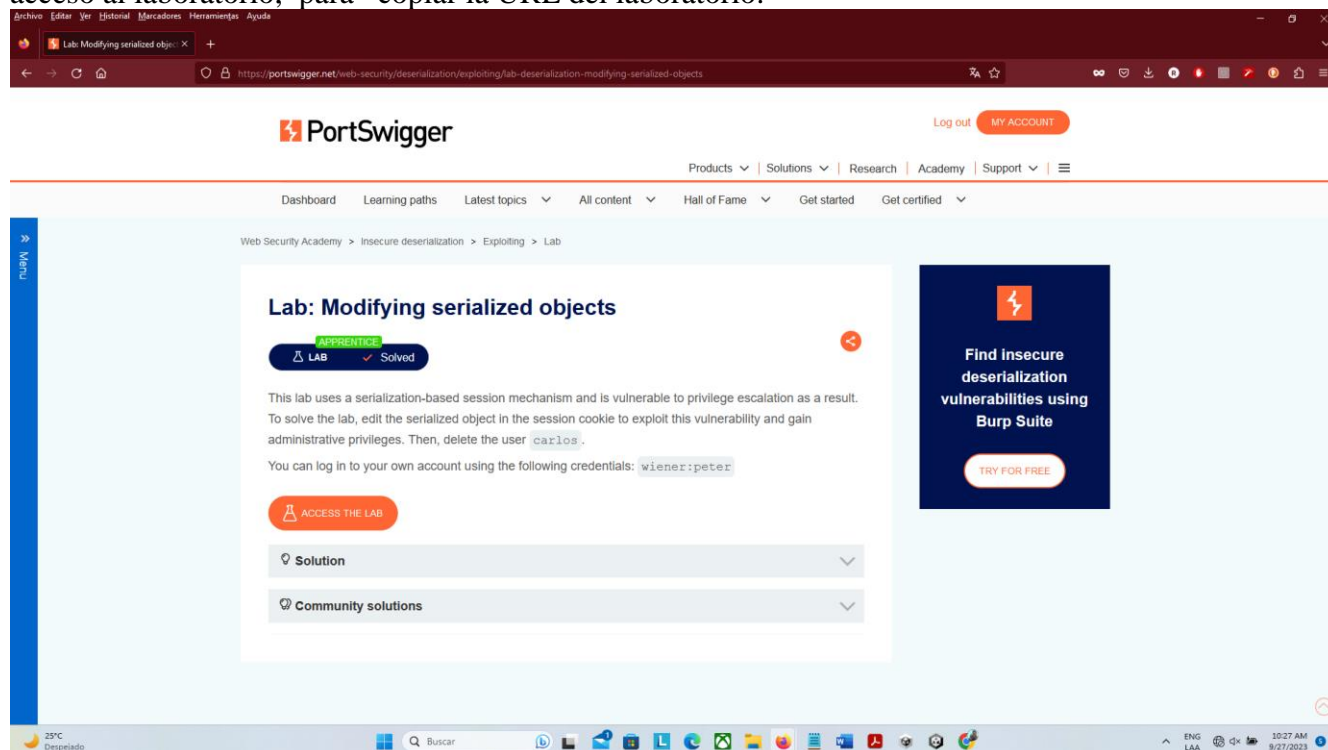
Primeramente para la práctica de esta actividad descargue el programa Burp Suite Community Edition, y luego en la página web Portswigger cree mi cuenta para poder realizar el ataque.



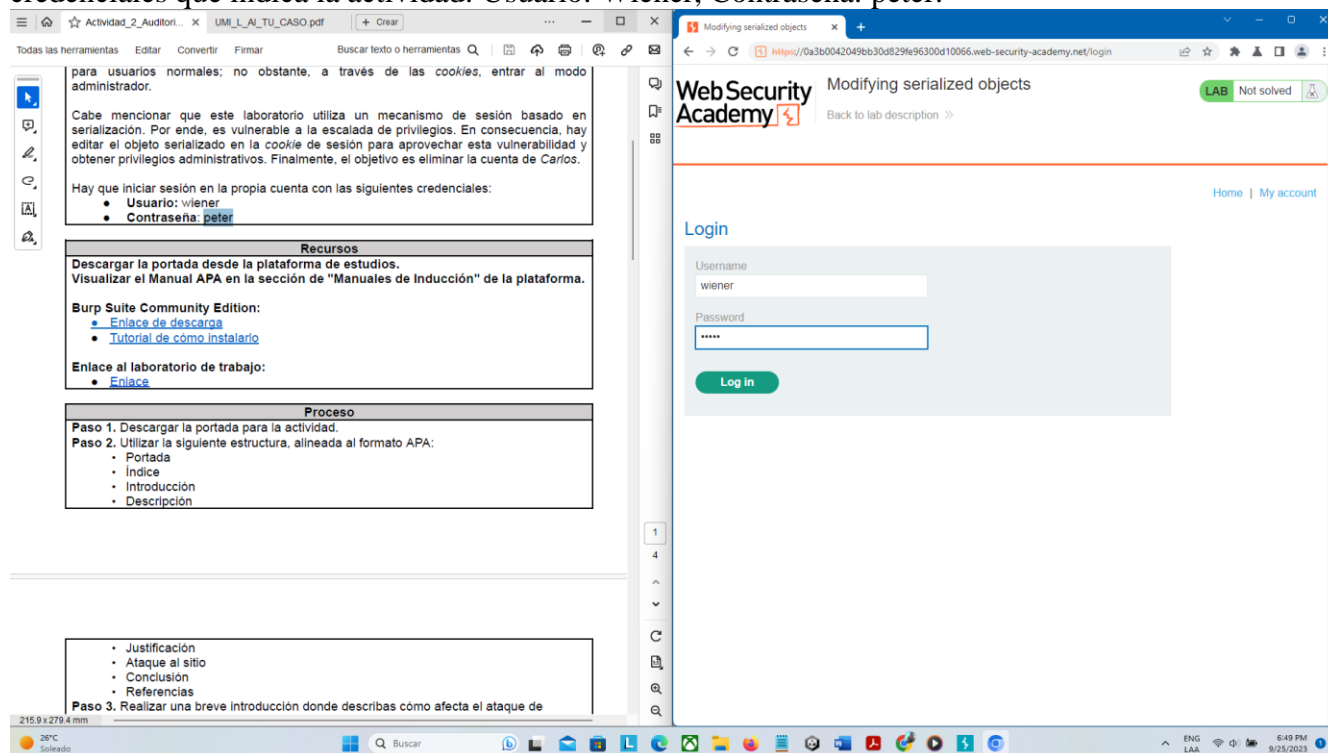
Posteriormente se ingresó al programa Burp suite con la configuración de default en la pestaña de proxy en la cual se oprimirá el botón de “open browser” la cual abre el navegador web.



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.

The screenshot shows the Burp Suite interface with the HTTP history tab active. A list of requests is displayed, with the POST request to /login selected. The request details are shown in the Inspector panel on the right, including the request body parameters and headers. The left panel shows a document titled 'Actividad\_2\_Auditor...' with a section for 'Formato de entrega' and 'Elementos de entrega'.

**Formato de entrega:**  
Plataforma de entrega: Plataforma de Estudios  
Formato de entrega: Documento PDF

**Elementos de entrega:**

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

The screenshot shows the Burp Suite interface with the Raw tab active for the selected POST request. The raw data of the request is displayed, and the session cookie is highlighted. The left panel shows the same document as before, but the 'Formato de entrega' section is now empty.

**Formato de entrega:**



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

The screenshot shows a web application interface on the left and the Burp Suite Decoder tool on the right. The web application displays a series of steps for a security exercise, including logging in as an administrator and modifying serialized objects. The Burp Suite Decoder is configured to decode the input as Text. The decoded output shows a JSON object with a 'b:0' value, indicating that the user is not an administrator.

**Web Application Interface:**

- Intercept is off** | **Action** | **Open Browser**
- Paso 15.** Es importante recordar que este tipo de ataque es **deserialización insegura**, por lo que es necesario obtener las cookies de la sesión para poder modificarlas.
- Paso 16.** Al ingresar al modo administrador a la página, se verá el siguiente menú:
- Users** | **Home** | **Admin panel** | **My account**
- wienner** - **Carlos**
- Acceder a la opción de **Admin Panel**, donde estarán los usuarios registrados en el sistema. Por ejemplo a los usuarios: **admin**, **wienner** (el que se inició sesión) y a **Carlos**, (usuario a eliminar según las instrucciones).
- Paso 17.** Al realizar la práctica de manera exitosa visualizará el siguiente cuadro:
- WebSecurity Academy** | **Modifying serialized objects** | **Submit** | **Back to lab description**
- Congratulations, you solved the lab!** | **Share your writeup** | **Continue writing**
- Nota.** Se recomienda revisar el video de la materia donde se realiza una prueba con este laboratorio.
- Paso 18.** Tomar capturas de pantalla del proceso realizado a lo largo de la práctica y adjuntarlas al documento en la sección **Ataque al sitio**. Además, describir los pasos realizados para entrar al modo administrador de la página.
- Paso 19.** Redactar una conclusión sobre la importancia de lo realizado en la actividad dentro de su campo laboral o vida cotidiana. (Mínimo 150 palabras), **Conclusión**
- Paso 20.** Adjuntar las referencias del material visitado para la realización de la actividad. **Referencia**
- Paso 21.** Guardar el archivo en formato PDF como: **NombreApellido\_A2**
- Formato de entrega:**  
Plataforma de entrega: Plataforma de Estudios  
Formato de entrega: Documento PDF
- Elementos de entrega:**

**Burp Suite Decoder:**

- Text** | **Hex**
- Decode as ...**
- Encode as ...**
- Hash ...**
- Smart decode**
- 0:4:"User":2;js:8;"username":s:6;"wienner":s:5;"admin":b:0}**

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 adminionistrador.

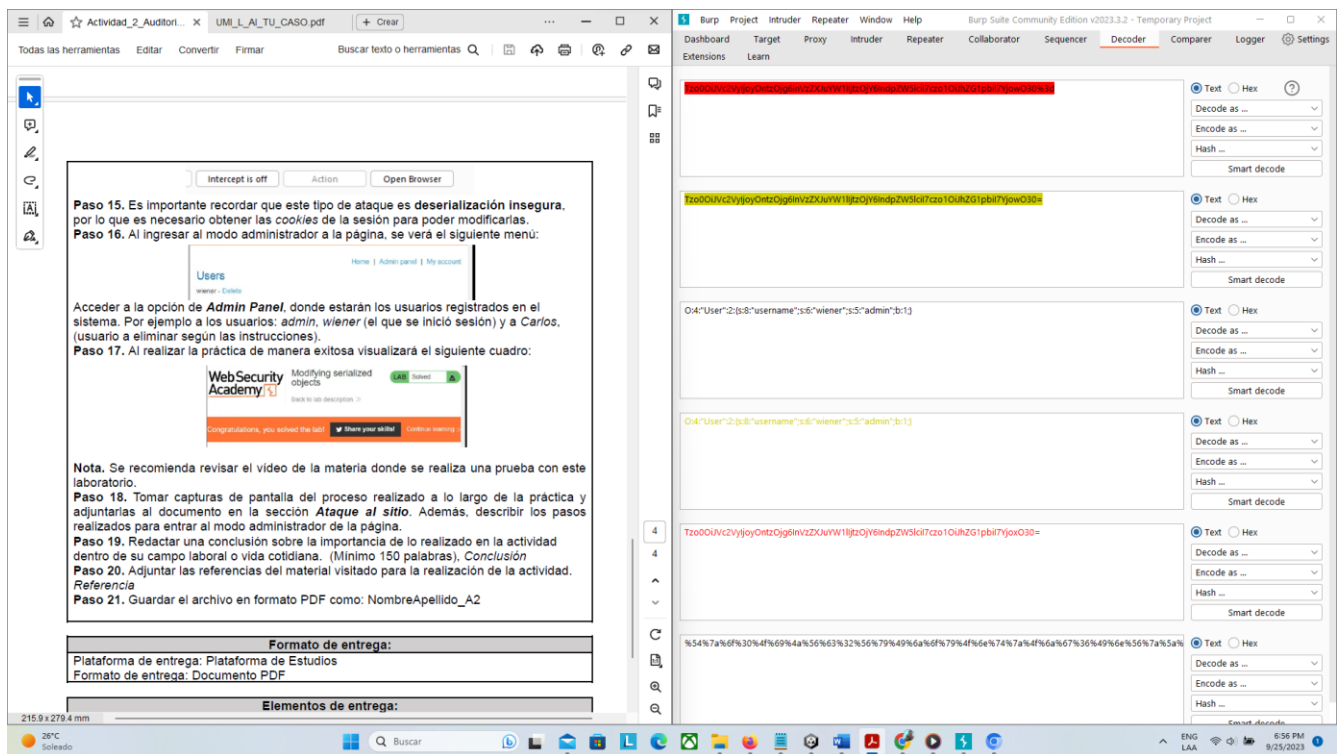
The screenshot shows the same web application interface on the left and the Burp Suite Decoder on the right. The decoded output now shows a JSON object with a 'b:1' value, indicating that the user is an administrator.

**Web Application Interface:**

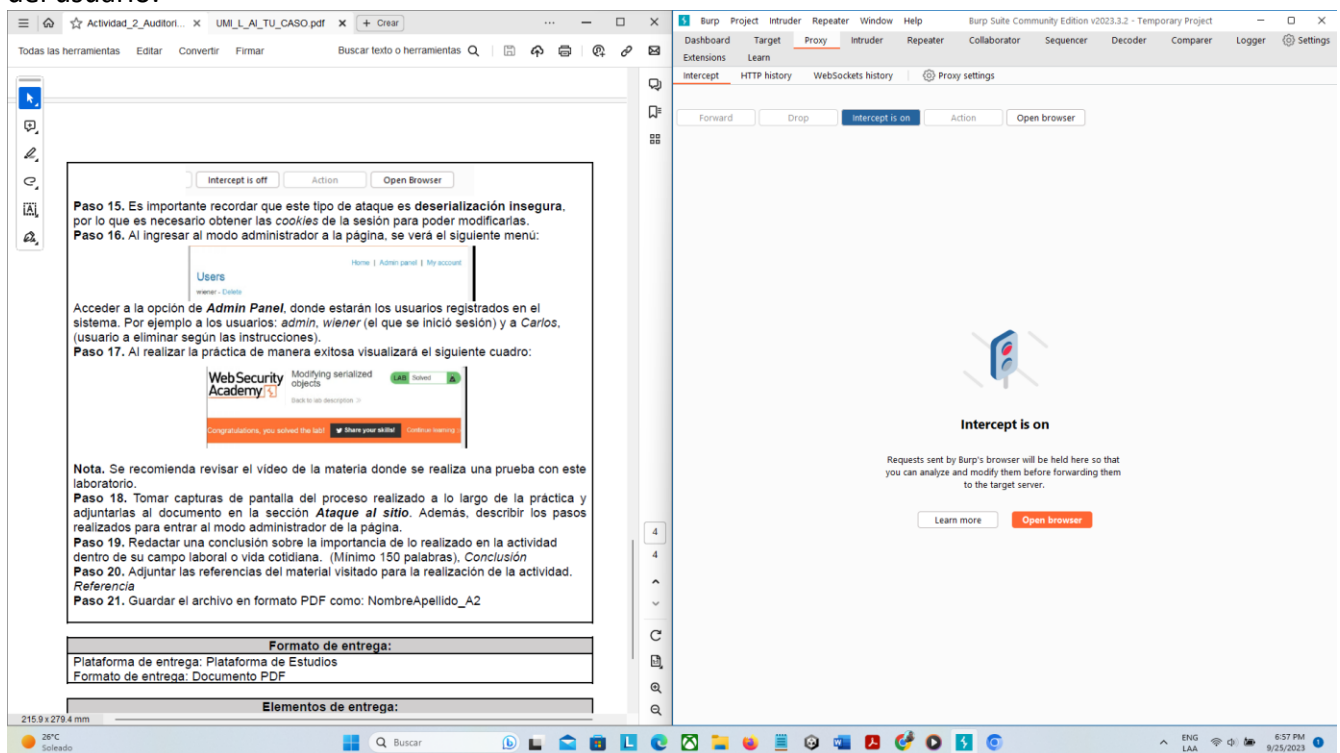
- Intercept is off** | **Action** | **Open Browser**
- Paso 15.** Es importante recordar que este tipo de ataque es **deserialización insegura**, por lo que es necesario obtener las cookies de la sesión para poder modificarlas.
- Paso 16.** Al ingresar al modo administrador a la página, se verá el siguiente menú:
- Users** | **Home** | **Admin panel** | **My account**
- wienner** - **Carlos**
- Acceder a la opción de **Admin Panel**, donde estarán los usuarios registrados en el sistema. Por ejemplo a los usuarios: **admin**, **wienner** (el que se inició sesión) y a **Carlos**, (usuario a eliminar según las instrucciones).
- Paso 17.** Al realizar la práctica de manera exitosa visualizará el siguiente cuadro:
- WebSecurity Academy** | **Modifying serialized objects** | **Submit** | **Back to lab description**
- Congratulations, you solved the lab!** | **Share your writeup** | **Continue writing**
- Nota.** Se recomienda revisar el video de la materia donde se realiza una prueba con este laboratorio.
- Paso 18.** Tomar capturas de pantalla del proceso realizado a lo largo de la práctica y adjuntarlas al documento en la sección **Ataque al sitio**. Además, describir los pasos realizados para entrar al modo administrador de la página.
- Paso 19.** Redactar una conclusión sobre la importancia de lo realizado en la actividad dentro de su campo laboral o vida cotidiana. (Mínimo 150 palabras), **Conclusión**
- Paso 20.** Adjuntar las referencias del material visitado para la realización de la actividad. **Referencia**
- Paso 21.** Guardar el archivo en formato PDF como: **NombreApellido\_A2**
- Formato de entrega:**  
Plataforma de entrega: Plataforma de Estudios  
Formato de entrega: Documento PDF
- Elementos de entrega:**

**Burp Suite Decoder:**

- Text** | **Hex**
- Decode as ...**
- Encode as ...**
- Hash ...**
- Smart decode**
- 0:4:"User":2;js:8;"username":s:6;"wienner":s:5;"admin":b:1}**



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



Después cambie la información de cookie session y la cambie por la que acabo de obtener con credenciales de administrador y me arrojó una nueva opción que es panel de administrador.

The image shows a PDF document on the left and a web browser on the right. The PDF document contains instructions for a lab titled "Modifying serialized objects". It includes steps 12 through 15, detailing the process of creating a new account, logging in, and using Burp Suite to intercept and modify session cookies. The web browser shows the WebSecurity Academy interface, specifically the "Modifying serialized objects" lab page. The page displays the user's account information, including the username "wiener" and an email field. The lab status is "Not solved".

**Paso 12.** Una vez dentro de la página del laboratorio se verá la siguiente pantalla:

**Lab: Modifying serialized objects**

Para poder realizar la práctica en el laboratorio, es importante generar una nueva cuenta en PortSwigger, caso contrario, no se podrá acceder a la práctica, y pedirá que se inicie sesión o crear una nueva cuenta.

Una vez creada la cuenta e iniciado sesión, entrar al laboratorio de práctica. Leer detenidamente las instrucciones que se dan en la sección *Contextualización*. Esta será la página que se debe atacar para entrar al modo administrador.

**Paso 13.** Iniciar sesión en la opción *My Account* con las credenciales proporcionadas. Estas son:

- Usuario: wiener
- Contraseña: Peter

**Paso 14.** Vuelve a *Burp* y da clic en el botón *Intercept is off*. Con esto, se encenderá el interceptador para captar todas las salidas de la página:

**Paso 15.** Es importante recordar que este tipo de ataque es *deserialización insegura*.

**WebSecurity Academy** Modifying serialized objects LAB Not solved

Home | Admin panel | My account | Log out

**My Account**

Your username is: wiener

Email

Update email

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.

The image shows a PDF document on the left and a web browser on the right. The PDF document contains instructions for a lab titled "Modifying serialized objects". It includes steps 17 through 21, detailing the process of accessing the Admin Panel, deleting users, and submitting a report. The web browser shows the WebSecurity Academy interface, specifically the "Modifying serialized objects" lab page. The page displays the user's account information, including the username "wiener" and a list of users: "wiener" and "carlos". The lab status is "Not solved".

**Paso 17.** Al realizar la práctica de manera exitosa visualizará el siguiente cuadro:

**WebSecurity Academy** Modifying serialized objects LAB Not solved

**Nota.** Se recomienda revisar el video de la materia donde se realiza una prueba con este laboratorio.

**Paso 18.** Tomar capturas de pantalla del proceso realizado a lo largo de la práctica y adjuntarlas al documento en la sección *Ataque al sitio*. Además, describir los pasos realizados para entrar al modo administrador de la página.

**Paso 19.** Redactar una conclusión sobre la importancia de lo realizado en la actividad dentro de su campo laboral o vida cotidiana. (Mínimo 150 palabras). *Conclusión*

**Paso 20.** Adjuntar las referencias del material visitado para la realización de la actividad. *Referencia*

**Paso 21.** Guardar el archivo en formato PDF como: NombreApellido\_A2

**Formato de entrega:**

Plataforma de entrega: Plataforma de Estudios

Formato de entrega: Documento PDF

**Elementos de entrega:**

Documento PDF: NombreApellido\_A2

Agregar el documento PDF de las actividades en el portafolio GitHub.

**WebSecurity Academy** Modifying serialized objects LAB Not solved

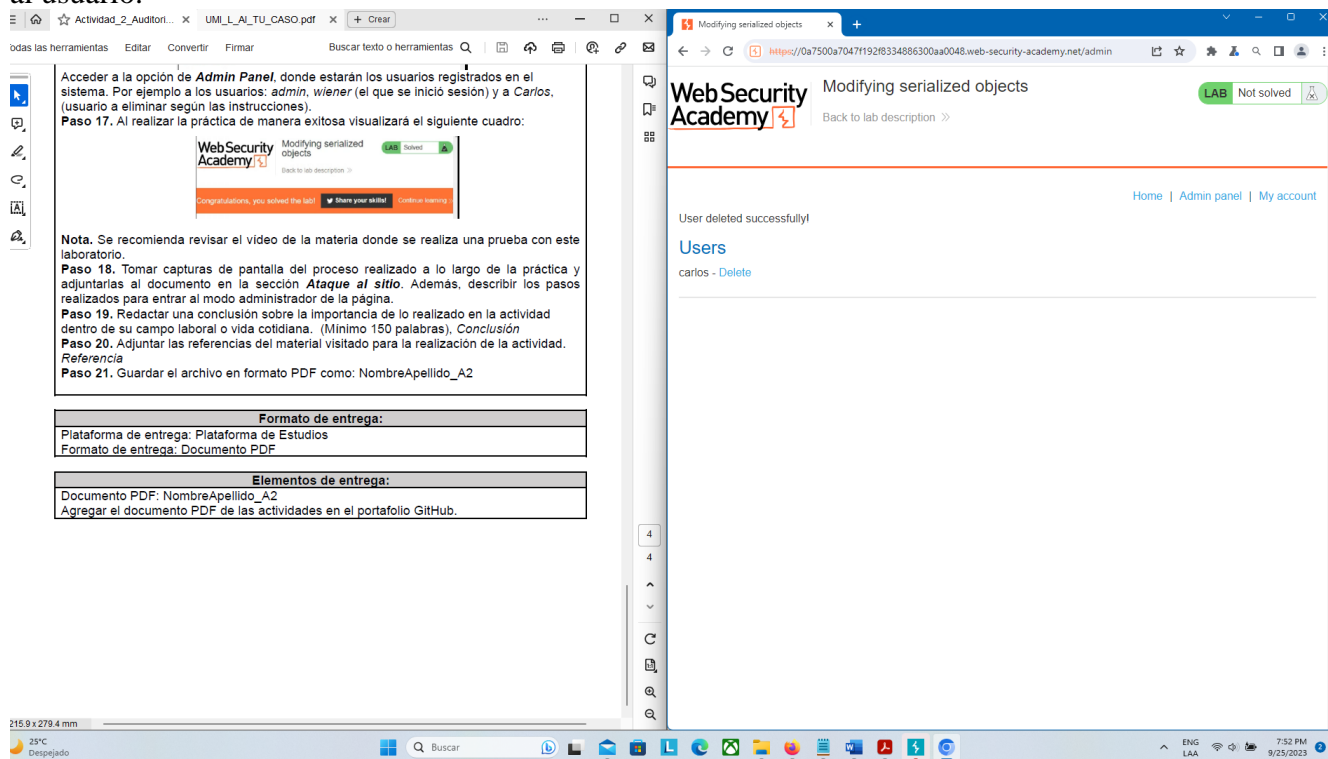
Home | Admin panel | My account

**Users**

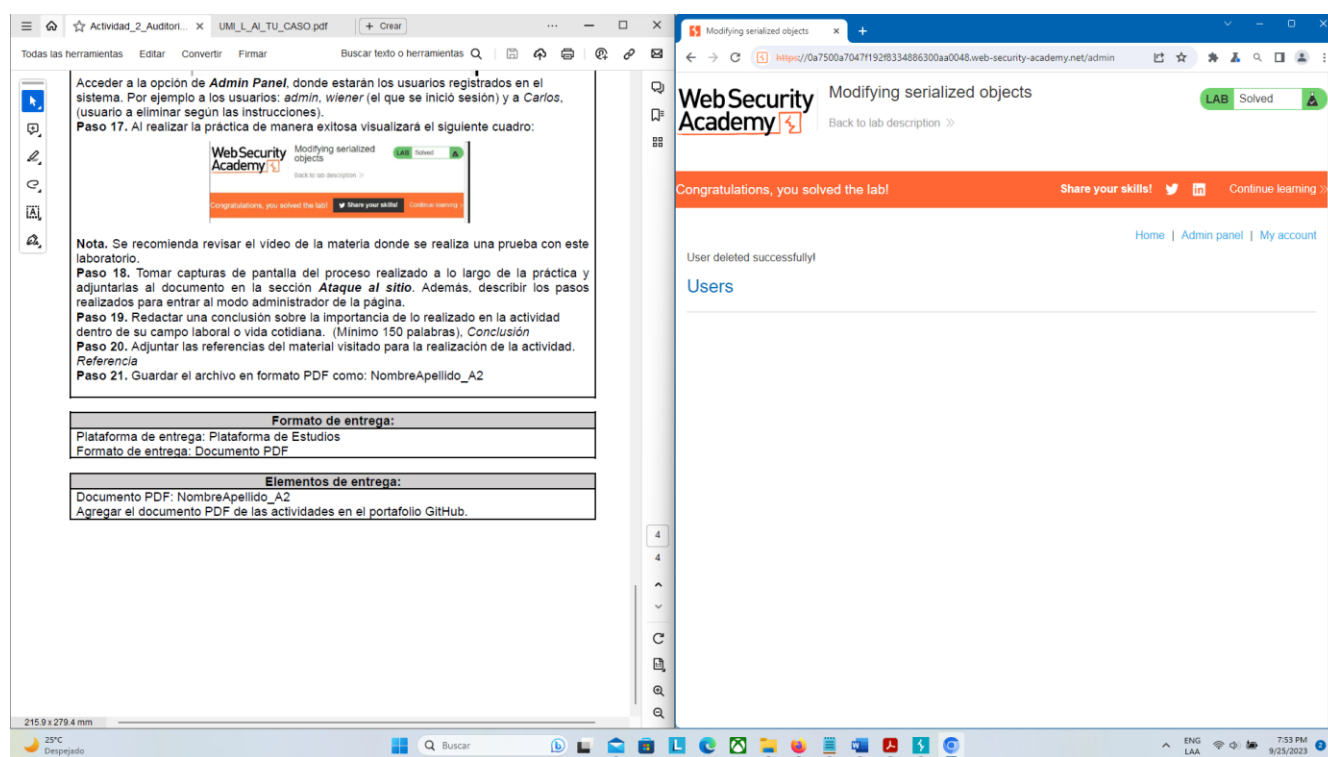
wiener - Delete

carlos - Delete

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 arrojó 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>