

Ingeniería en Desarrollo de Software

Actividad: Número 2.

Nombre de la Actividad: Deserialización insegura.

Nombre del Curso: Auditoria informática.

Tutor: Jessica Hernández Romero.

Alumno: Omar Juárez Carmona.

Fecha: 06 – Octubre – 2023.

INDICE

| | |
|------------------------------------|----|
| Contextualización y actividad..... | 3 |
| Introducción..... | 4 |
| Descripción..... | 5 |
| Justificación..... | 8 |
| Ataque al sitio..... | 10 |
| Conclusión..... | 18 |
| Referencias y link..... | 19 |

CONTEXTUALIZACION Y ACTIVIDAD

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

INTRODUCCION

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

La pérdida de autenticación puede tener consecuencias graves para los usuarios de Internet. Algunas de las formas en que los ataques de pérdida de autenticación pueden afectar a los usuarios incluyen:

- Reutilización de credenciales conocidas.

Si un atacante tiene acceso a una lista de pares de usuario y contraseña válidos, puede intentar iniciar sesión en varias cuentas utilizando esas credenciales. Esto puede llevar a la suplantación de identidad y al acceso no autorizado a información personal o sensible.

- Ataques de fuerza bruta.

Los atacantes pueden intentar adivinar contraseñas utilizando programas automatizados que prueban diferentes combinaciones hasta encontrar la correcta. Esto puede comprometer las cuentas y permitir el acceso no autorizado.

- Contraseñas débiles o por defecto.

Si una aplicación permite el uso de contraseñas débiles o por defecto, los atacantes pueden aprovechar esto para acceder a las cuentas de los usuarios.

- Procesos débiles para recuperación de credenciales.

Si una aplicación no tiene procesos efectivos para recuperar contraseñas olvidadas o credenciales perdidas, los atacantes pueden aprovechar esto para acceder a las cuentas.

- Almacenamiento inseguro de contraseñas.

Si las contraseñas se almacenan en texto plano o utilizando funciones de hash débiles, los atacantes pueden obtener acceso a las contraseñas y utilizarlas para acceder a las cuentas.

- Falta de autenticación multi-factor.

La falta de autenticación multi-factor o la implementación ineficaz de ella pueden hacer que las cuentas sean más vulnerables a ataques.

- Exposición del identificador de sesión.

Si el identificador de sesión se expone en la URL, los atacantes pueden obtener acceso no autorizado a las cuentas.

- Reutilización del identificador de sesión.

Si el identificador de sesión se reutiliza después del inicio de sesión, los atacantes pueden obtener acceso no autorizado a las cuentas.

- No invalidación adecuada de identificadores de sesión.

Si los identificadores de sesión no se invalidan correctamente, los atacantes pueden utilizar identificadores antiguos para acceder a las cuentas.

Es importante tener en cuenta que estas son solo algunas formas en que los ataques de pérdida de autenticación pueden afectar a los usuarios. Para protegerse contra estos ataques, se recomienda implementar la autenticación multi-factor siempre que sea posible, utilizar contraseñas seguras y únicas, y asegurarse de que las aplicaciones sigan prácticas seguras para el almacenamiento y gestión de credenciales.

DESCRIPCION

La auditoría informática involucra las funciones de inicio de sesión y registro de usuarios a la conexión de base de datos, así como la utilización de la herramienta de trabajo de software Burp Suite Community Edition.

Debemos de saber que la deserialización insegura se clasifica como la vulnerabilidad número ocho en la lista de OWASP-Top 10. La deserialización insegura es una vulnerabilidad que ocurre cuando los datos no confiables se usan para abusar de la lógica de una aplicación, infligir un ataque de denegación de servicio (DoS) o incluso ejecutar código arbitrario.

Para entender esta vulnerabilidad, es necesario entender el proceso de serialización. La serialización es el proceso de traducir estructuras de datos o estados de objetos a un formato que puede almacenarse y reconstruirse con posterioridad. La deserialización, por otro lado, es lo opuesto a la serialización, es decir, transformar los datos serializados provenientes de un archivo, secuencia o socket de red en un objeto. Es en este último proceso donde reside la vulnerabilidad.

La mayoría de los lenguajes de programación ofrecen la posibilidad de personalizar los procesos de deserialización. Desafortunadamente, con frecuencia es posible que un atacante abuse de estas características de deserialización cuando la aplicación deserializa datos no confiables que controla el atacante. Los ataques de deserialización inseguros permiten que un atacante realice ataques de denegación de servicio (DoS), omisiones de autenticación y ataques de ejecución remota de código.

El “Instituto Nacional de Estándares y Tecnología” perteneciente al Departamento de Comercio de Los Estados Unidos incluye en su base de datos varias vulnerabilidades y exposiciones comunes relacionadas a deserialización insegura, algunas de estas son:

CVE-2017-9805 – Deserialización insegura que afecta al complemento REST en Apache Struts 2.1.1 en versiones 2.3.x antes de 2.3.34 y 2.5.x antes de 2.5.13. Esta vulnerabilidad usa un XStreamHandler con una instancia de XStream para la deserialización sin ningún tipo de filtrado, lo que puede conducir a la EJECUCIÓN REMOTA DE COMANDOS.

CVE-2018-1851 – Deserialización insegura que afecta el servicio de cola de impresión en Microsoft Windows XP SP2 y SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2 y R2 SP1, y Windows 7 Gold y SP1 permitiendo a los atacantes remotos la EJECUCIÓN REMOTA DE COMANDOS.

CVE-2018-6496 – Deserialización insegura que genera la FALSIFICACIÓN REMOTA DE SOLICITUDES ENTRE SITIOS afectando a los buscadores de los servidores UCMBD versiones 4.10, 4.11, 4.12, 4.13, 4.14, 4.15, y 4.15.1.

CVE-2018-6497 – Deserialización insegura que afecta a servidores UCMBD versión DDM Content Pack V 10.20, 10.21, 10.22, 10.22 CUP7, 10.30, 10.31, 10.32, 10.33, 10.33 CUP2, 11.0 y servidores CMS versión 2018.05. – EJECUCIÓN REMOTA DE COMANDOS.

CVE-2018-7489 – Deserialización insegura que afecta el complemento FasterXML jackson-databind antes de la versión 2.7.9.3, 2.8.x, antes de la versión 2.8.11.1 y 2.9.x y antes de la versión 2.9.5 – EJECUCIÓN REMOTA DE COMANDOS.

Esperamos aprender en esta 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 y eliminar la cuenta de Carlos con un usuario y contraseña proporcionada.

JUSTIFICACION

Burp Suite es una plataforma capaz de llevar a cabo las auditorías de seguridad de una organización con el objetivo de evitar ataques de software maliciosos.

Ahora bien, en este apartado analizaremos con mayor profundidad que se puede hacer con Burp Suite, qué herramientas ofrece esta plataforma para el cuidado de la ciber seguridad de una empresa.

En primer lugar, su función básica es la de realizar pruebas de exploración y escanear vulnerabilidades que puedan llegar a tener las aplicaciones web. El escaneo de vulnerabilidades se puede llevar a cabo de forma automatizada, o a través de un método avanzado de forma manual. Una vez que se llevó adelante el escaneo y la exploración, Burp Suite ofrece un análisis claro y conciso de las vulnerabilidades y agrega algunas recomendaciones. Recordemos que el sentido de encontrar las vulnerabilidades es poder resolverlas antes de que un delincuente cibernético se aproveche de ellas. Además de presentar las vulnerabilidades y dar recomendaciones, también informa los payloads que se utilizaron.

Cómo mencionamos previamente, Burp Suite es una plataforma que integra la posibilidad de realizar pruebas de seguridad y de atacar aplicaciones web con el objetivo de fortalecer los sistemas de seguridad. Se trata de un complemento ideal para todo el proceso de prueba. El mapeo inicial, el análisis de la superficie de ataque de la aplicación y el descubrimiento y explotación de las vulnerabilidades de la aplicación hacen que Burp Suite sea reconocida como una herramienta muy efectiva para las auditorías.

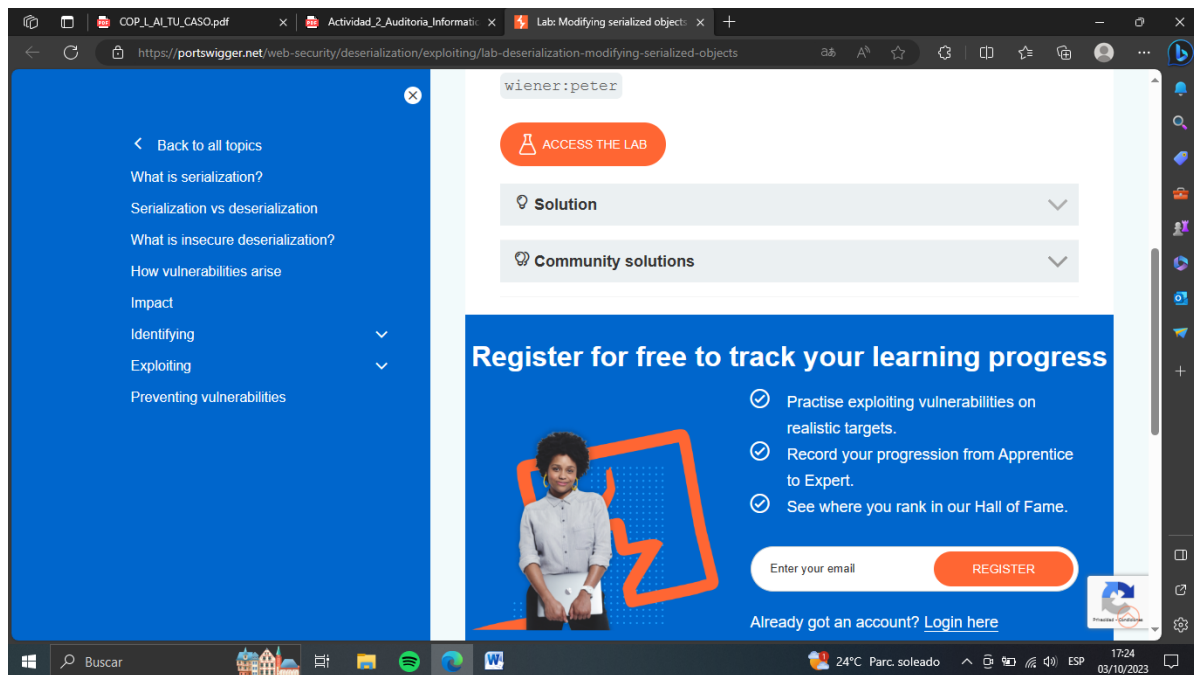
En general, se utiliza también para testear modificaciones pequeñas que puedan afectar la seguridad. Es la automatización de la modificación de las peticiones lo que hace a la velocidad del proceso. Una cuestión a la que ya hemos hecho referencia es la tarea que tiene Burp Suite como intermediario en el tráfico del navegador

web. Con el proxy entre el navegador y la red puede interceptar las peticiones que se realicen e inspeccionar el tráfico. Con Burp Suite además es posible conectarse a las aplicaciones web a través de distintos métodos que ofrece la propia plataforma. Por otro lado, Burp Suite consta de una ventaja considerable que permite ampliar el campo de acción de quienes la utilizan. Nos referimos a extender, una de sus herramientas que posibilita la instalación de una gran cantidad de extensiones. De esta manera, es posible ampliar las funcionalidades de la plataforma. Se trata de una herramienta que le da mucho potencial a la plataforma. Existen dos formas de instalar una extensión, las cuales describiremos más adelante. Otra de las herramientas que ofrece Burp Suite es Burp Intruder. Burp Intruder se relaciona con la función de realizar ataques que ofrece Burp Suite. Con ella se pueden realizar ataques programados que pongan a prueba nuestro sistema. Si bien es una herramienta que está disponible en la versión gratuita de Burp Suite, ofrece su máximo potencial con Burp Professional, la versión paga. Cuando nos referimos a que se puede hacer con Burp Suite, no podemos dejar de mencionar su herramienta target. Esta última, disponible en Burp Free, permite fijar un objetivo y construir un SiteMap a partir de él. Como bien marcamos al principio, Burp Suite puede realizar ciertas acciones de manera automatizada. Recordemos que su principal funcionalidad es la de encontrar vulnerabilidades en las aplicaciones web para evitar que sufran intromisiones maliciosas. Es para eso, en particular, que existe la herramienta que los desarrolladores han llamado spider. Se trata de un instrumento por el cual es posible inspeccionar las páginas web y recursos de la aplicación de forma automática. Además, con la herramienta repeater, es posible controlar de forma manual las peticiones HTTP interceptadas por el proxy, cambiar parámetros, cabeceras y reenviarlas nuevamente.

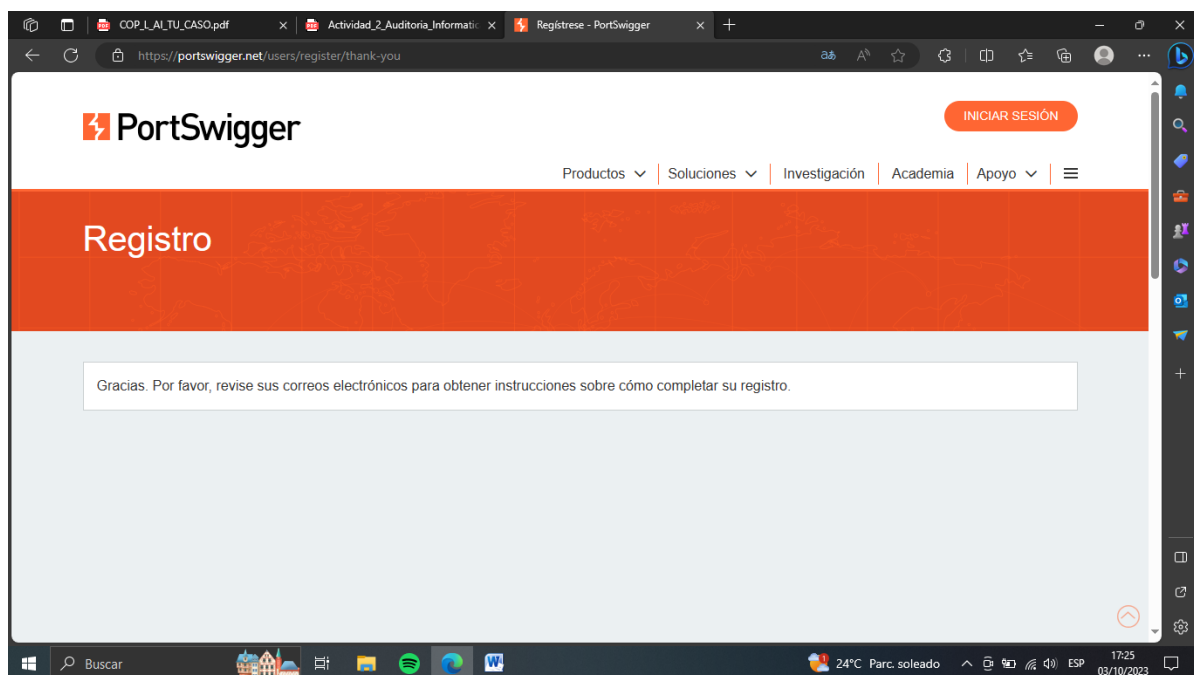
Por estas y más razones es recomendable utilizare este software para una auditoria informática. Sin más preámbulo, continuemos con nuestra actividad.

ATAQUE AL SITIO

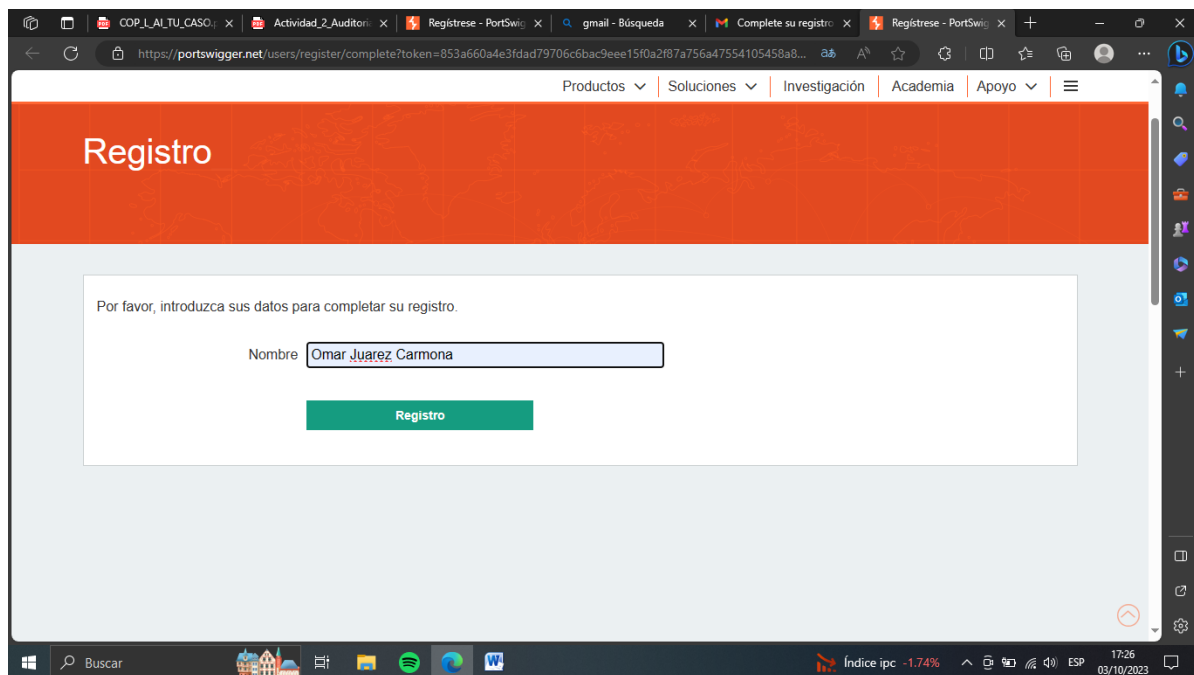
Acceso al laboratorio



Registro en PortSwigger

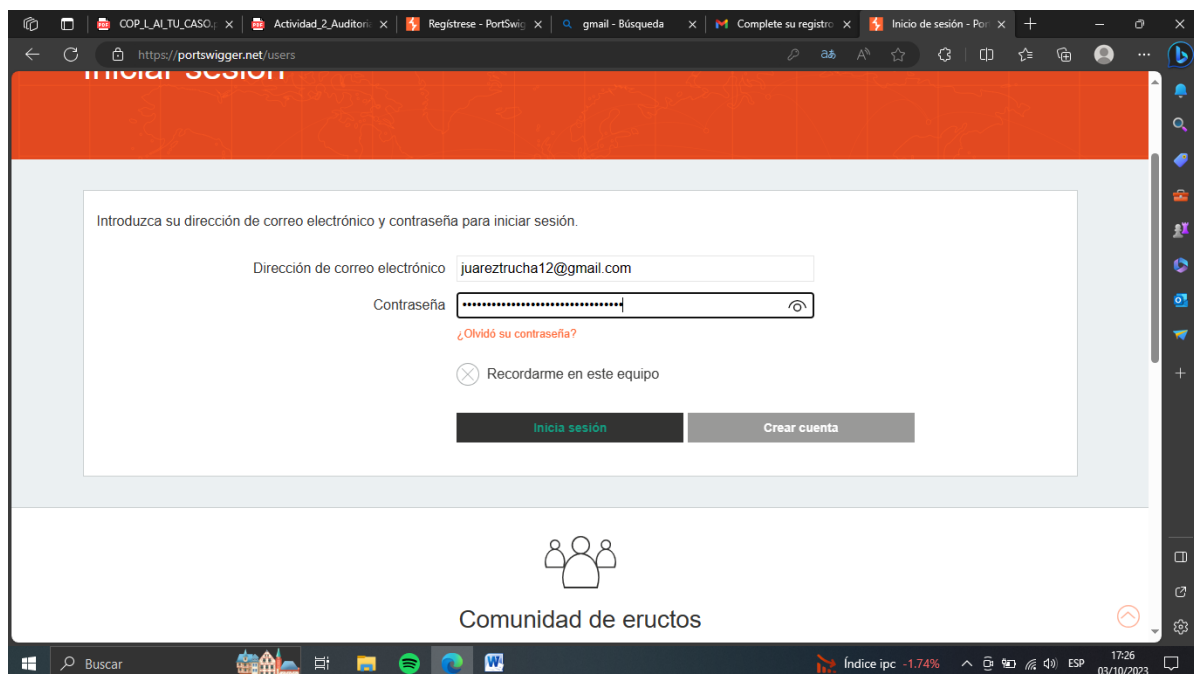


Registro con usuario en PortSwigger



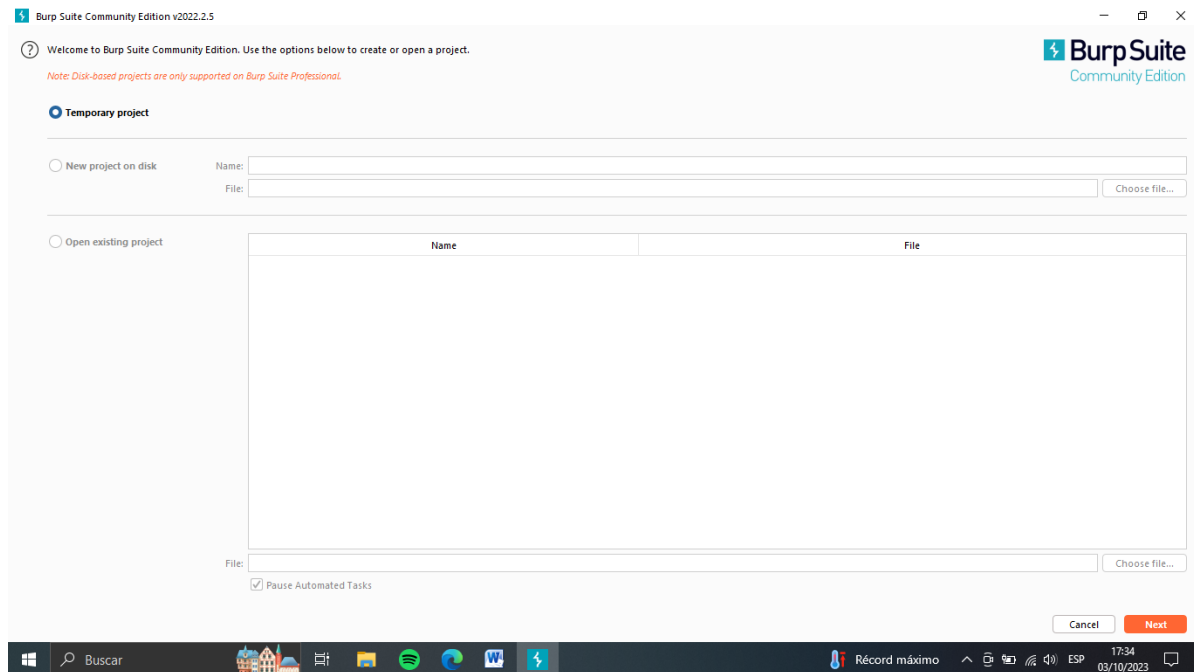
The screenshot shows a web browser window with the URL <https://portswigger.net/users/register/complete?token=853a660a4e3fdad79706c6bac9eee15f0a2f87a756a47554105458a8...>. The page has an orange header with the word "Registro" in white. Below the header, there is a white box containing the text "Por favor, introduzca sus datos para completar su registro." and a form with a label "Nombre" and a text input field containing "Omar Juárez Carmona". Below the input field is a green button labeled "Registro". The browser's taskbar at the bottom shows the Windows logo, a search bar, and several application icons. The system tray on the right shows the date and time as 17:26 on 03/10/2023.

Registro con clave de parte de PortSwigger

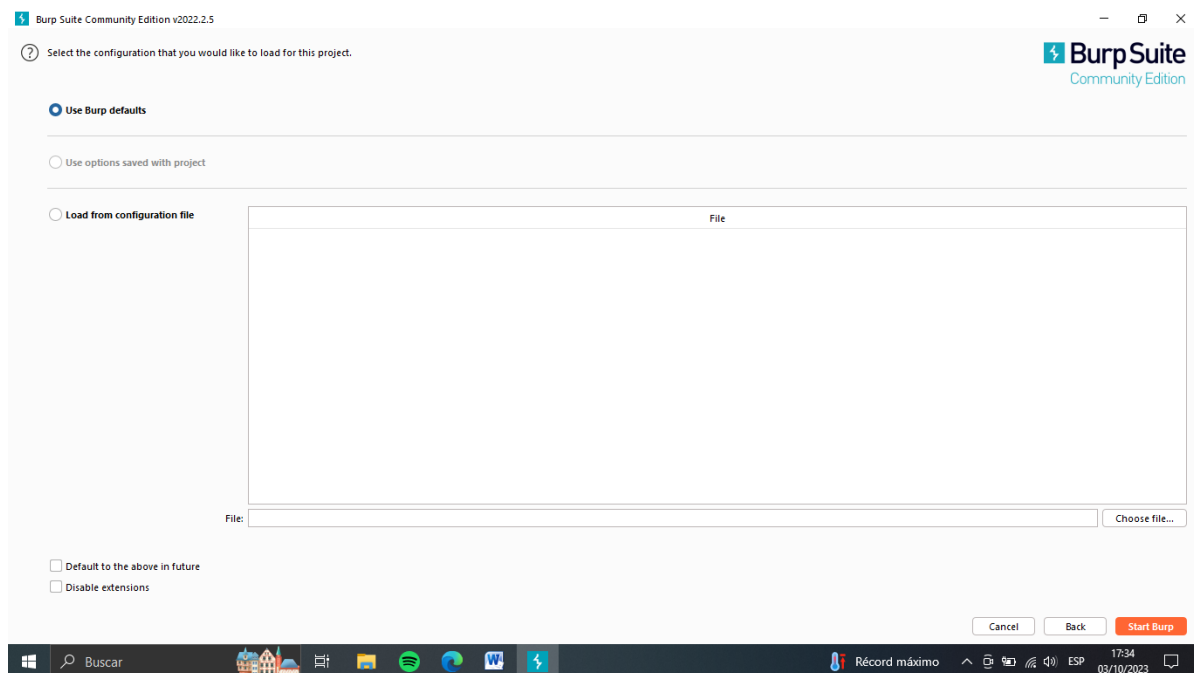


The screenshot shows a web browser window with the URL <https://portswigger.net/users>. The page has an orange header with the text "Inicio de sesión" in white. Below the header, there is a white box containing the text "Introduzca su dirección de correo electrónico y contraseña para iniciar sesión." and a form with two input fields: "Dirección de correo electrónico" containing "juareztrucha12@gmail.com" and "Contraseña" containing a masked password. Below the password field is a link that says "¿Olvidó su contraseña?". There is also a checkbox labeled "Recordarme en este equipo" which is currently unchecked. At the bottom of the form are two buttons: "Iniciar sesión" (green) and "Crear cuenta" (grey). Below the form, there is a logo consisting of three stylized figures and the text "Comunidad de eructos". The browser's taskbar at the bottom shows the Windows logo, a search bar, and several application icons. The system tray on the right shows the date and time as 17:26 on 03/10/2023.

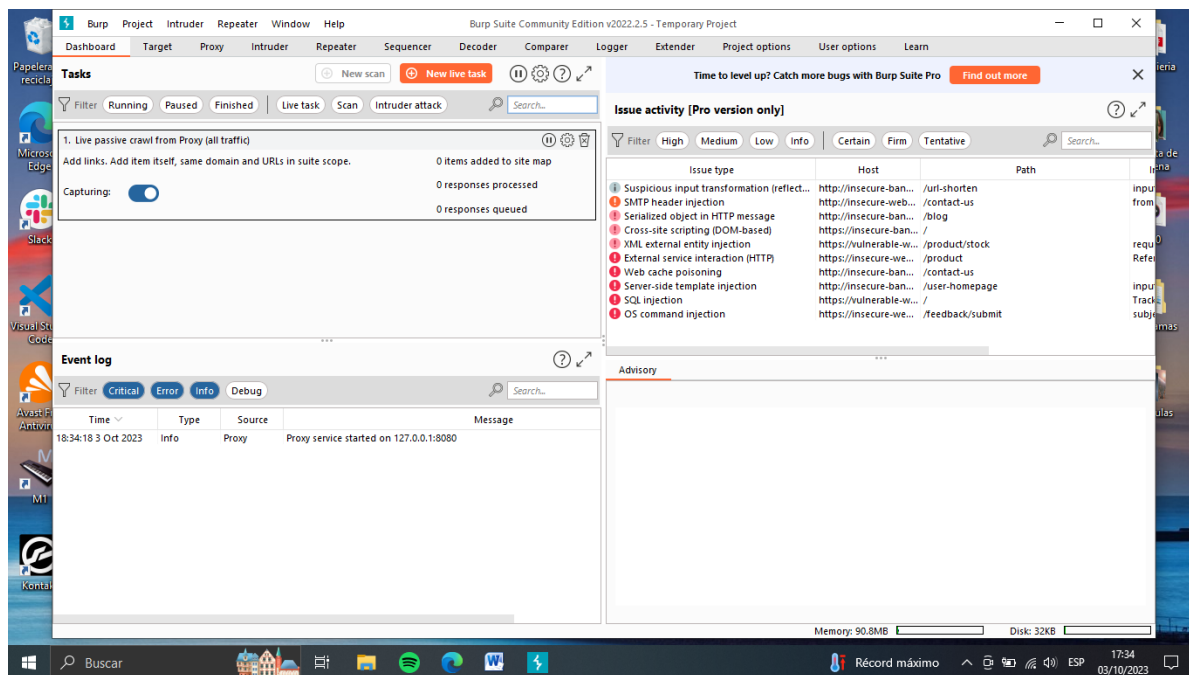
Accediendo a BurpSuite



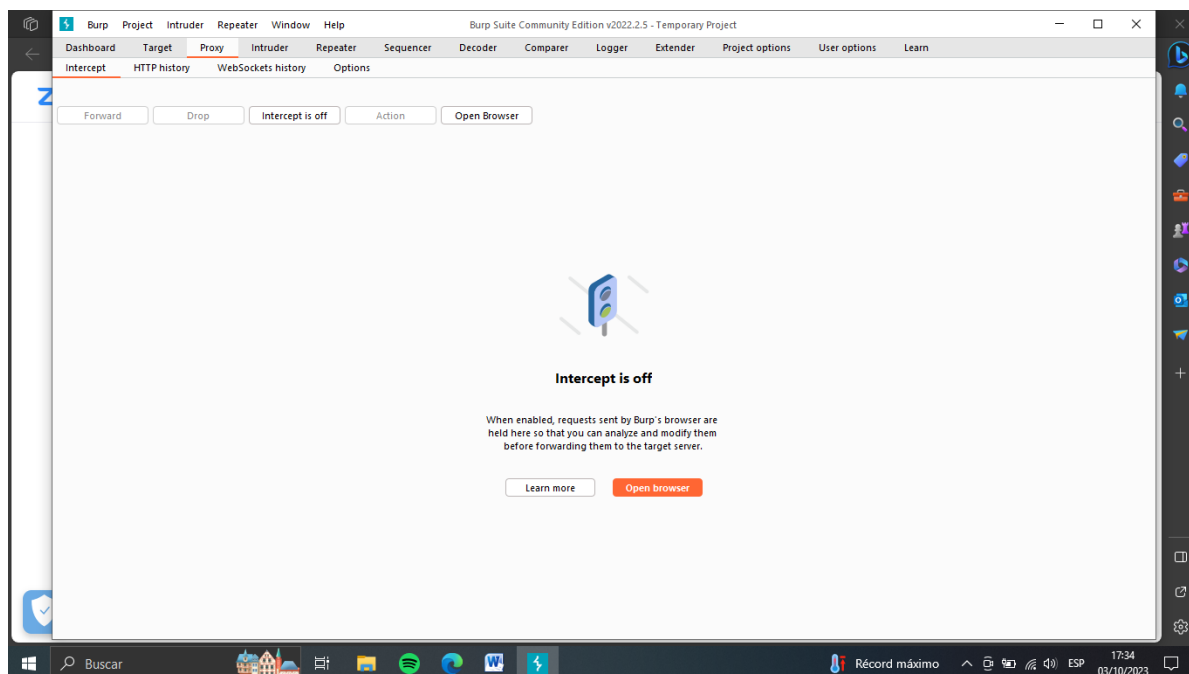
Accediendo a BurpSuite



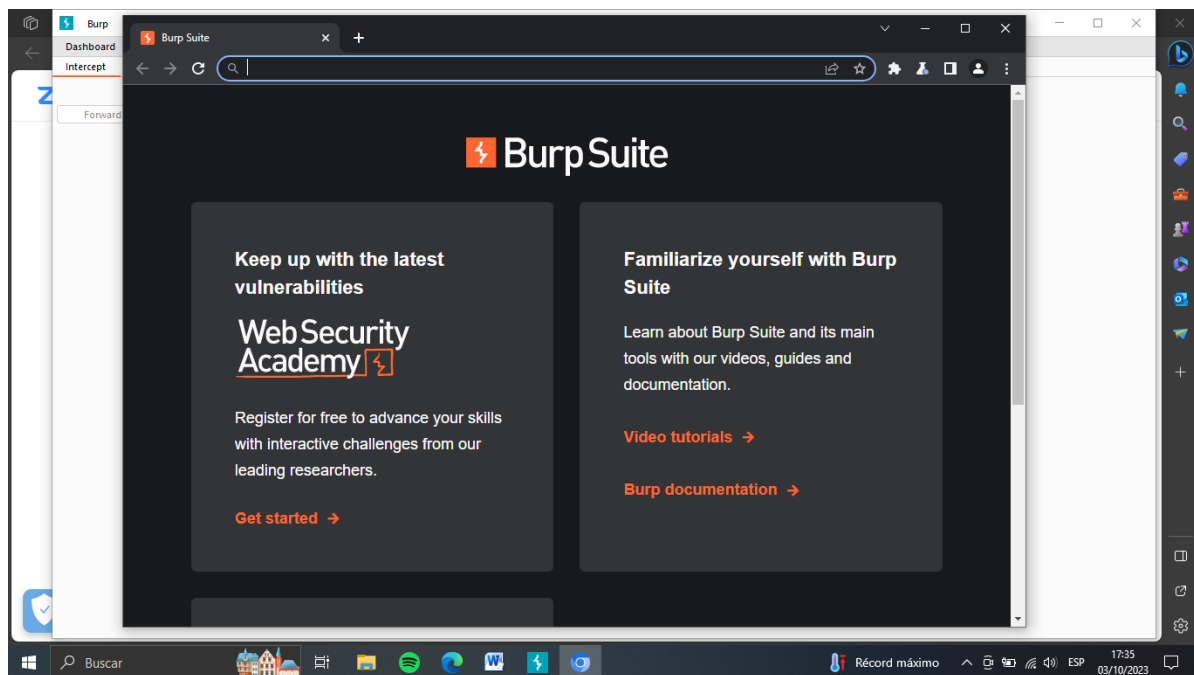
Página principal de Burp Suite



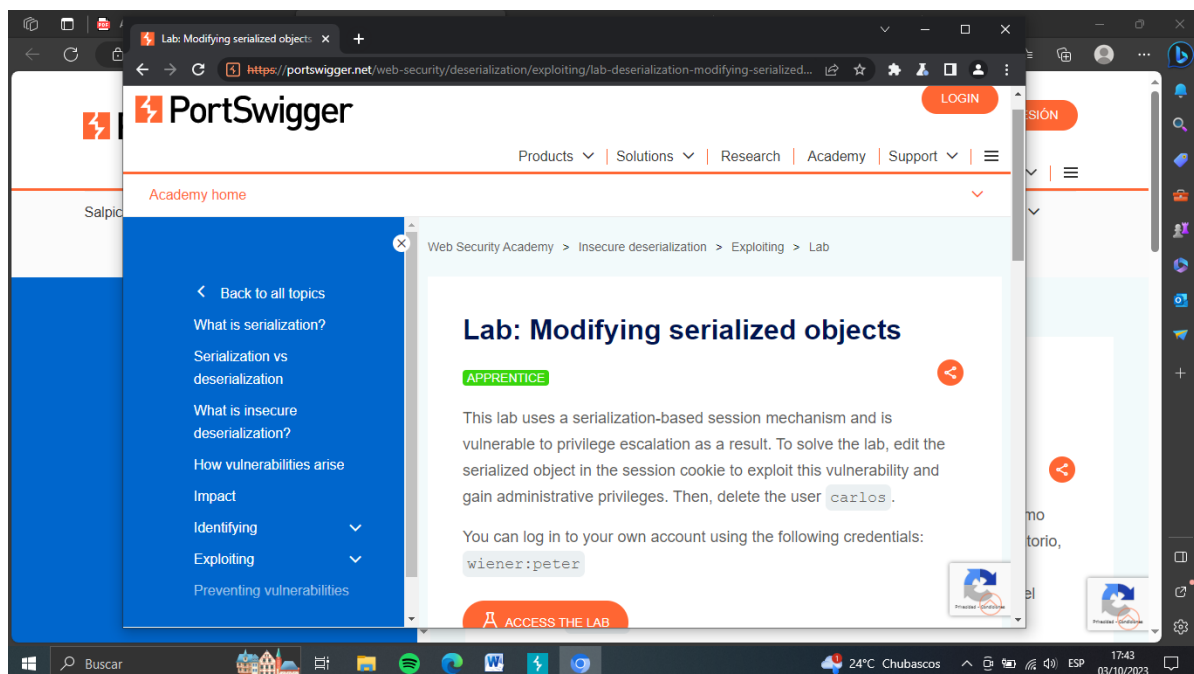
Accediendo al Proxy dentro de Burp Suite



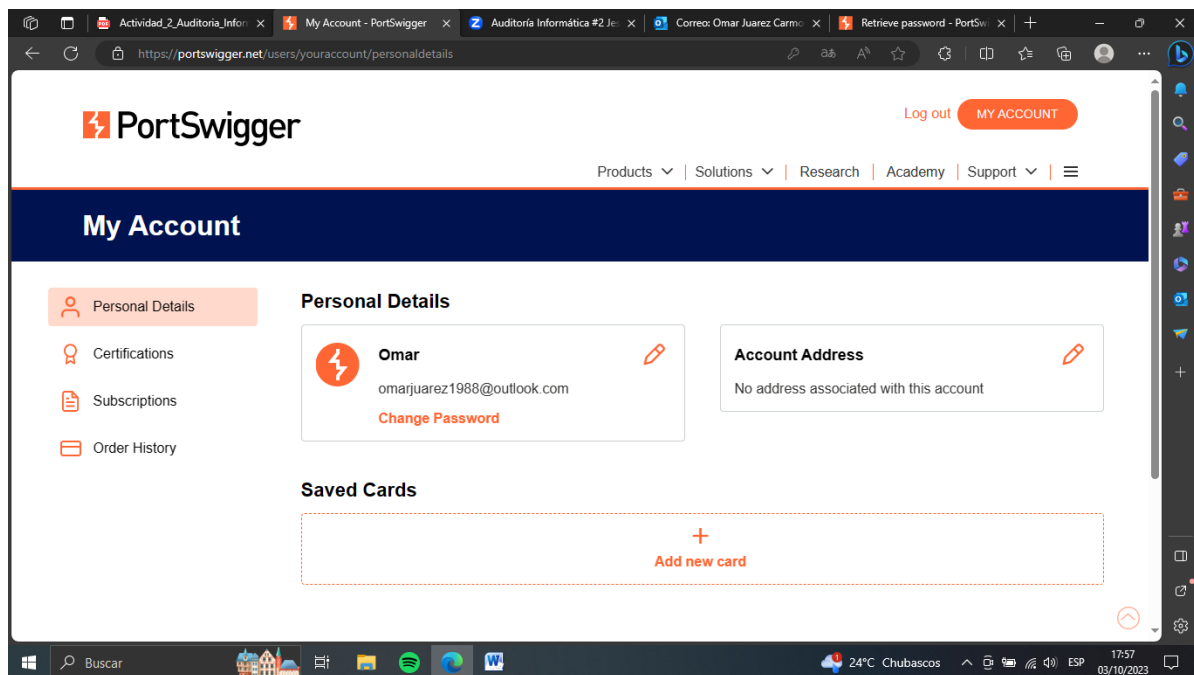
Corriendo el Browser de BurpSuite



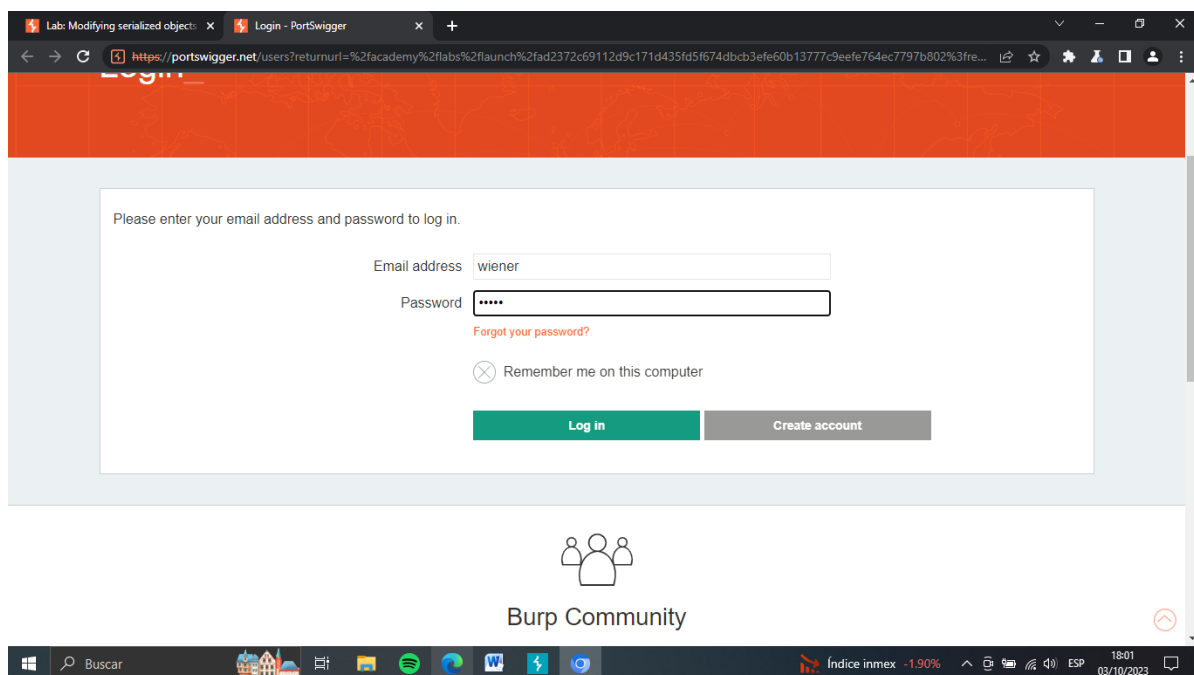
Link de PortSwigger



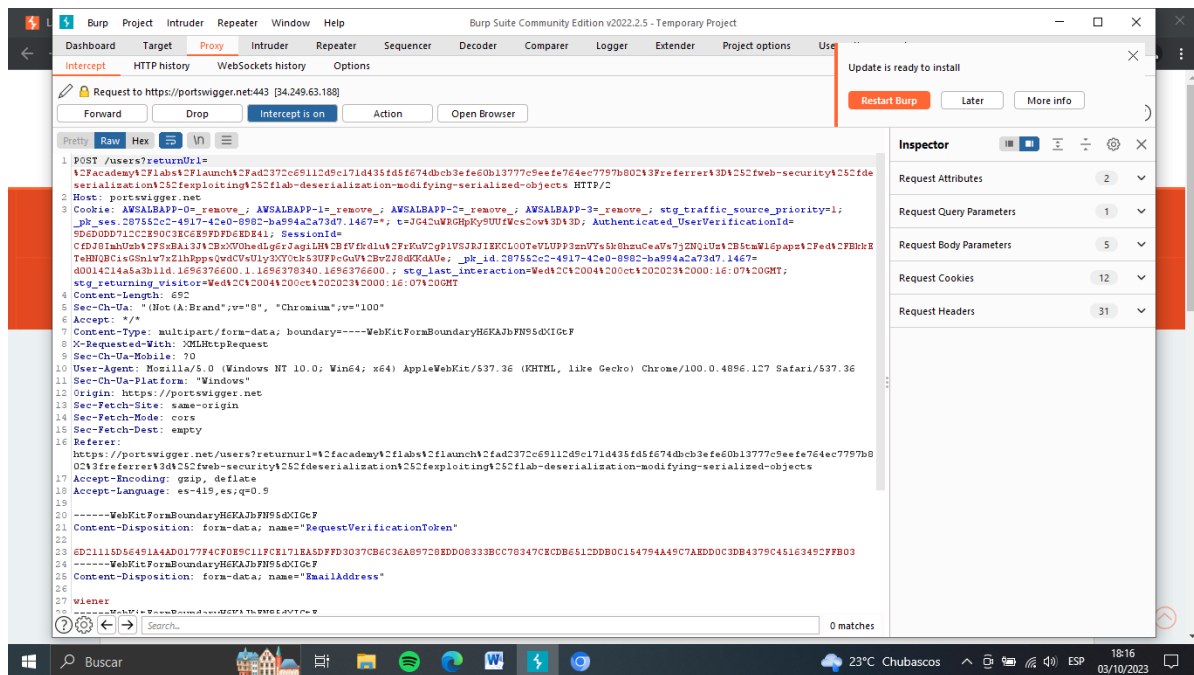
Accediendo a cuenta de PortSwigger



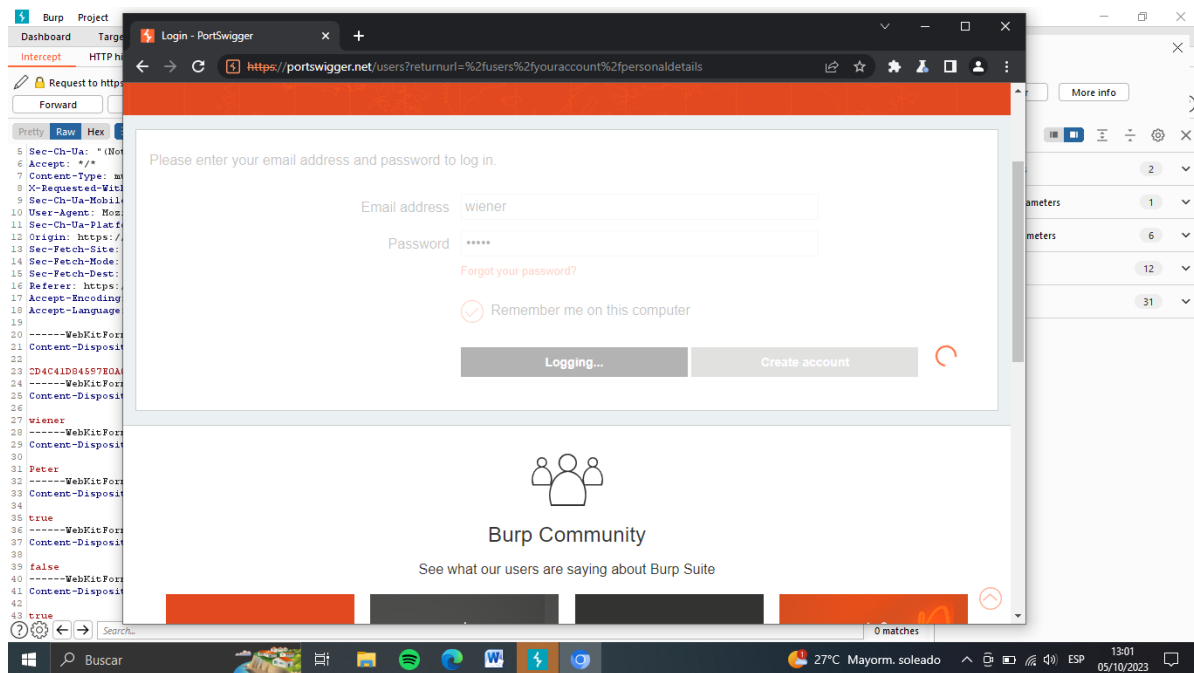
Intentando ingresar en el Browser con wiener y peter



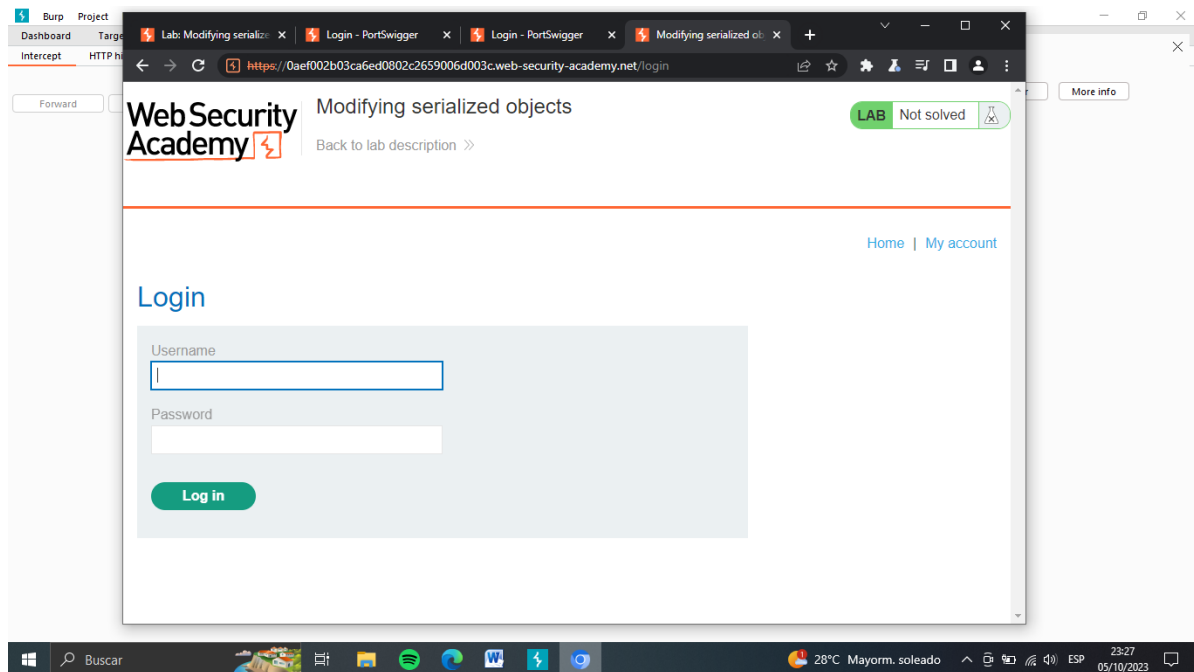
Código descrito al momento de ingresar donde arroja información de usuario y contraseña



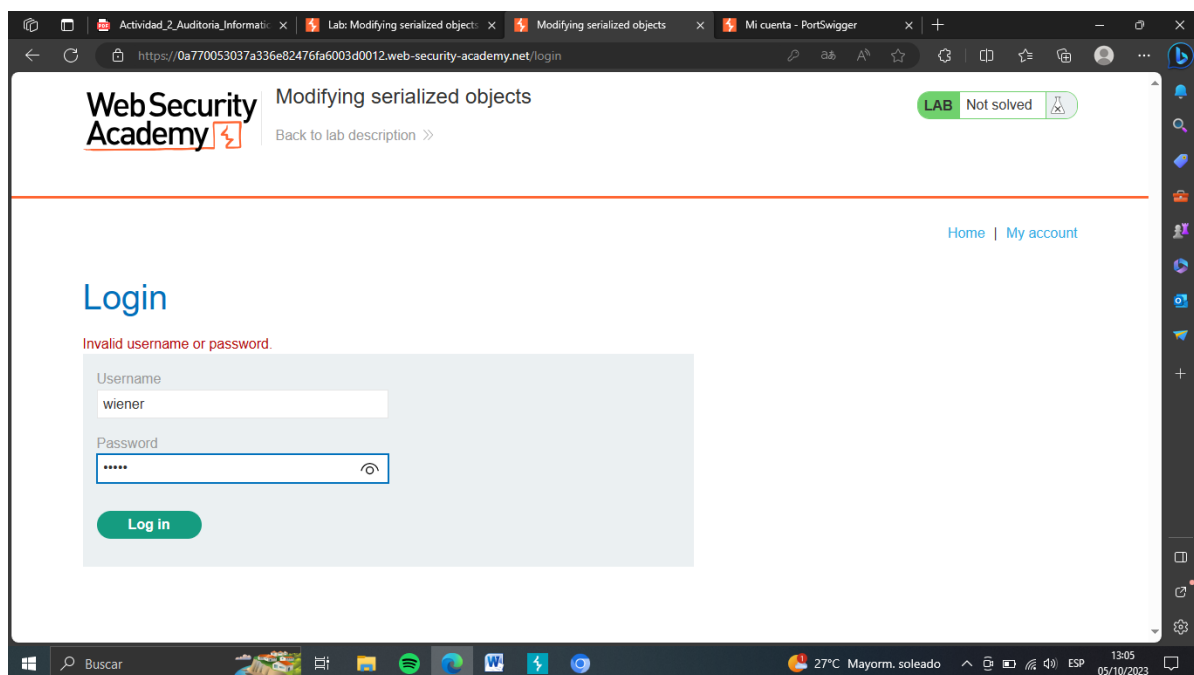
Cargando al tratar de iniciar sesión



Accediendo a BurpSuite para iniciar sesión con wiener y Peter.



Login en BurpSuite.



CONCLUSION

La deserialización insegura es una vulnerabilidad crítica que ocurre cuando una aplicación o una API deserializa datos manipulados por un atacante en el lado del servidor. Durante este proceso, un atacante puede abusar de la lógica de la aplicación y realizar ataques de denegación de servicio (DoS), omitir autenticaciones o incluso ejecutar código malicioso de forma remota. Para prevenir esta vulnerabilidad, es importante implementar medidas de seguridad adecuadas, como la validación y autenticación de datos, y utilizar bibliotecas y marcos de trabajo seguros.

El impacto de las amenazas a las vulnerabilidades de los sitios web ha sido tan alto que OWASP ha realizado año con año la lista de las 10 amenazas más peligrosas para los software y sus usuarios, incluidas las dos amenazas que vimos en esta unidad número dos.

Por lo anterior es indispensable proteger las aplicaciones de las vulnerabilidades de entidades externas XML para así fortalecer la seguridad de las aplicaciones web.

Aunado a lo anterior, es vital saber cómo identificar, prevenir o reparar estas vulnerabilidades que amenazan nuestros equipos, para así garantizar su seguridad.

Hemos realizado la actividad número 2, en donde utilizamos la herramienta de trabajo de BurpSuite para poder entrar al laboratorio con un usuario y así poder robar y modificar información con un usuario legal dentro de este laboratorio.

Digamos que nos robamos la información para poder modificar como si fuésemos un usuario correcto dentro de esta página diferentes rubros.

Hemos aprendido a utilizar la herramienta de trabajo de BurpSuite y así poder hackear información y poder entrar en modo incognito a cierta página para poder hacer modificaciones en sus sistemas sin que se den cuenta los usuarios oficiales.

Esperamos seguir aprendiendo tantas cosas valiosas para poder ser unos auditores informáticos exitosos.

REFERENCIAS Y LINK

A07 Fallas de Identificación y Autenticación - OWASP Top 10:2021. (n.d.).

Owasp.org. Retrieved September 21, 2023, from

[https://owasp.org/Top10/es/A07_2021-
Identification and Authentication Failures/](https://owasp.org/Top10/es/A07_2021-Identification_and_Authentication_Failures/)

Professional / Community 2022.2.5. (2022, April 20). Burp Suite Release Notes.

[https://portswigger.net/burp/releases/professional-community-2022-2-
5?requestededition=community&requestedplatform](https://portswigger.net/burp/releases/professional-community-2022-2-5?requestededition=community&requestedplatform)

Castillo, A. (1586827274000). *Deserialización insegura – OWASP Top 8.*

Linkedin.com. [https://es.linkedin.com/pulse/deserializaci%C3%B3n-
insegura-owasp-top-8-alexander-castillo](https://es.linkedin.com/pulse/deserializaci%C3%B3n-insegura-owasp-top-8-alexander-castillo)

Lab: Modifying serialized objects. (n.d.). Portswigger.net. Retrieved October 6,

2023, from [https://portswigger.net/web-
security/deserialization/exploiting/lab-deserialization-modifying-serialized-
objects](https://portswigger.net/web-security/deserialization/exploiting/lab-deserialization-modifying-serialized-objects)

LINK DE GITHUB

[Omarsitho1988 \(github.com\)](https://github.com/Omarsitho1988)