Universidad Corporativa | 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: Gabriel German Verdugo Solís

Fecha: 18 de febrero del 2024

INDICE

INTRODUCCION

En esta actividad, se nos pide realizar una prueba de vulnerabilidad de Cross Site Scripting (XSS). En ella 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. El Cross Site Scripting (XSS) es uno de los ataques más populares y vulnerables que se conoce. Está considerado como uno de los ataques más arriesgados para las aplicaciones web y también puede traer consecuencias muy graves. El XSS se compara a menudo con otros ataques similares en el lado del cliente, ya que durante este ataque se utilizan principalmente lenguajes del lado del cliente. Sin embargo, el ataque XSS se considera más arriesgado, debido a su capacidad para dañar incluso tecnologías, en teoría menos vulnerables. El ataque Cross Site Scripting es una inyección de código malicioso, que se ejecutará en el navegador de la víctima. El script malicioso puede guardarse en el servidor web y ejecutarse cada vez que el usuario llame a la funcionalidad correspondiente. También se puede realizar sin ningún script guardado en el servidor web. El objetivo principal de este ataque es robar los datos de identidad de un usuario, como cookies, tokens de sesión y otra información. En la mayoría de los casos, este ataque se utiliza para robar las cookies del usuario. Como sabemos, las cookies nos ayudan a iniciar la sesión automáticamente. Por lo tanto, con las cookies robadas, podemos iniciar sesión con otras identidades. Y esta es una de las razones por las que este ataque se considera uno de los más arriesgados. El ataque XSS se realiza en el lado del cliente. Se puede realizar con diferentes lenguajes de programación en el lado del cliente. Sin embargo, la mayoría de las veces este ataque se realiza con JavaScript y HTML.

DESCRIPCION

Se realizar una prueba de vulnerabilidad de Cross Site Scripting (XSS). En ella se debe obtener las credenciales que se ingresen para iniciar sesión. La vulnerabilidad de Cross-Site Scripting (XSS) es un tipo de vulnerabilidad de seguridad en aplicaciones web que permite a un atacante inyectar código malicioso, generalmente JavaScript, en una página web o aplicación web que luego se ejecuta en el navegador de un usuario. Esta vulnerabilidad puede permitir que el atacante:

1.- Robe información confidencial: El atacante puede utilizar el código malicioso para robar cookies de sesión, credenciales de usuario, datos personales u otra información sensible almacenada en el navegador del usuario.

2.- Suplante la identidad del usuario: Al robar cookies de sesión, un atacante puede hacerse pasar por un usuario legítimo y acceder a sus cuentas y datos.

3.- Realice acciones maliciosas en nombre del usuario: Una vez que el atacante tiene acceso a la sesión de un usuario, puede llevar a cabo acciones en su nombre, como realizar transacciones no autorizadas o cambiar la configuración de la cuenta.

JUSTIFICACION

Es importante saber que debemos de conocer a detalle la implementación. La vulnerabilidad de Cross-Site Scripting (XSS) es una amenaza de seguridad significativa y se justifica debido a varias razones clave: Explotación de información confidencial: La explotación exitosa de una vulnerabilidad de XSS permite a un atacante acceder a información confidencial almacenada en el navegador de un usuario, como cookies de sesión, credenciales de inicio de sesión y datos personales. Esto podría comprometer la privacidad y la seguridad de los usuarios. Suplantación de identidad (phishing): Al robar cookies de sesión o credenciales de usuario, un atacante podría hacerse pasar por un usuario legítimo, lo que puede llevar a la realización de acciones maliciosas en nombre del usuario, como el robo de cuentas o la propagación de mensajes de phishing.

Impacto en la integridad de los datos: XSS puede llevar a la manipulación no autorizada de datos en aplicaciones web. Un atacante puede realizar cambios en la información almacenada en la aplicación, lo que puede tener un impacto significativo en la integridad de los datos. Riesgos para la seguridad de la aplicación: Una vulnerabilidad de XSS podría permitir a un atacante tomar control de una aplicación web, lo que podría llevar a la ejecución de comandos maliciosos, la instalación de malware o la divulgación de información sensible.

Propagación de ataques: Los ataques de XSS a menudo se propagan rápidamente, ya que pueden afectar a múltiples usuarios a través de un solo punto de entrada malicioso. Esto puede tener un efecto dominó y dañar a un gran número de usuarios y sistemas. Cumplimiento legal y reputación: Las empresas y organizaciones pueden enfrentar repercusiones legales y daños en su reputación si se descubre que sus aplicaciones web son vulnerables a ataques de XSS. Los

reguladores pueden imponer multas y sanciones, y los clientes pueden perder la confianza en la seguridad de sus servicios. Dada la amplia gama de riesgos y consecuencias asociados con la vulnerabilidad de XSS, es esencial que las organizaciones tomen medidas proactivas para identificar y remediar estas vulnerabilidades en sus aplicaciones web. Esto incluye la implementación de mejores prácticas de seguridad de desarrollo de aplicaciones, pruebas de seguridad regulares y la educación de los equipos de desarrollo y operaciones sobre cómo prevenir y mitigar las amenazas de XSS.

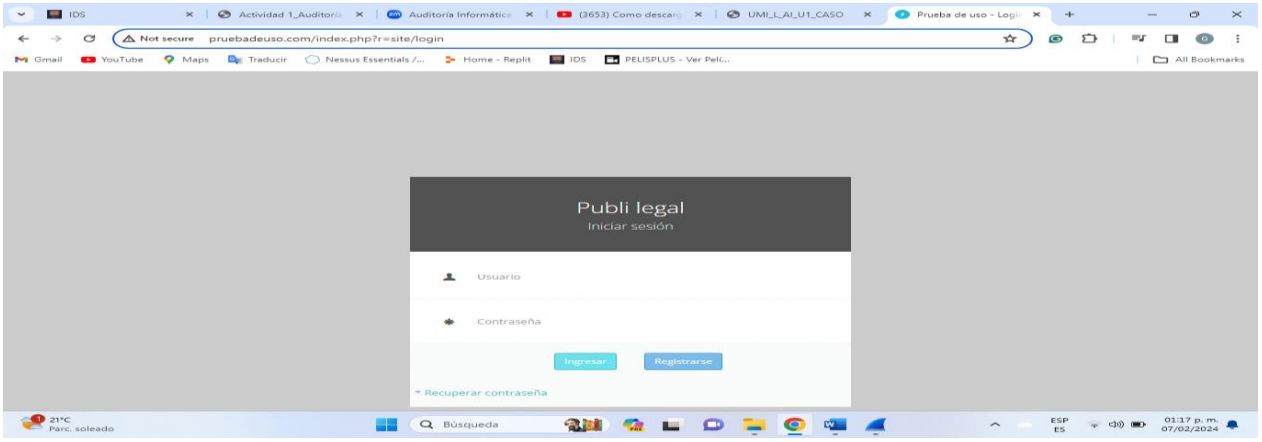
Burp Suite, es una plataforma capaz de llevar a cabo las auditorías de seguridad, de una organización con el objetivo de evitar ataques de software maliciosos.

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. Burp Suite es una herramienta de pruebas de seguridad diseñada para evaluar la seguridad de aplicaciones web y sistemas. Funciona como un proxy web que intercepta las solicitudes y respuestas HTTP entre un cliente web (como un navegador) y el servidor web.

ETAPA 1

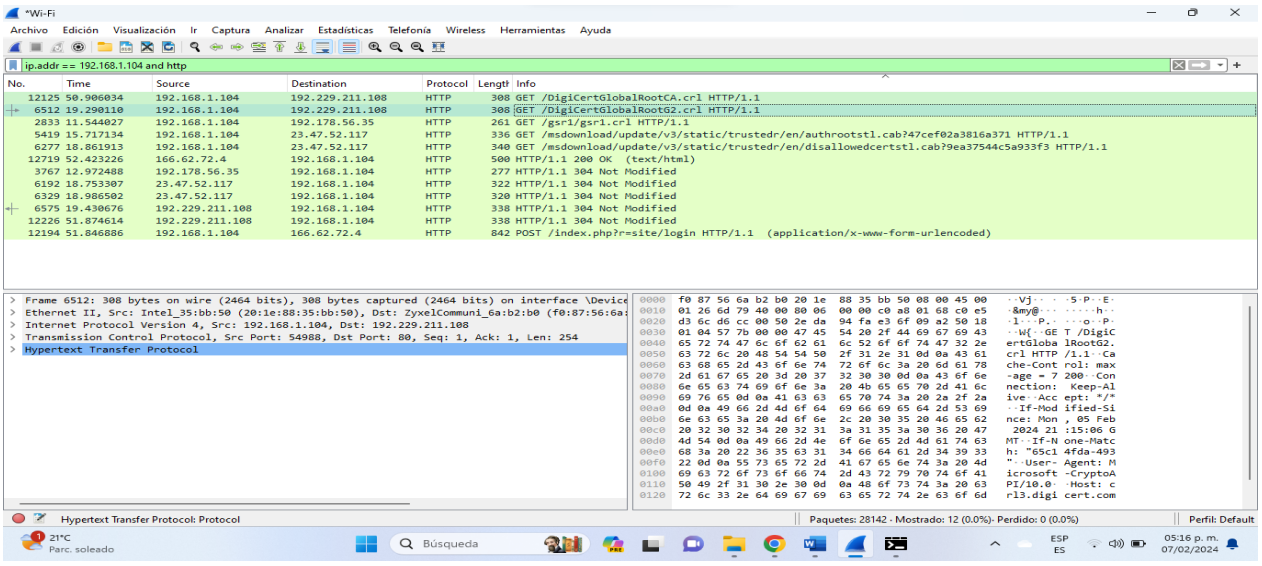
DESCRIPCION DEL SITIO WEB

En esta actividad se utilizará una página web no segura para poder realizar la prueba de vulnerabilidad. En este screenshot se muestra la pagina a utilizar

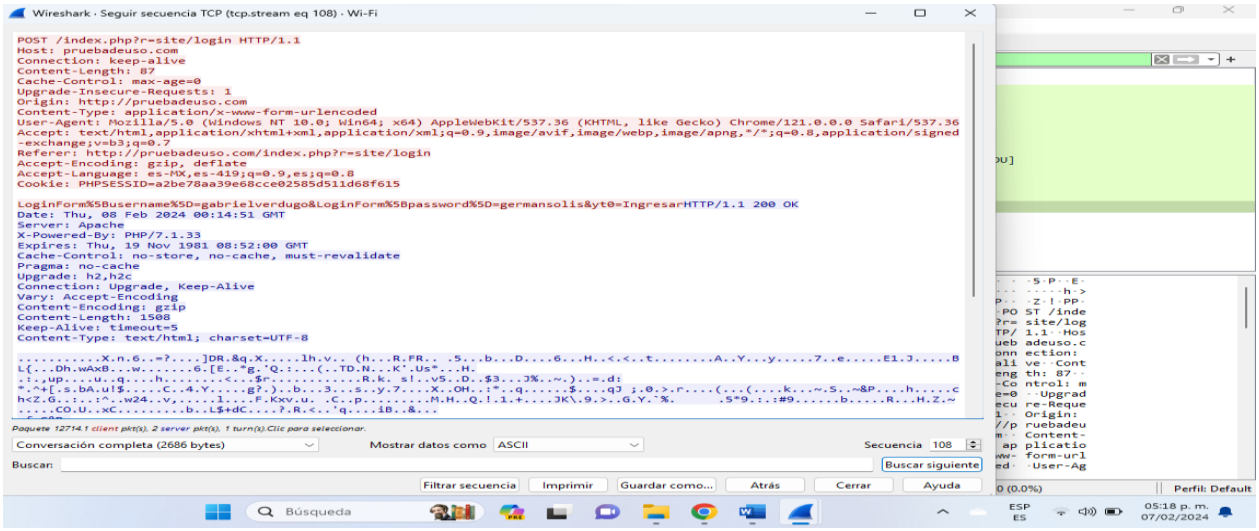


ATAQUE AL SITIO WEB

En esta imagen se muestra el funcionamiento de la prueba con wireshark



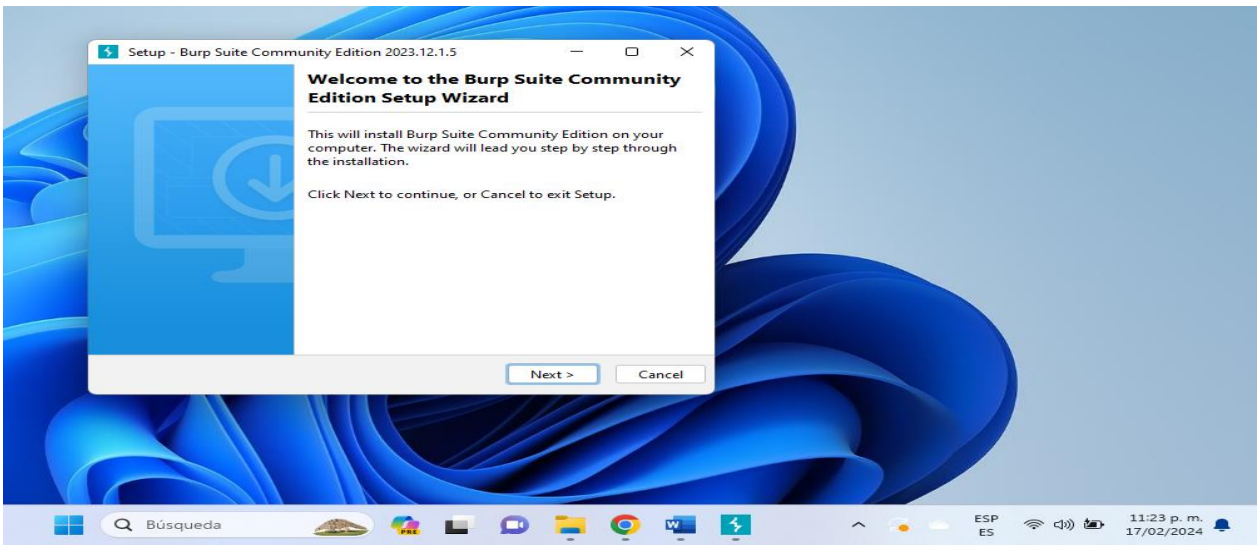
En esta imagen se muestra ya la contraseña y el usuario utilisado para querer ingresar ala pagina web donde se intento poner como usuario gabrielverdugo y en password germansolis

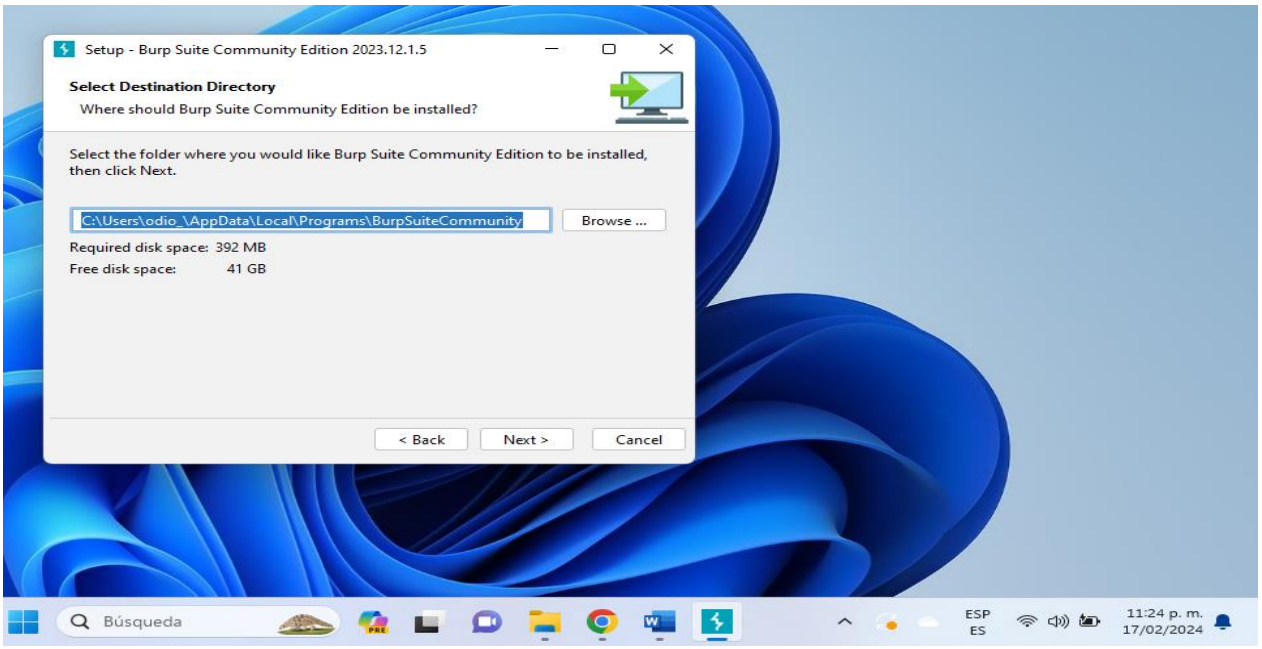


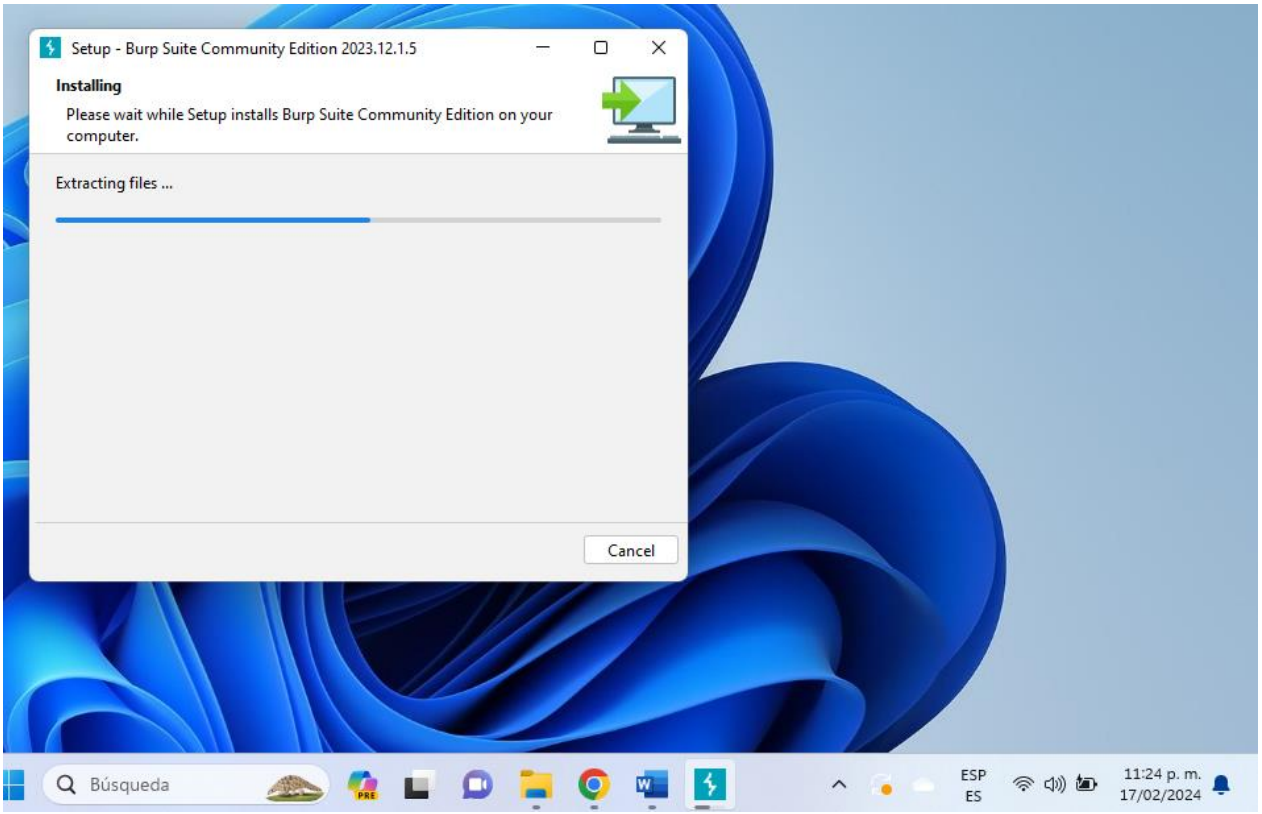
ETAPA 2

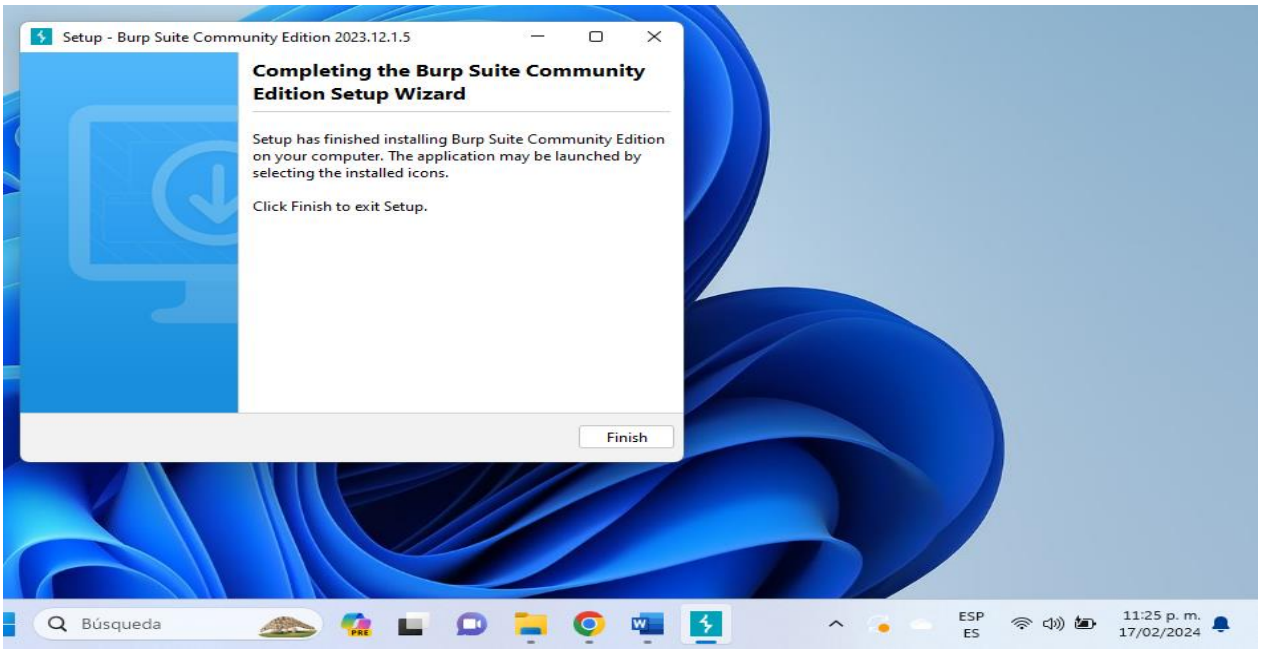
ATAQUE AL SITIO

En esta imagen se muestra la instalación de burp suite community

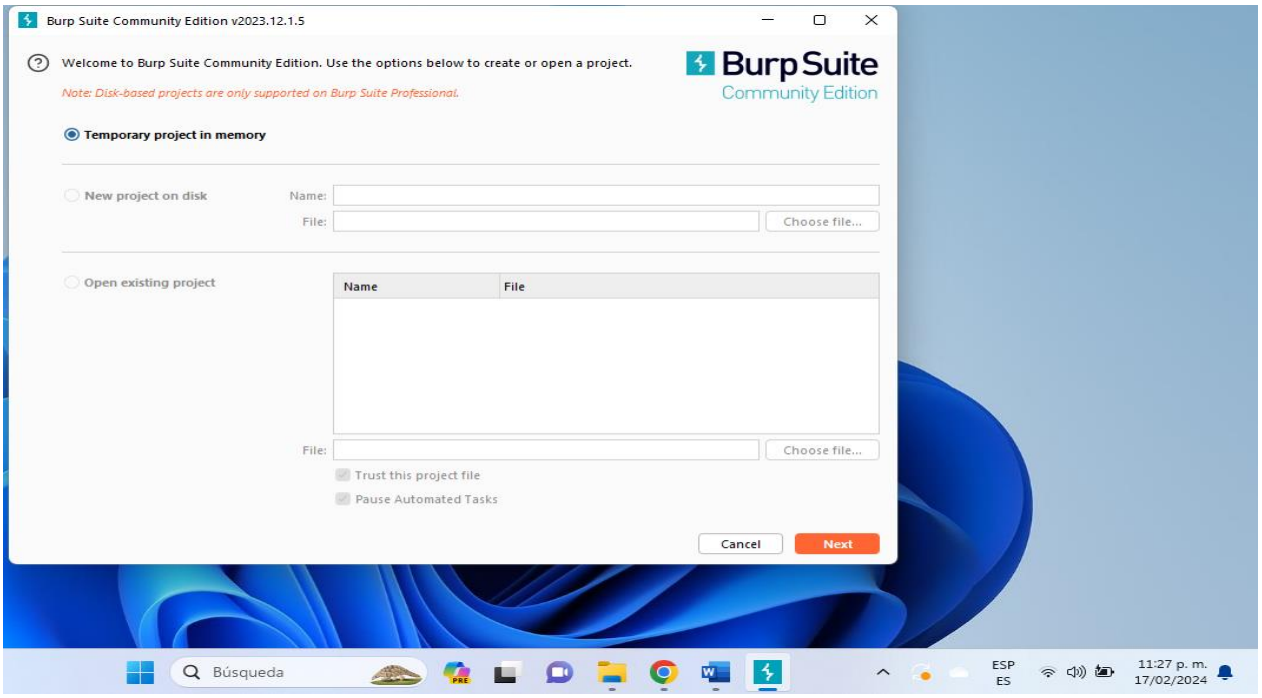



Setup - Burp Suite Community Edition 2023.12.1.5
Select Destination Directory
Where should Burp Suite Community Edition be installed?
Select the folder where you would like Burp Suite Community Edition to be installed, then click Next.
C:\Users\odio_\AppData\Local\Programs\BurpSuiteCommunity
Browse ...
Required disk space: 392 MB
Free disk space: 41 GB
< Back
Next >
Cancel
Búsqueda
ESP
ES
11:24 p. m.
17/02/2024

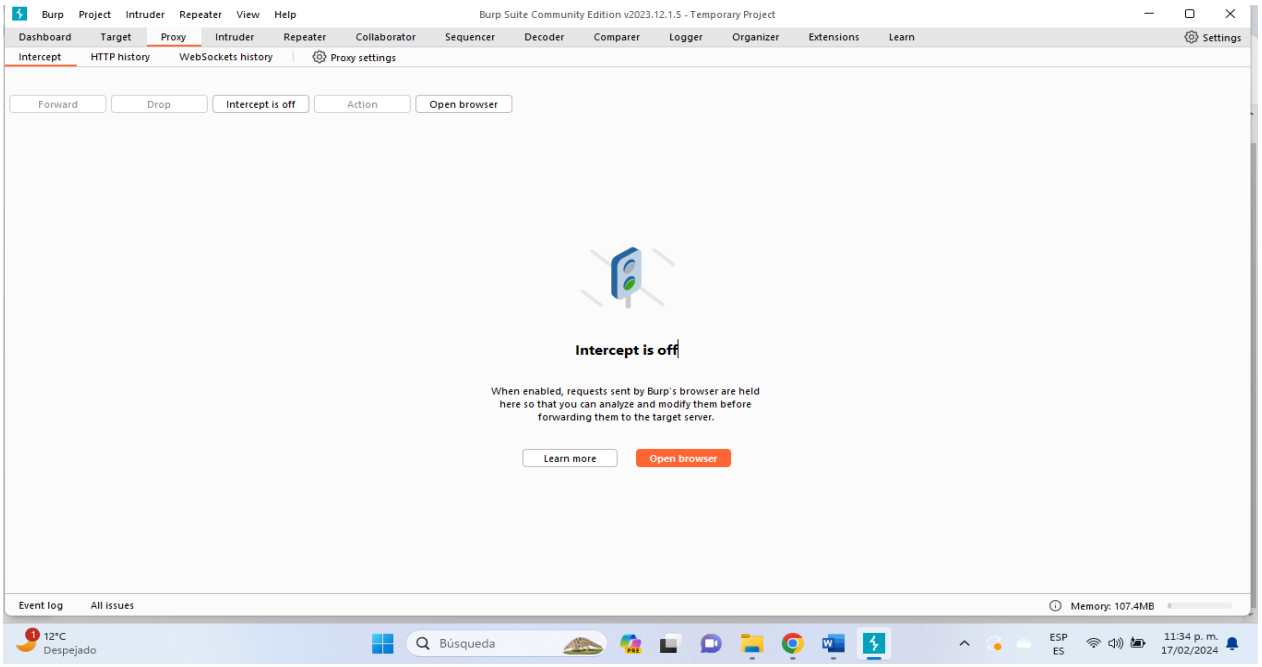

Setup - Burp Suite Community Edition 2023.12.1.5
Installing
Please wait while Setup installs Burp Suite Community Edition on your computer.
Extracting files ...
Cancel
Búsqueda
ESP
ES
11:24 p. m.
17/02/2024



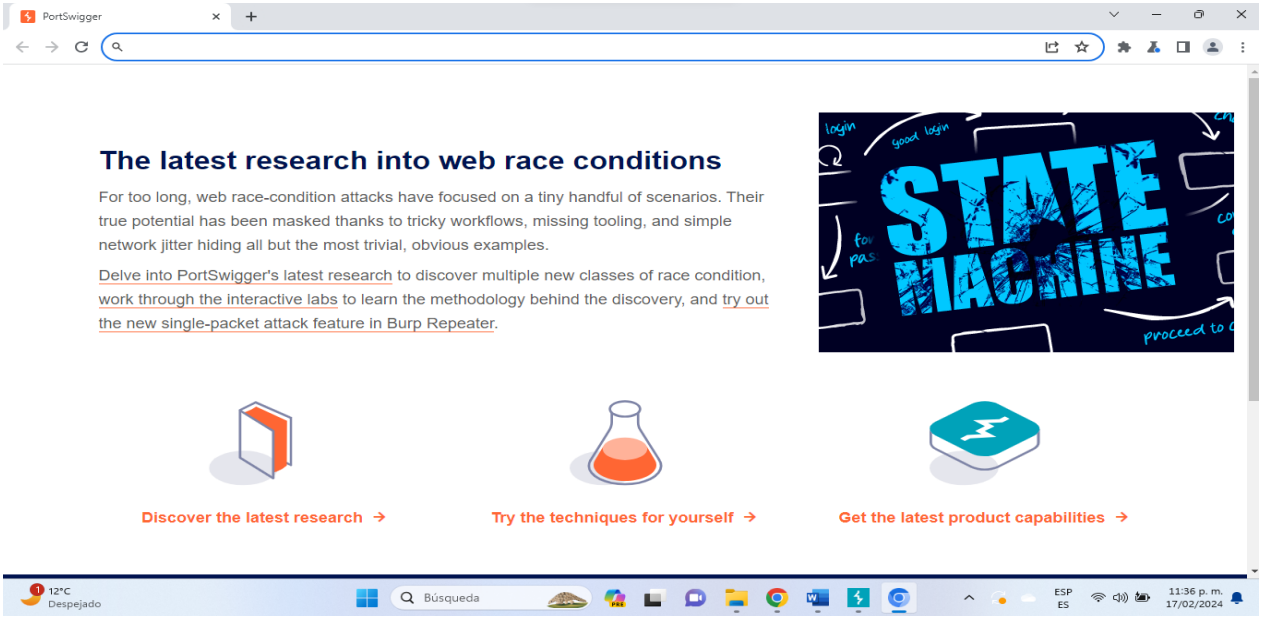
En esta imagen se muestra la entrada ala herramienta a utilizar



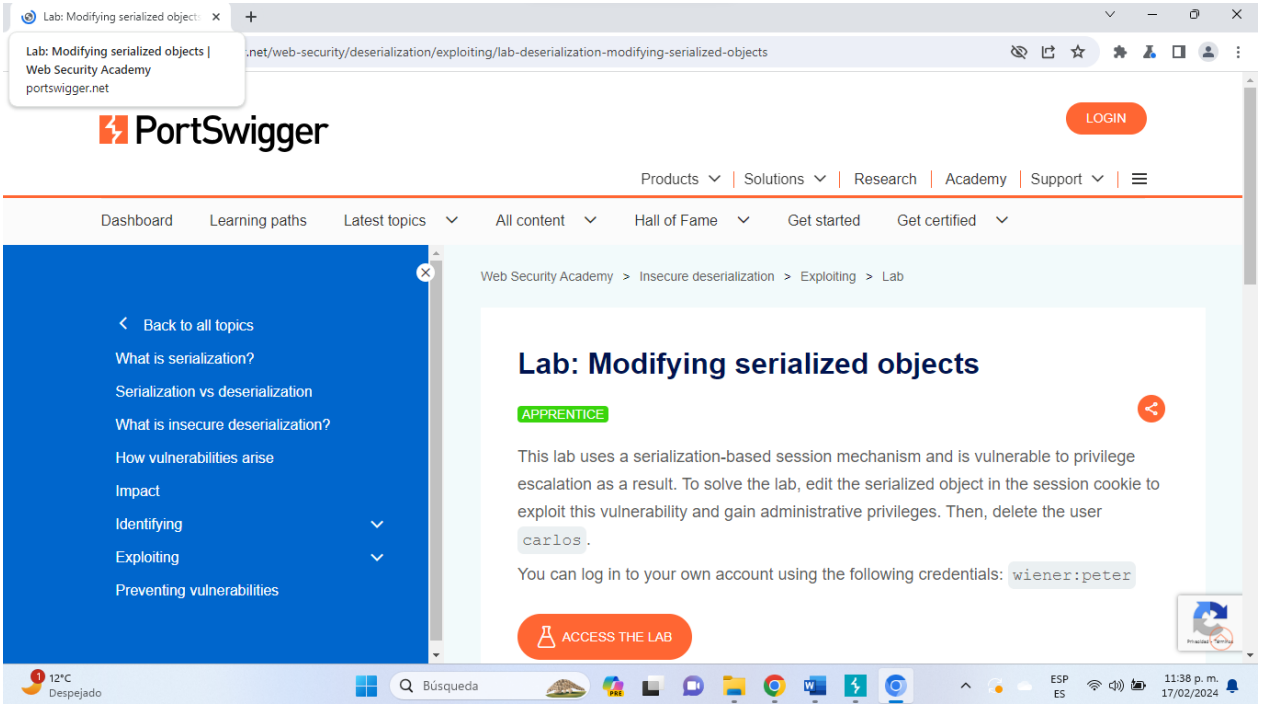
En esta imagen se muestra para ingresar ala pagina con open browser



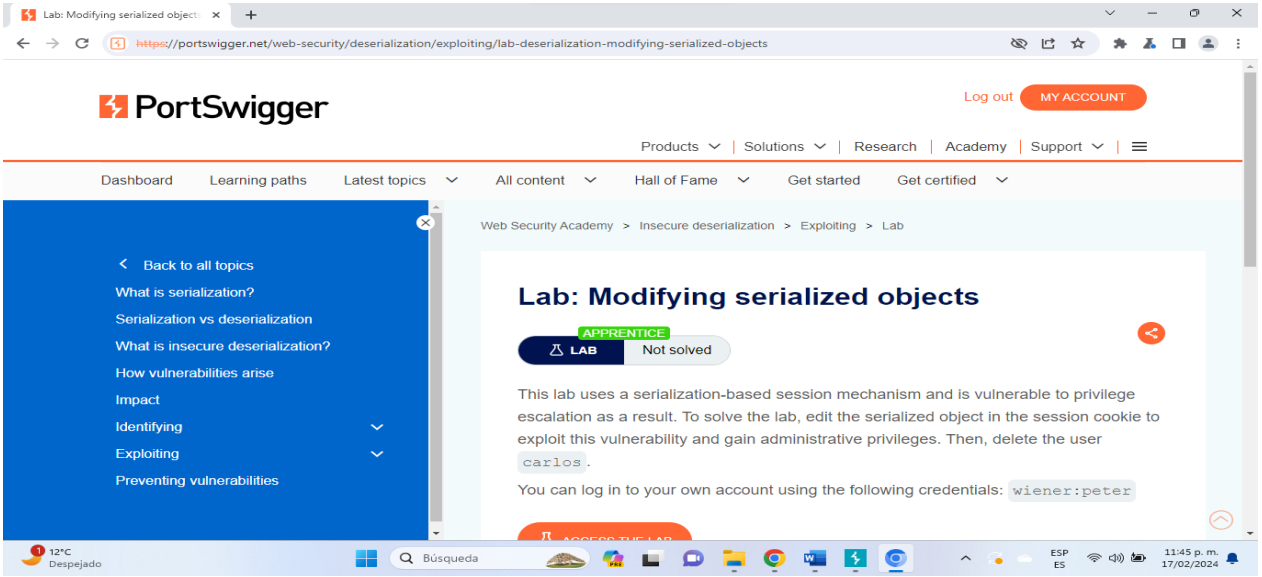
En esta imagen se muestra la entrada ala pagina donde se estara atrabajando



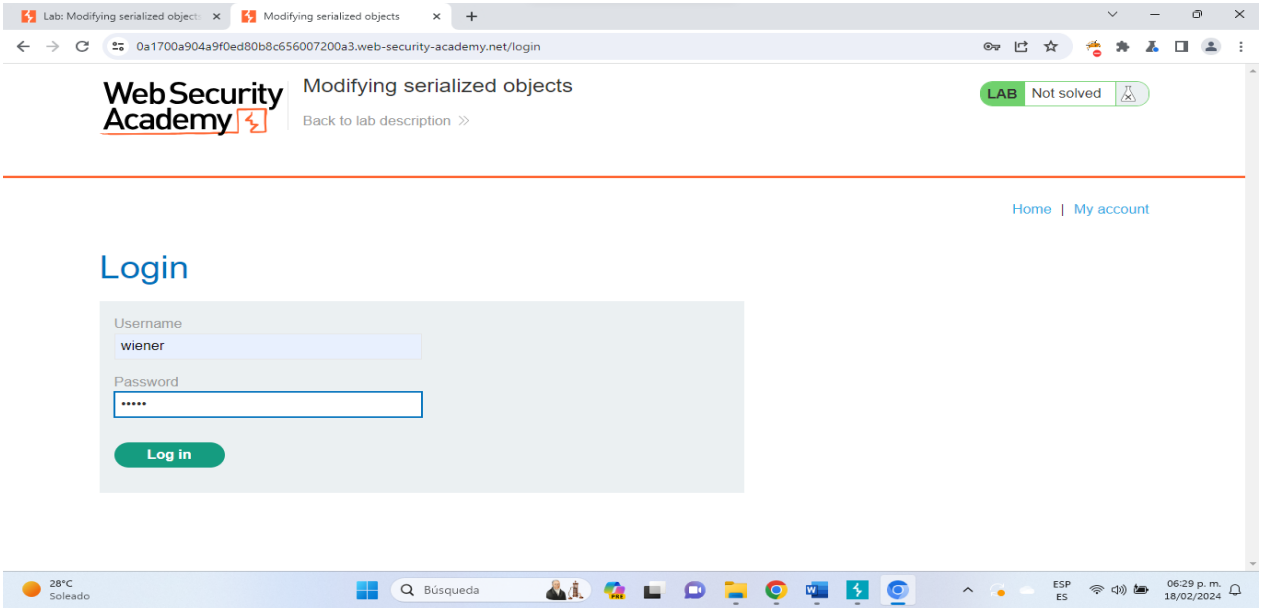
En esta imagen se muestra el enlace copiado para trabajar con el laboratorio

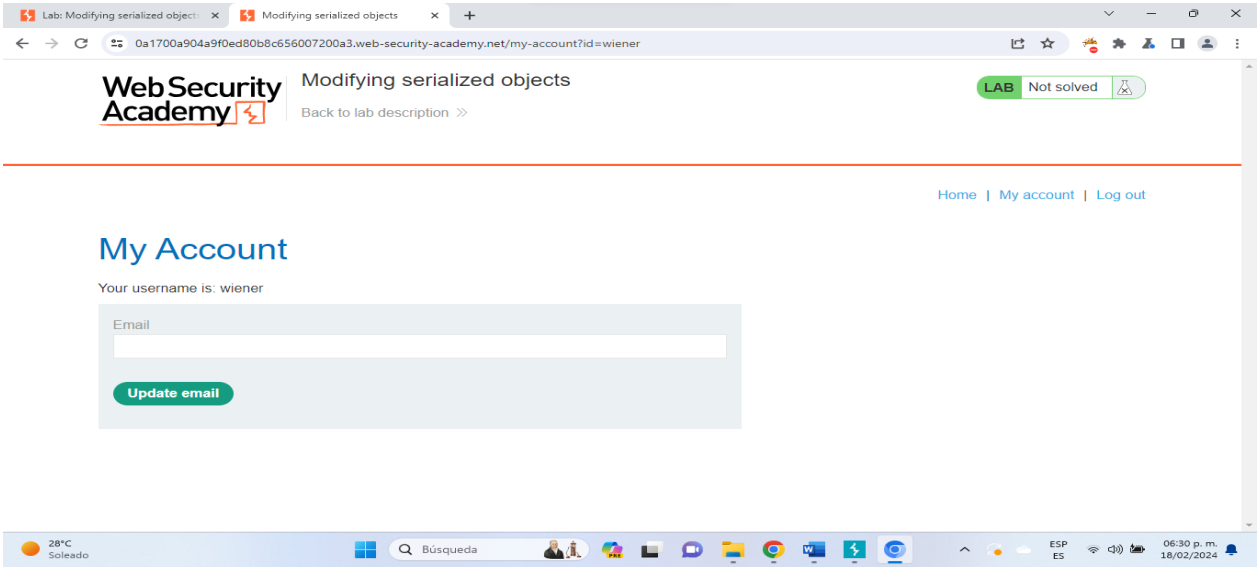


En esta imagen se muestra el incio de secion con el login creado

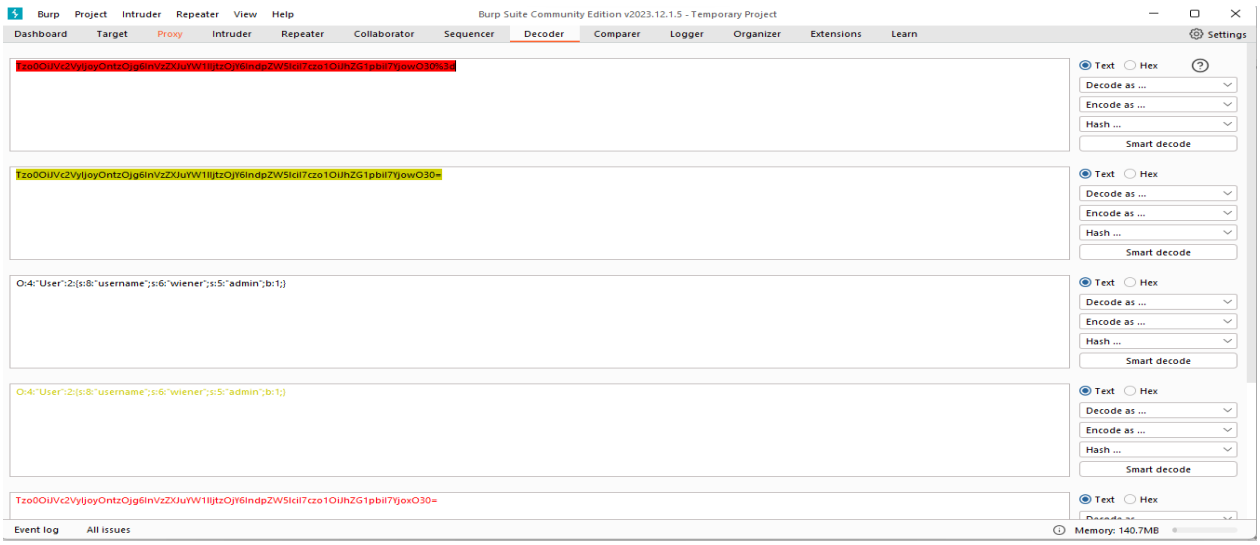


En estas imagenes se muestra el incio de secion en my account con el usuario: wiener contraseña: peter

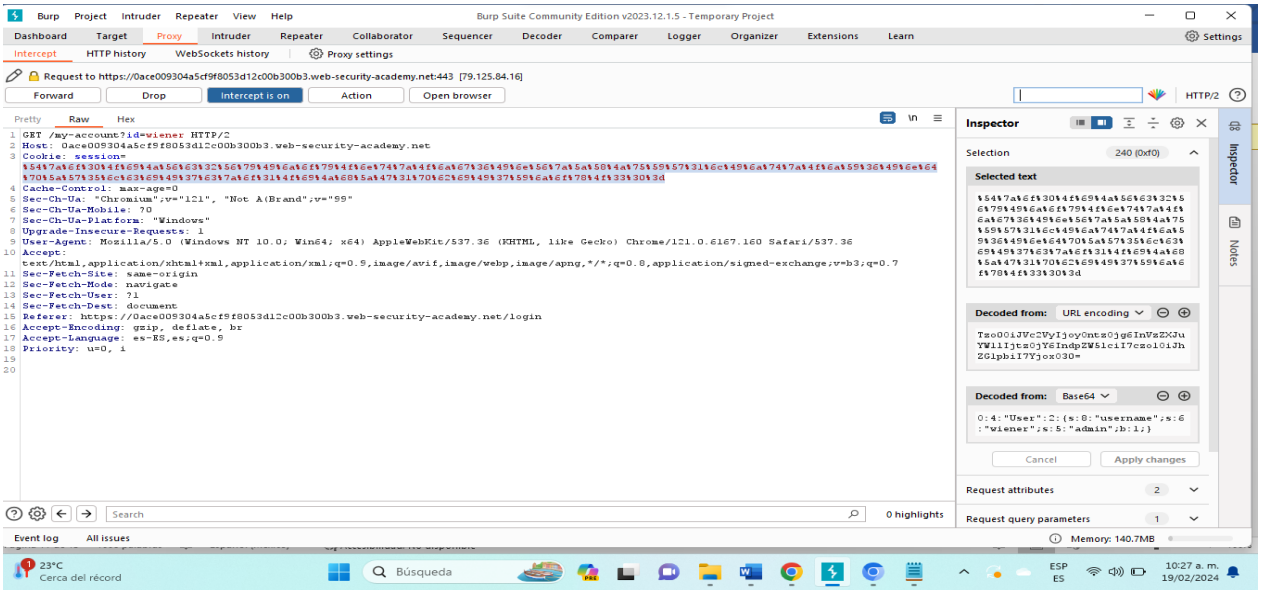




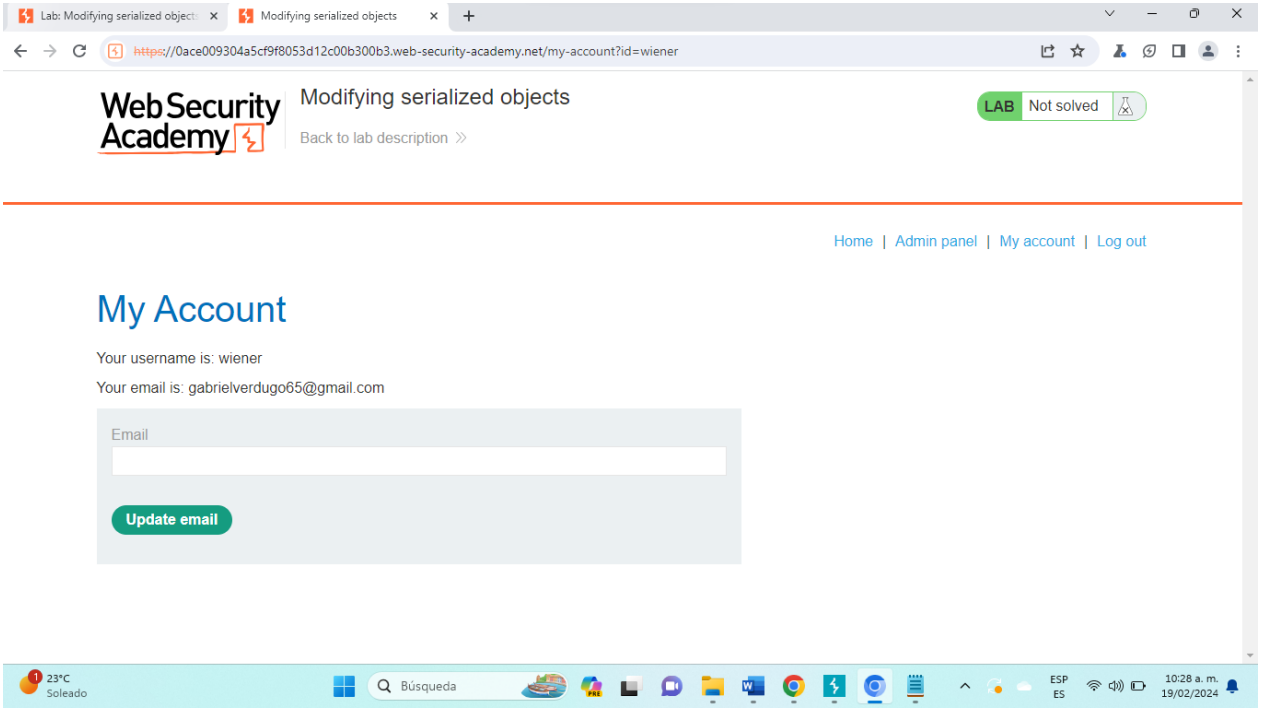
Se manda el cookies al decoder para decodificar y se cambia el o al 1 para pasar a modo administrador



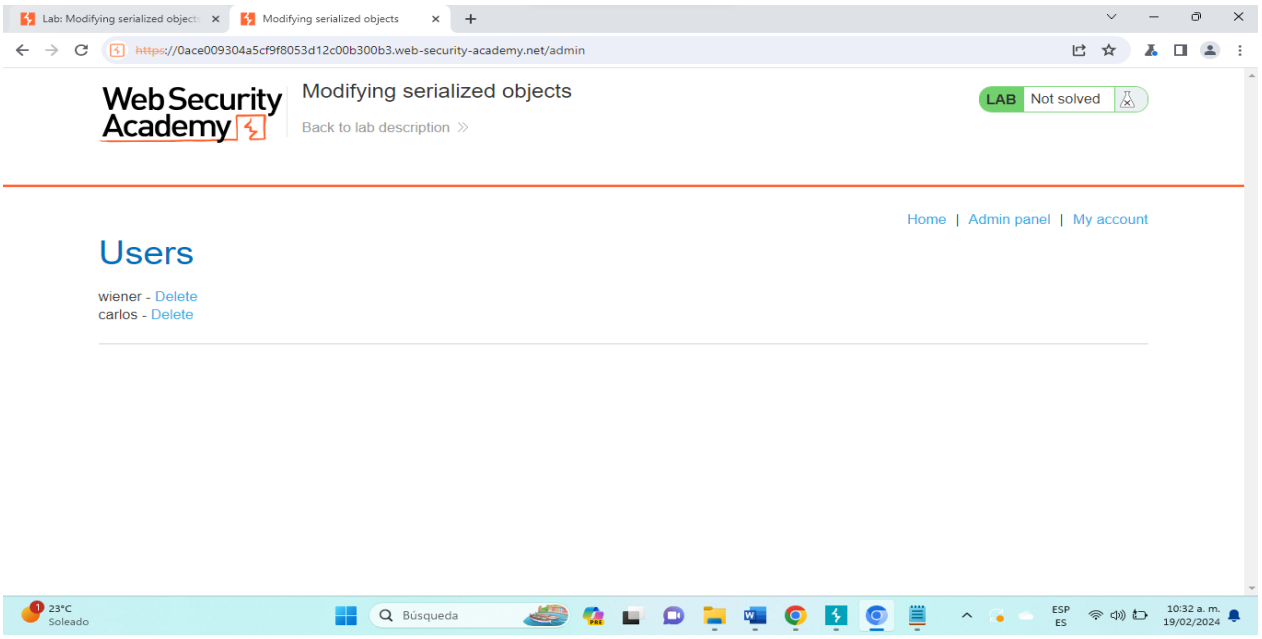
Se pega cookies en el intercept



Se muestra en modo administrador



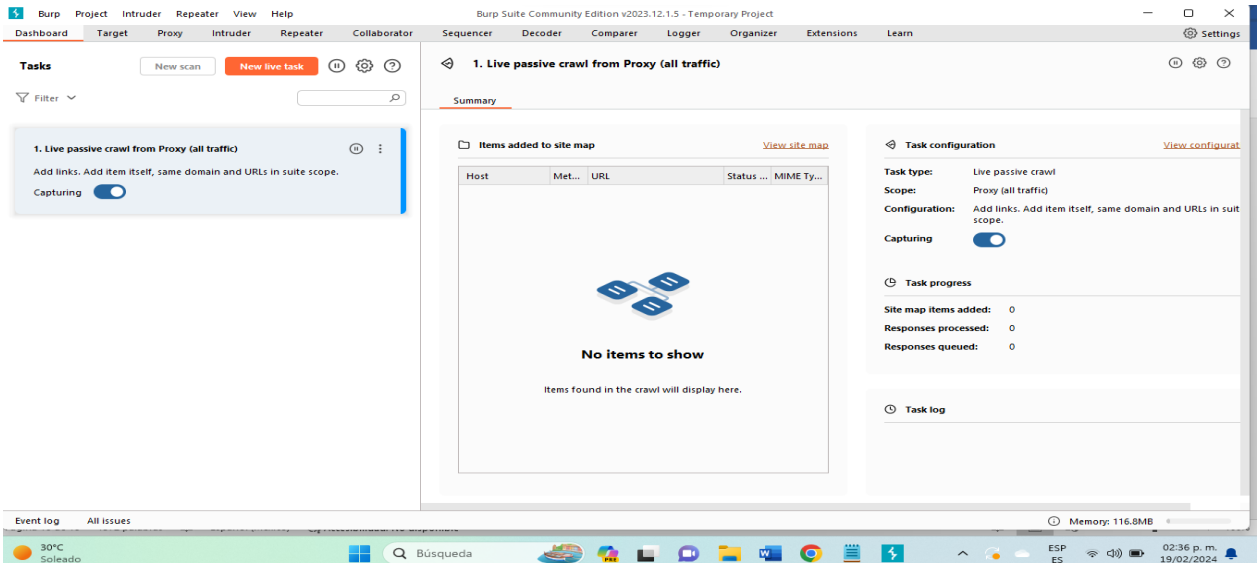
Se muestran los usuarios para poder borrar el usuareo de carlos



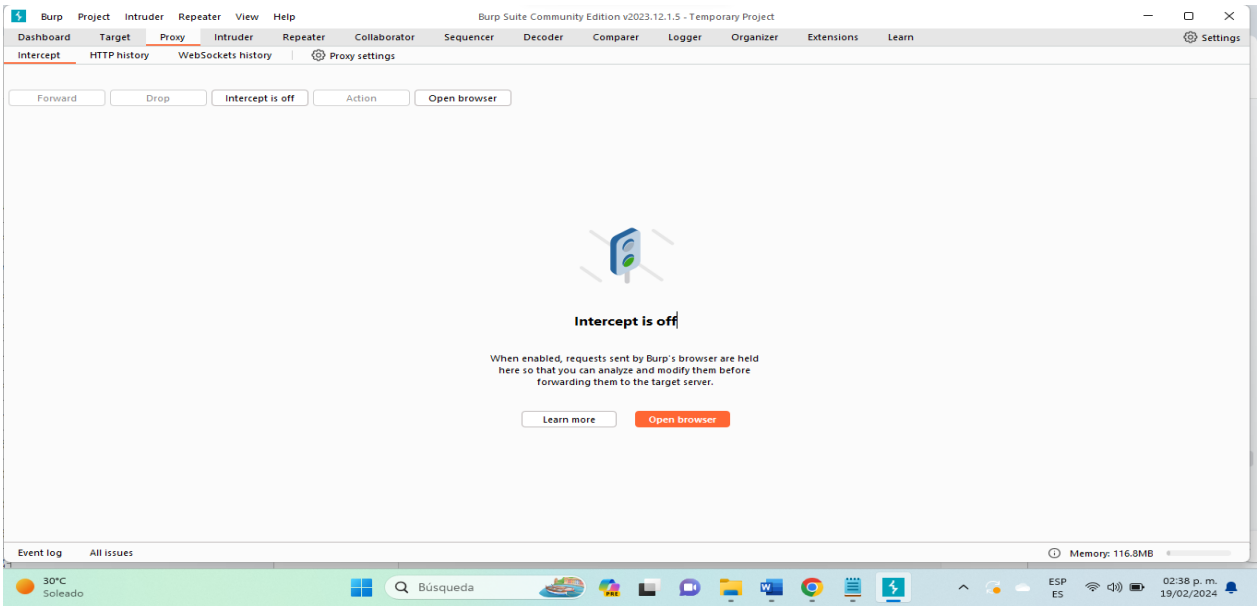
ETAPA 3

Ataque al sitio

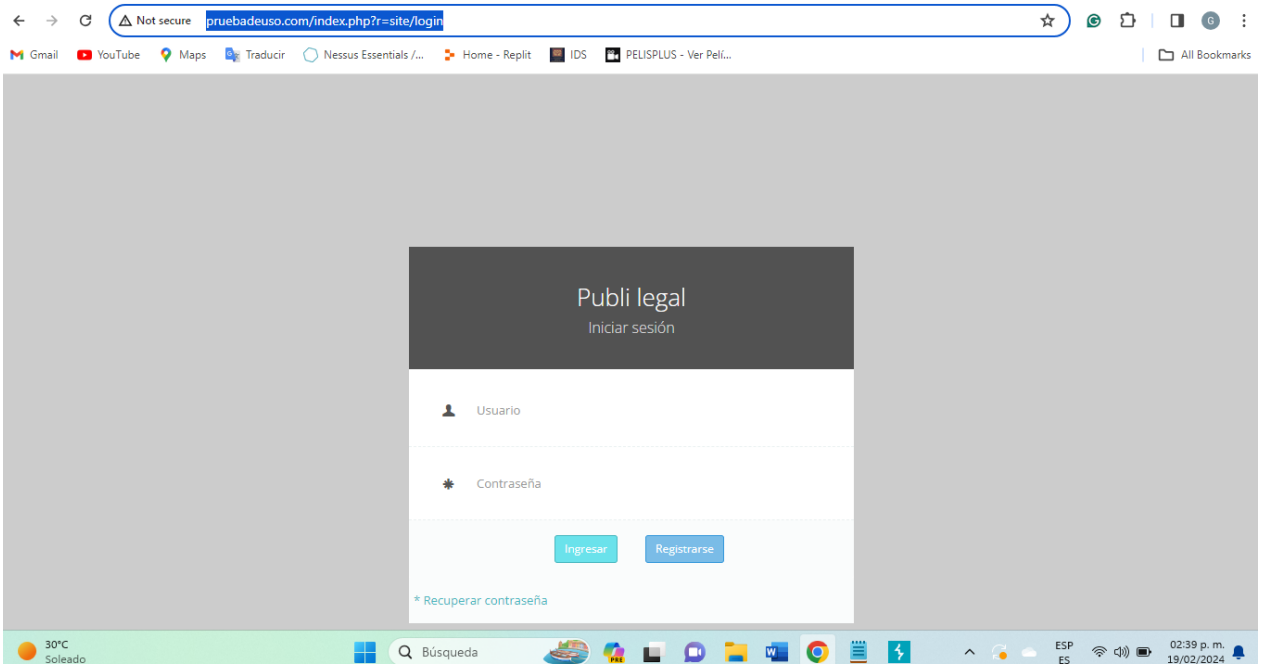
Se inicia burp suite



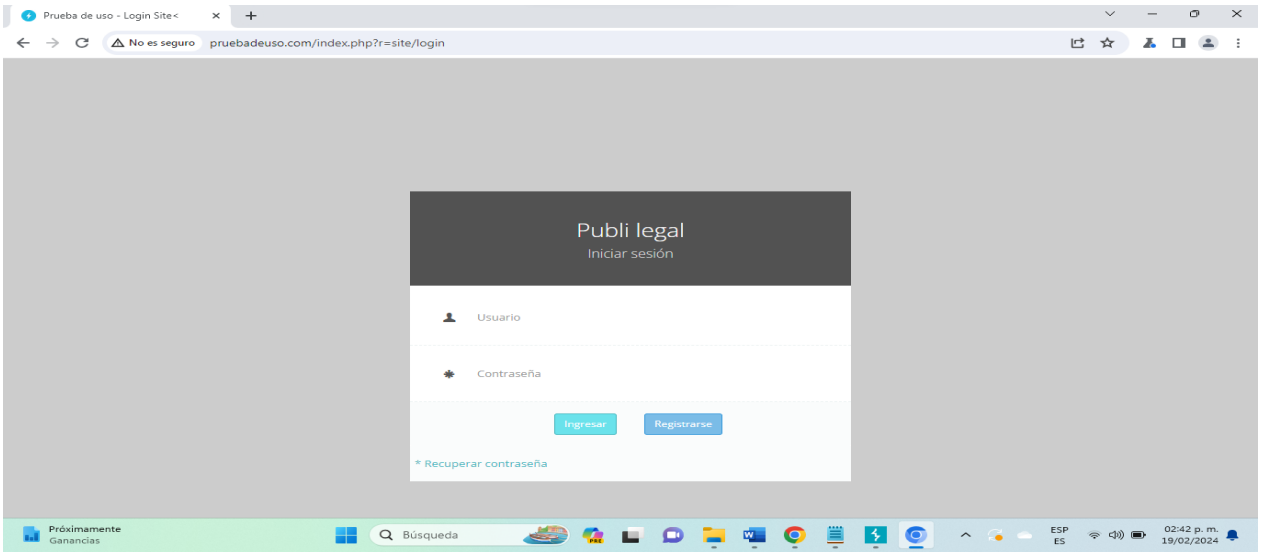
Ir a la sección proxy y dar click en abrir el navegador.



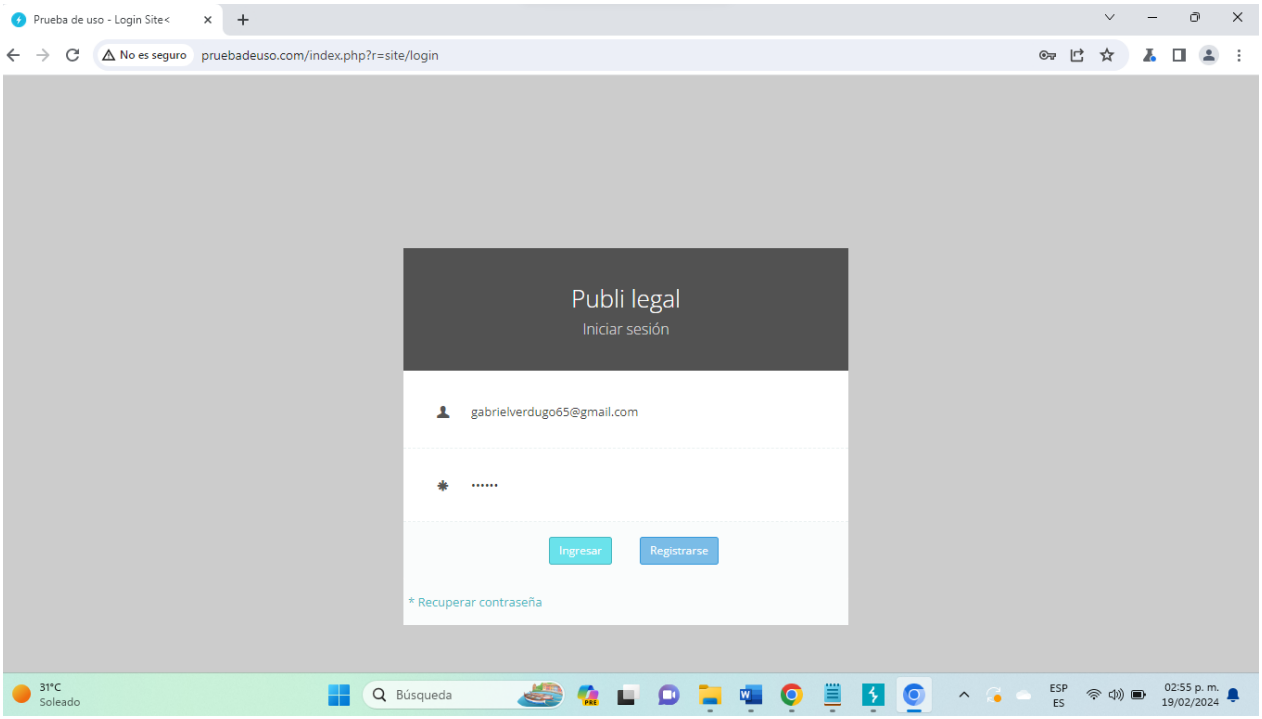
En el navegador que utiliza *Burp Suite*, entrar al sitio web del proyecto que se subió en la *Actividad* 1.

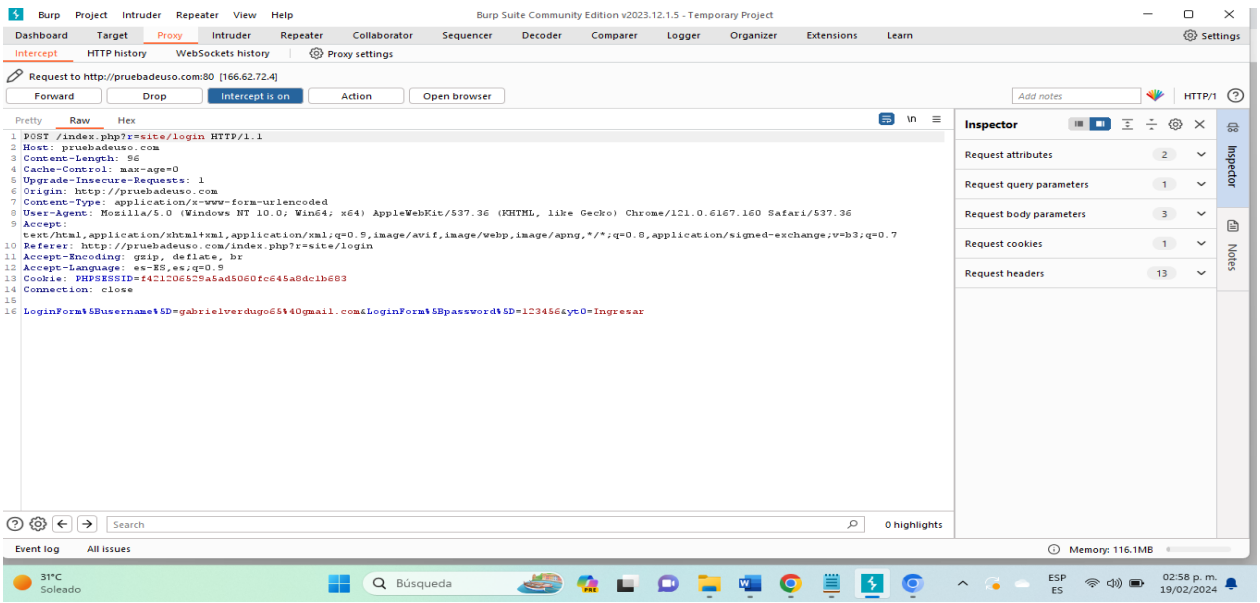


Dentro del sitio web, en la página de *login*, en el programa de Burp Suite, encender el interceptor. Luego, iniciar sesión con las credenciales correctas.

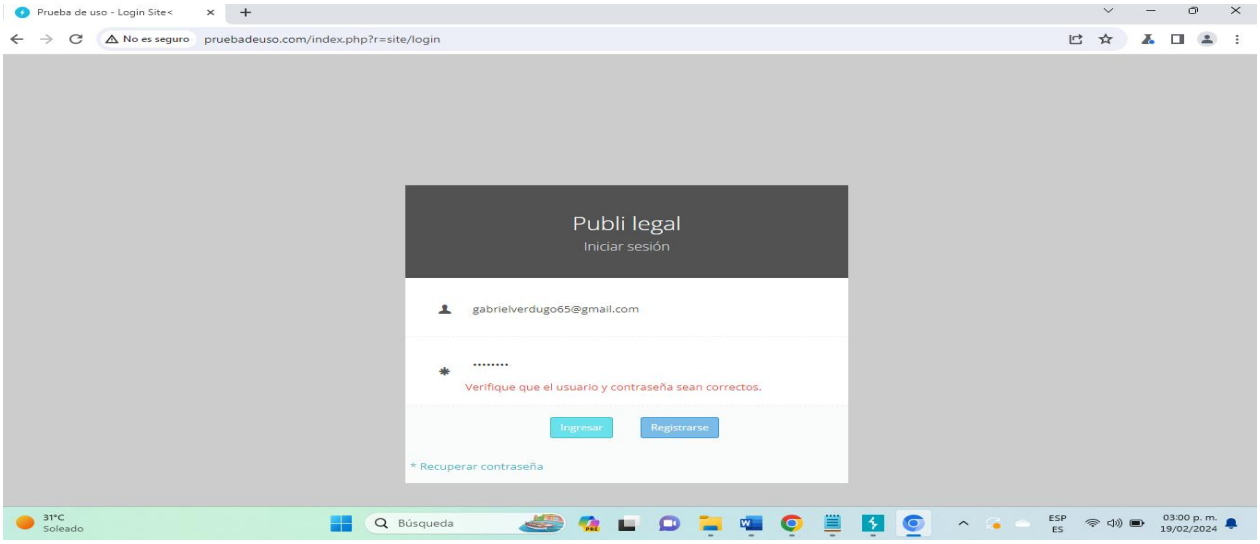


Iniciar sesión con las credenciales correctas y cómo podemos observar en Burp Suite a parecido la página que estamos interceptando, al final podemos ver las credenciales que inicio sesión y su contraseña.

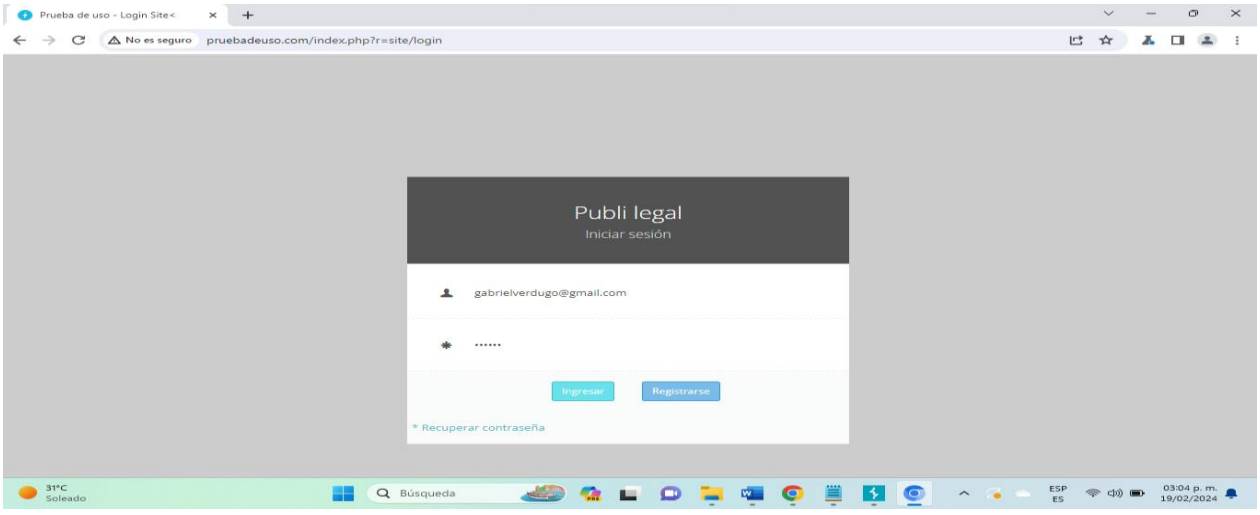




En esta imagen alteramos la contraseña como va del 1 al 6, le vamos agregar dos números más que seria 7 y 8. (La contraseña 12345678). Y le damos donde dice forward, como podemos observar nos manda un mensaje de error.



En esta segunda prueba vamos a alterar el correo electrónico gabrielverdugo65@gmail.com Ahora el correo se llamará gabrielverdugo@gmail.com eliminando los números del correo y le damos en forward.



CONCLUSION

Conocer y entender las vulnerabilidades establecidas en nuestro sitio web, con la ayuda de la herramienta Wireshark, podemos saber que estrategias de seguridad podemos implementar para evitar que nuestro software tenga vulnerabilidad y los datos puedan ser robados. En definitiva, para lograrlo, es vital saber cómo realizar auditorías que nos permita verificar la calidad y seguridad del programa o el sitio web que se está utilizando. Así es como identificar qué tipo de vulnerabilidad pudiéramos tener. La deserialización insegura es una vulnerabilidad crítica que ocurre cuando una aplicación o una API de serializa 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 softwares y sus usuarios, incluidas las dos amenazas que vimos en esta unidad número dos. En esta actividad hemos aprendido a utilizar la herramienta de trabajo de BurpSuite. y así poder hackear la información, para entrar en modo incognito a cierta página para poder hacer modificaciones en sus sistemas sin que se den cuenta los usuarios. El objetivo principal de este ataque es robar los datos de identidad de un usuario, como cookies, tokens de sesión y otra información. En la mayoría de los casos, este ataque se utiliza para robar las cookies del usuario. Como sabemos, las cookies nos ayudan a iniciar la sesión automáticamente. Por lo tanto, con las

cookies robadas, podemos iniciar sesión con otras identidades. Y esta es una de las razones por las que este ataque se considera uno de los más arriesgados.

REFERENCIAS BIBLIOGRAFICAS

Ramírez, H. (2023a, abril 5). *Pérdida de datos ¿qué es y cómo prevenirla?* Grupo Atico34. https://protecciondatos-lopd.com/empresas/perdida-datos/

Salmerón, A., & Salmerón, A. (2023, 9 septiembre). *¿Qué es Wireshark y para qué?* Informática y Tecnología Digital. https://informatecdigital.com/redes/que-es-wireshark-y-para-que/

Toledo, R. (2023, 24 mayo). ¿Cómo funcionan los datos de autenticación y por qué son importantes? *cibernos grupo*. https://www.grupocibernos.com/blog/como-funcionan-los-datos-de-autenticacion-y-por-que-son-tan-importantes

A07 Fallas de identificación y autenticación - OWASP Top 10:2021. (s. f.). https://owasp.org/Top10/es/A07_2021-Identification_and_Authentication_Failures/

The WhiteHat Panther. (2022, 17 marzo). *Hackeando Login Page por Fuerza Bruta -PortSwigger Academy* [Vídeo]. YouTube. https://www.youtube.com/watch?v=NOYfWjsobZg

dokkillo. (2021, 8 diciembre). *Access Control Lab: funcionalidad de administrador desprotegida con url no predictible* [Vídeo]. YouTube. https://www.youtube.com/watch?v=lQhJ7I-3wJw

Castillo, A. (2020, 8 mayo). *Ataques en Sistemas de Autenticación – OWASP Top 2*. https://es.linkedin.com/pulse/ataques-en-sistemas-de-autenticaci%C3%B3n-owasp-top-2-alexander-castillo

Bnke0x0. (2022b, abril 5). *User ID Controlled by Request Parameter With Password Disclosure | PortSwigger (Video solution)* [Vídeo]. YouTube. https://www.youtube.com/watch?v=b2TXT8AYUqY

Link github