****

**Actividad [#3]**

**[Cross Site Scripting (XSS) ]**

**[Auditoría Informática]**

**Ingeniería en Desarrollo de Software**

**Tutor: Jessica Hernández Romero**

**Alumno: Manuel Enrique Ramirez Lopez**

**Fecha: 13/02/2023**

***Indice***

*[Introduccion](#_Toc19530)* [1](#_Toc19530)

*[Descripción](#_Toc2849)* [2](#_Toc2849)

*[Justificación](#_Toc1530)* [3](#_Toc1530)

*[Etapa 1](#_Toc14407)* [4](#_Toc14407)

[Investigación de Pérdida de Autentificacion y Gestión de Sesiones 4](#_Toc7689)

[Descripción del sitio web 6](#_Toc1846)

[Ataque al sitio 7](#_Toc2819)

*[Etapa 2](#_Toc21902)* [8](#_Toc21902)

[Investigación de Deserialización Insegura 8](#_Toc30787)

[Ataque al sitio 9](#_Toc15506)

*[Etapa 3](#_Toc4109)* [11](#_Toc4109)

[Investigación 11](#_Toc855)

[Ataque al sitio 13](#_Toc13177)

*[Conclucion](#_Toc19332)* [14](#_Toc19332)

*[Referencias](#_Toc30393)* [15](#_Toc30393)

# *Introduccion*

Los ataques de secuencias de comandos entre sitios (XSS) pueden afectar gravemente a los usuarios de Internet al permitir que los atacantes ejecuten secuencias de comandos maliciosas en sus navegadores web. Estos scripts pueden robar información confidencial, como contraseñas e información bancaria, o redirigir a los usuarios a sitios web falsos y peligrosos. Además, los ataques XSS pueden comprometer la seguridad de los sitios web afectados y proporcionar a los atacantes acceso a la información del usuario y los datos del sitio web. Por lo tanto, es importante que los usuarios de Internet tomen precauciones para protegerse de los ataques XSS, como usar un software de seguridad actualizado y evitar hacer clic en enlaces sospechosos.

# *Descripción*

Se espera aprender sobre cómo el ataque de Cross Site Scripting puede permitir a los atacantes ejecutar scripts maliciosos en los navegadores web de los usuarios de Internet, lo que puede conducir a la revelación de información confidencial y al compromiso de la seguridad del sitio web afectado. También se espera aprender sobre las formas en que los usuarios pueden protegerse contra los ataques XSS y cómo los desarrolladores de sitios web pueden prevenir los ataques XSS mediante el uso de prácticas de codificación seguras y la validación adecuada de la entrada de usuario.

# *Justificación*

Un ataque de secuencias de comandos en sitios cruzados (XSS) es una técnica de ataque común que permite a los atacantes inyectar código malicioso en sitios web legítimos, comprometer la seguridad del sitio web y robar información confidencial del usuario. Los ataques XSS son una amenaza real y continua para los usuarios de Internet y los sitios web, y pueden tener graves consecuencias tanto para las personas como para las empresas. Por lo tanto, es importante que los desarrolladores de sitios web y los usuarios de Internet comprendan el riesgo de los ataques XSS y tomen medidas para protegerse contra ellos. Para mantenerse seguro en línea y proteger la información confidencial, es importante comprender cómo funcionan los ataques XSS y cómo prevenirlos.

# *Etapa 1*

## **Investigación de Pérdida de Autentificacion y Gestión de Sesiones**

Ataque de pérdida de autentificacion y gestión de sesiones

***¿Cómo funciona este ataque?***

Un ataque de pérdida de autentificacion y gestión de sesiones se basa en explotar vulnerabilidades en la implementación de la gestión de sesiones y autentificacion en una aplicación o sistema web. Por ejemplo, si un sitio web no implementa correctamente la expiación de sesiones, un atacante puede robar una sesión activa y acceder a información o realizar acciones con el permiso de la víctima. Otra técnica común es interceptar y manipular los tokens de sesión, lo que permite a un atacante tomar el control de una sesión existente. Para protegerse contra estos tipos de ataques, es importante implementar adecuadamente la gestión de sesiones y la autentificacion y asegurarse de seguir las mejores prácticas de seguridad recomendadas.

***¿Cómo afecta este tipo de ataques a los sitios y usuarios?***

Un ataque de pérdida de autentificacion y gestión de sesiones puede tener graves consecuencias para los sitios web y sus usuarios. Algunos de los efectos incluyen:

Robo de información confidencial: Los atacantes pueden acceder a información confidencial, como nombres de usuario y contraseñas, datos bancarios, información personal, etc.

Uso no autorizado de la cuenta de la víctima: Los atacantes pueden utilizar la cuenta de la víctima para realizar acciones fraudulentas, como compras en línea, transferir fondos, publicar contenido no deseado, etc.

Daño a la reputación: Un ataque exitoso puede dañar la reputación de un sitio web y disuadir a los usuarios de confiar en él en el futuro.

Costos de la respuesta a incidentes: Los sitios web pueden enfrentar costos significativos para investigar y corregir los efectos de un ataque de pérdida de autentificacion y gestión de sesiones.

Por lo tanto, es importante que los sitios web implementen medidas de seguridad adecuadas y sigan las mejores prácticas recomendadas para protegerse contra este tipo de ataques.

***¿Cómo se puede prevenir?***

Para prevenir un ataque de pérdida de autentificacion y gestión de sesiones, es importante seguir las siguientes mejores prácticas de seguridad:

Implementar autentificacion de dos factores (2FA): La autentificacion de dos factores proporciona una capa adicional de seguridad al requerir dos formas de identificación, como una contraseña y un código de seguridad enviado por mensaje de texto o autentificacion por aplicación.

Implementar tokens de sesión seguros: Los tokens de sesión deben ser únicos y seguros y deben expirar después de un período de tiempo corto.

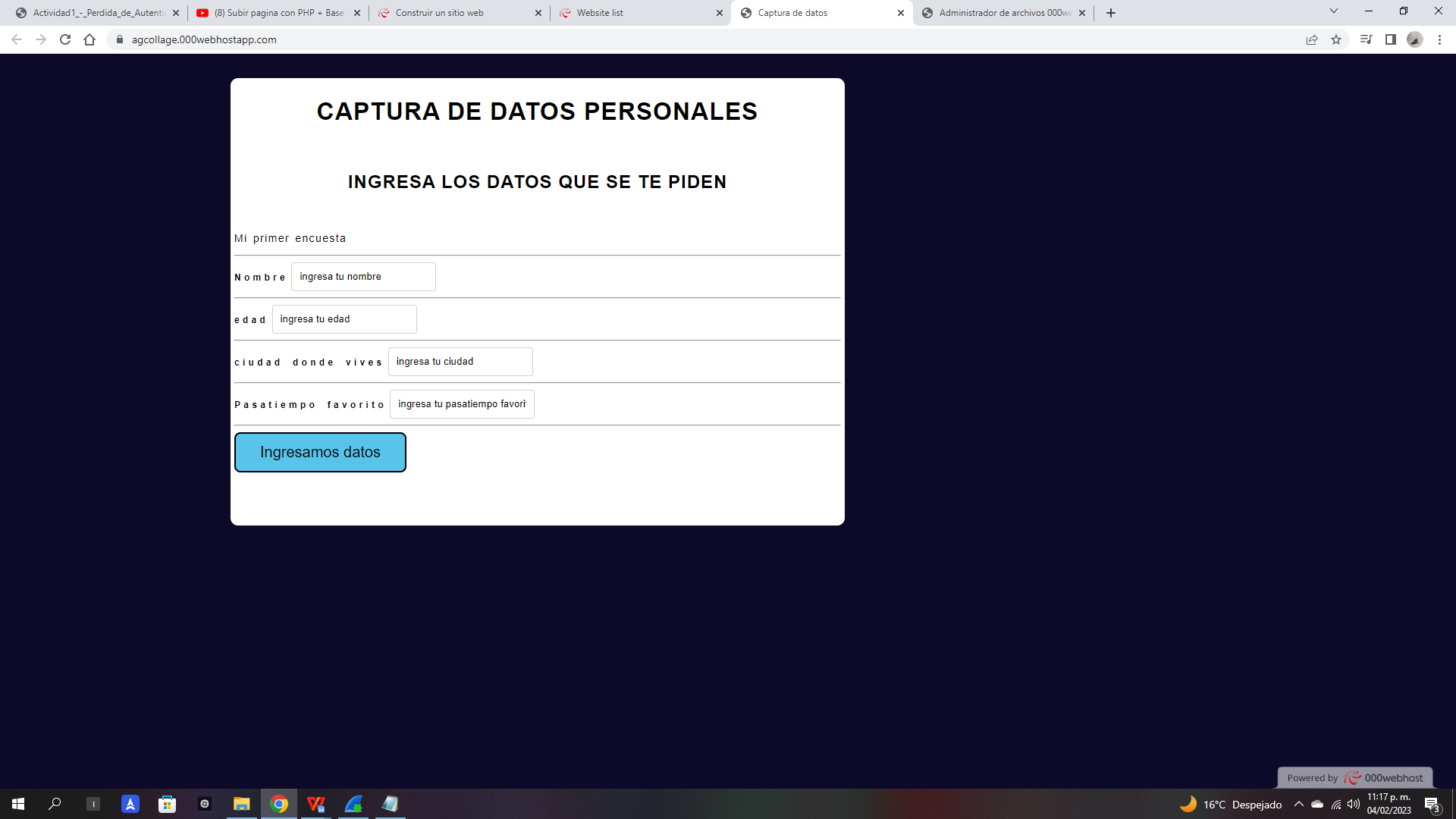
Almacenar contraseñas de manera segura: Las contraseñas deben ser almacenadas de manera segura, utilizando un algoritmo de hash seguro y una sal adicional.

Proteger la transmisión de datos: La transmisión de datos, incluidos los tokens de sesión, debe protegerse mediante cifrado SSL/TLS.

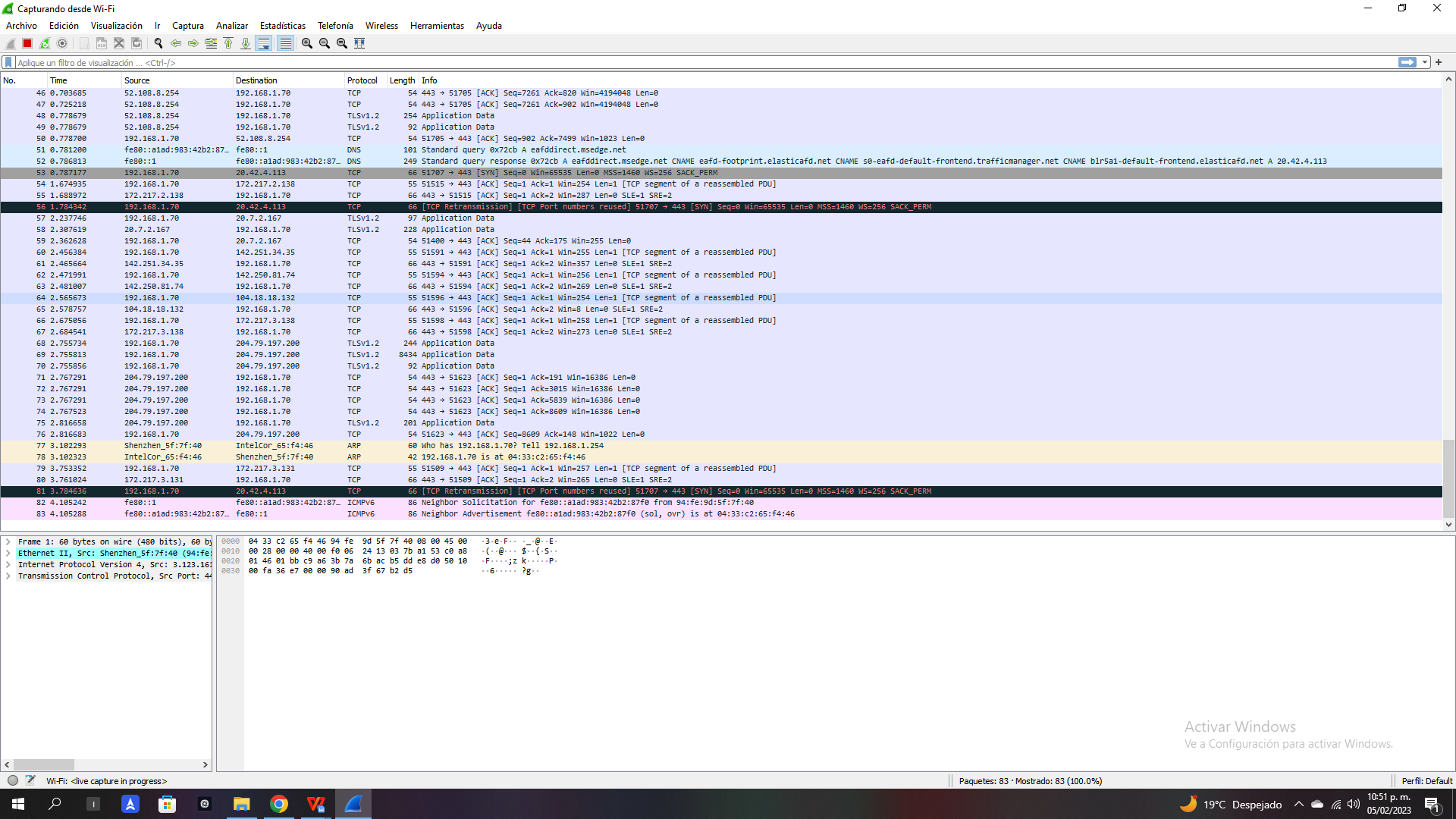
Realizar pruebas de penetración periódica: Es importante realizar pruebas de penetración periódica para identificar y corregir vulnerabilidades en la gestión de sesiones y autenticación.

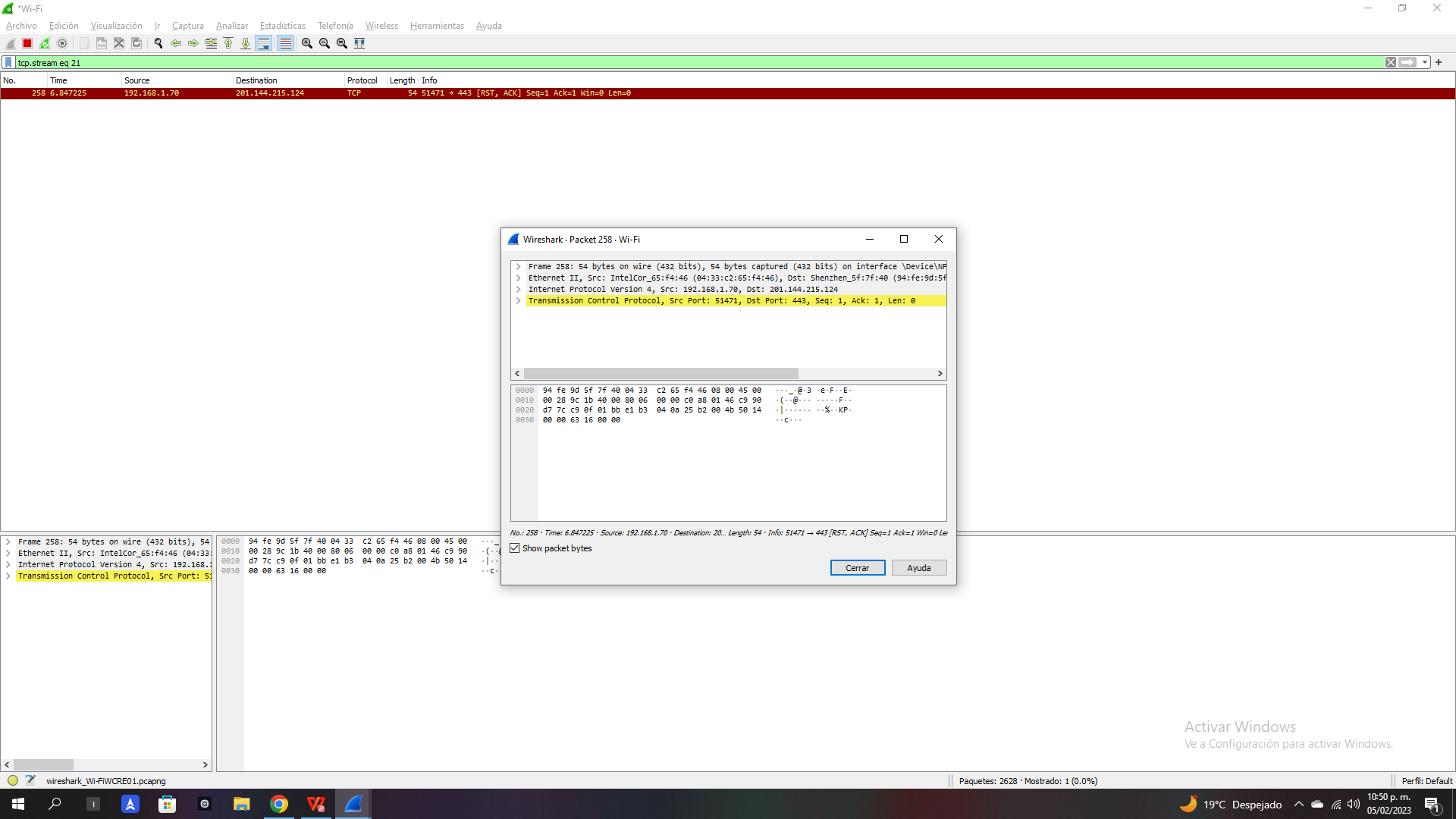
Además de estas medidas, es importante mantener actualizado sobre las últimas amenazas y vulnerabilidades y aplicar parches y actualizaciones de seguridad de manera oportuna.

## **Descripción del sitio web**

**Datos para el posterior registro donde arrojara mensaje personalizado.**

## **Ataque al sitio**

Paquetes enviados/ escaneados desde la opción Wifi



Seguimiento ante la apertura de inicio de sesión

# *Etapa 2*

## Investigación de Deserialización Insegura

***¿Cómo funciona este ataque?***

El interceptar informacion no encapsulada seria la forma mas sencilla de ejemplificar este tipo de ataque donde el atacante busca obtener acceso mediante terceros con autorización autentica donde envía ligas/ enlaces con código malicioso donde busca que haga clic y este agregue datos de acceso y por medio de la transferencia de datos “cookie” tomar dicha informacion y suplantar su acceso y ya una ves dentro poder hacer y desacer lo que tenga a su alcance.

***¿Cómo afecta este ataque a los software y sus usuarios?***

La deserialización insegura puede ser explotada por un atacante para ejecutar código malicioso en el sistema del usuario, lo que puede resultar en la fuga de información confidencial o el control total del sistema por parte del atacante. Los usuarios que utilizan software vulnerable a la deserialización segura están en riesgo de sufrir daños graves. Por lo tanto, es importante que los desarrolladores aborden este problema de seguridad e implementen medidas de protección adecuadas en sus aplicaciones.

***¿Cómo se puede prevenir?***

Algunas medias para prevenir:

Validación de entrada: Validar cuidadosamente todas las entradas antes de deserializarlas para asegurarse de que cumplan con los requisitos esperados y no contengan datos maliciosos.

Uso de bibliotecas seguras: Utilice bibliotecas de serialización que hayan sido dañadas de forma segura y hayan sido probadas rigurosamente.

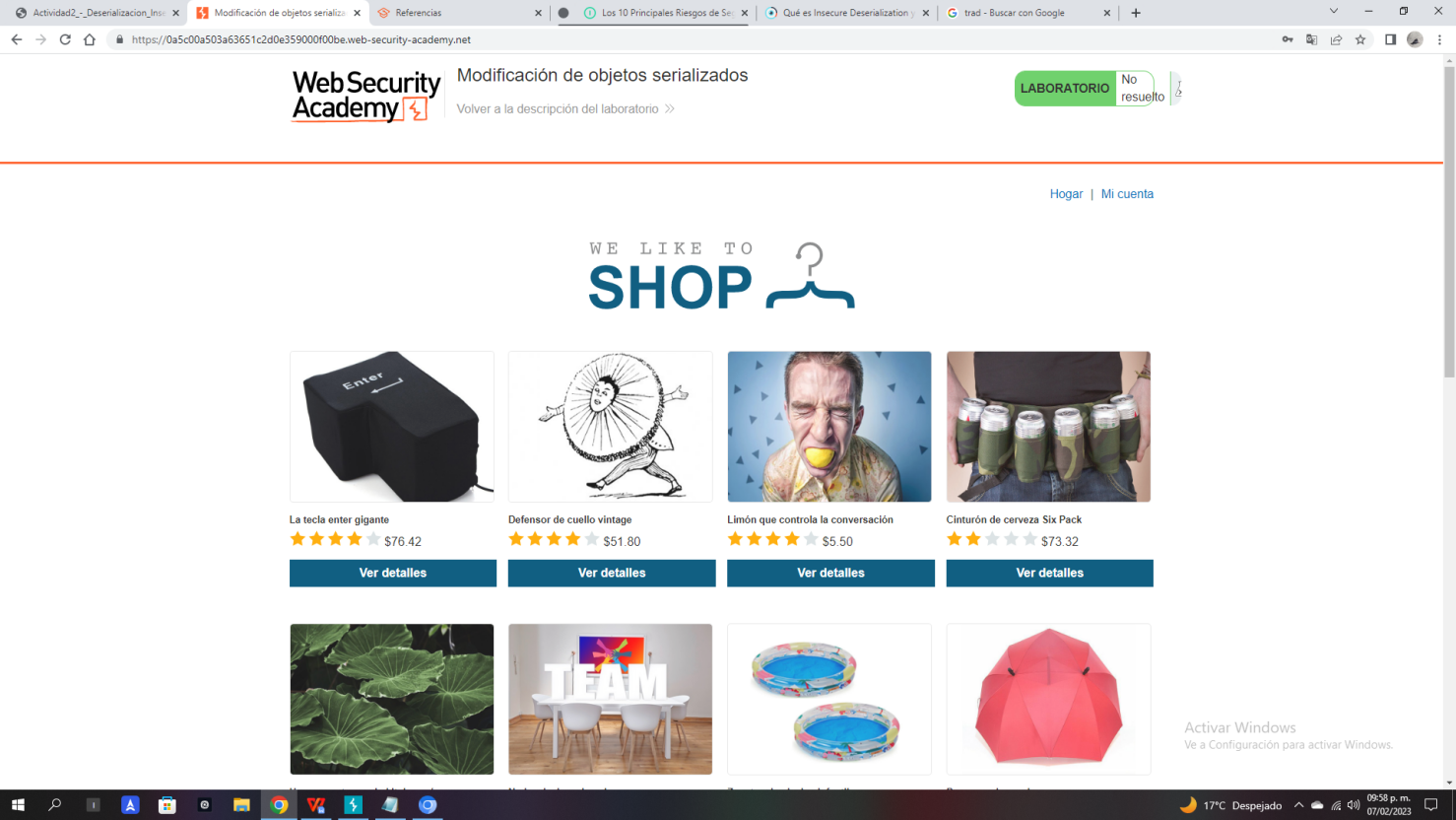
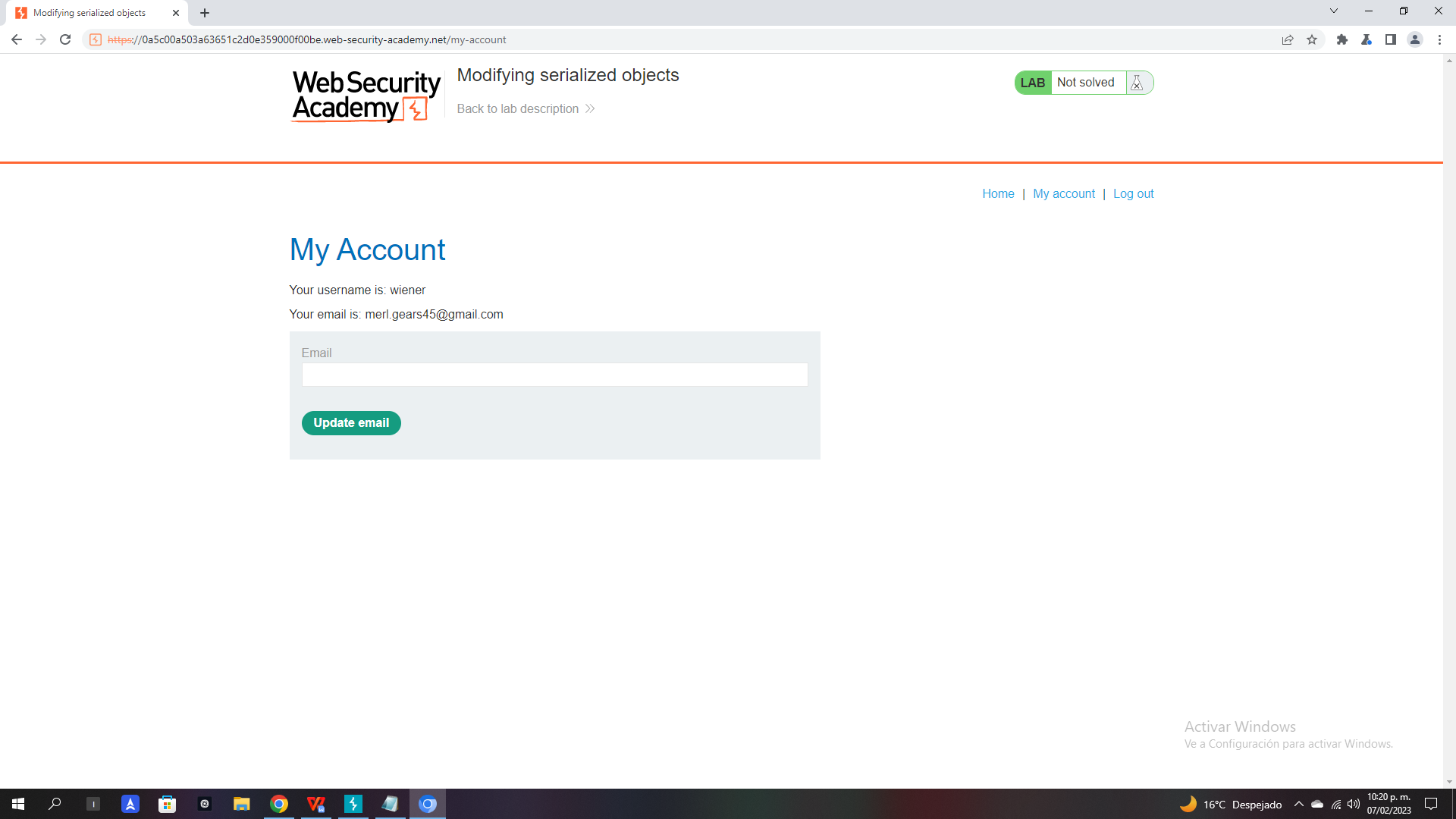
Desactivar la ejecución de código no confiable: Desactive la ejecución automática de código durante la deserialización para evitar la ejecución de código malicioso.

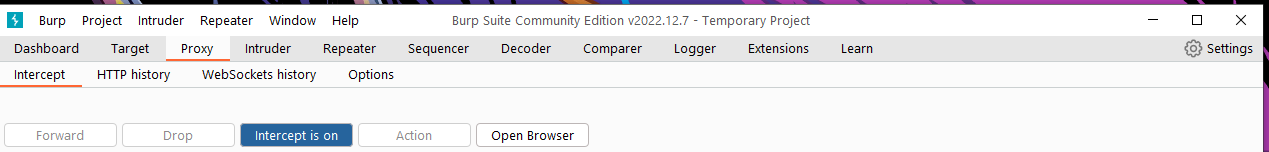
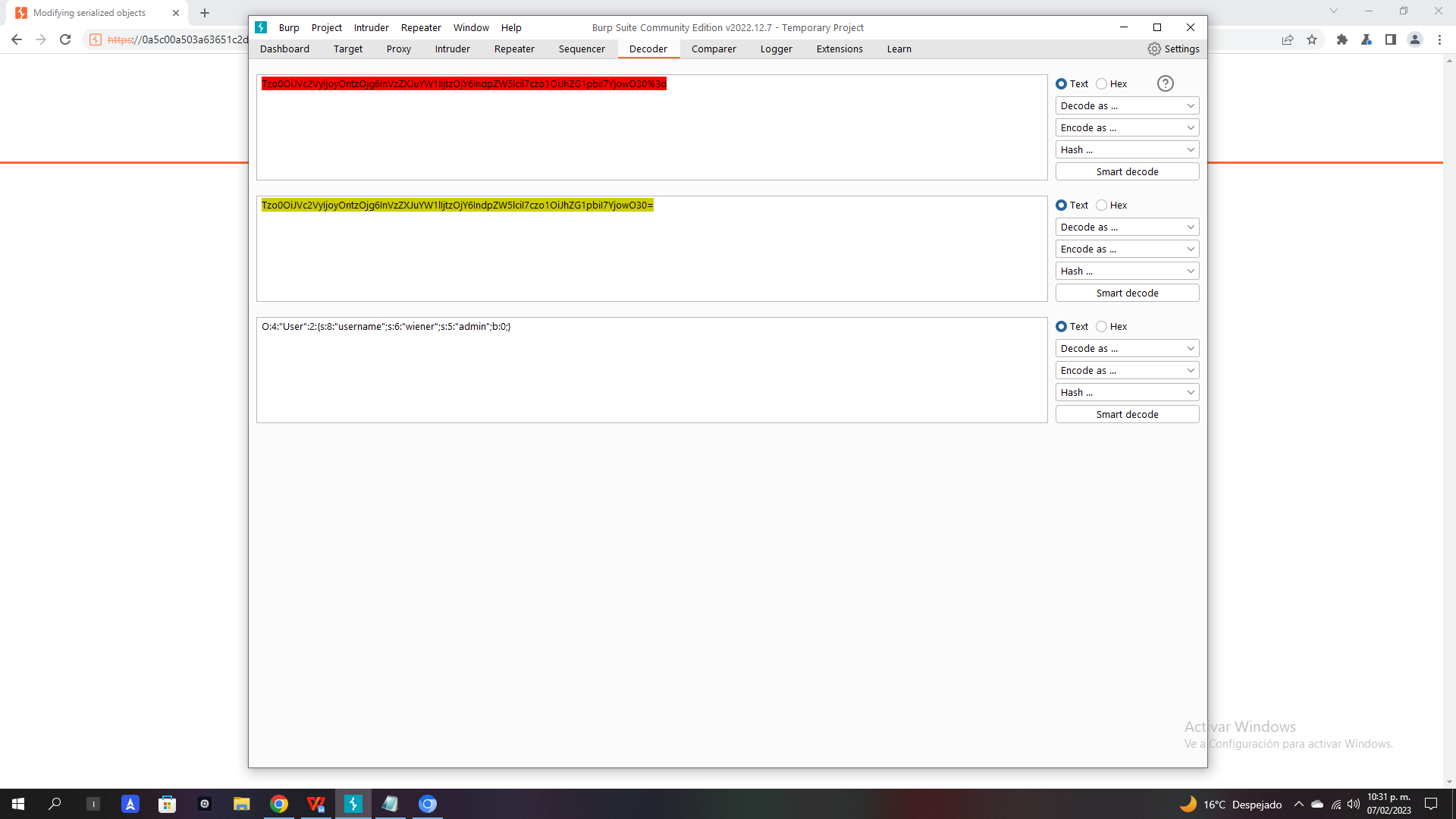
Verificación de firmas digitales: Verifique las firmas digitales de los objetos deserializados para asegurarse de que provienen de una fuente confiable.

Monitoreo y registro: Monitoreo y registro de las actividades relacionadas con la deserialización para detectar posibles ataques y tomar medidas para maximizar-los.

Es importante destacar que la prevención de la deserialización insegura es un proceso continuo y requiere la implementación de medidas de seguridad adecuadas, la revisión periódica de las prácticas de seguridad existentes y la actualización de las mismas en función de las nuevas amenazas y riesgos.

## Ataque al sitio



**

# *Etapa 3*

## Investigación

***¿Cómo funciona este ataque?***

Cross-site scripting (XSS) es un ataque que explota vulnerabilidades en páginas web. El ataque permite que un atacante inyecte código malicioso (generalmente JavaScript) en una página web legítima, lo que le permite ejecutar código malicioso en el navegador de un usuario que visita la página web infectada. Hay dos tipos principales de XSS:

XSS reflejado: este tipo de XSS ocurre cuando un atacante logra inyectar un script malicioso en una página web para que se ejecute inmediatamente cuando el usuario visita la página.

XSS persistente: este tipo de XSS ocurre cuando un atacante logra inyectar permanentemente un script malicioso en una página web, lo que significa que cualquier usuario que visite la página se verá perjudicado por el código malicioso.

De cualquier manera, los atacantes pueden robar información confidencial de los usuarios, como nombres de usuario y contraseñas.

***¿Cómo afecta este ataque a los software y sus usuarios?***

El Cross-Site Scripting (XSS) puede tener un impacto significativo en los software y sus usuarios. Algunos de los efectos más comunes incluyen:

Robo de información: El atacante puede utilizar el código malicioso para robar información confidencial del usuario, como contraseñas, nombres de usuario, direcciones de correo electrónico, y otros datos sensibles.

Modificación de la página web: El atacante también puede modificar el contenido de la página web infectada, lo que puede confundir a los usuarios

***¿Cómo se puede prevenir?***

Existen varias formas de prevenir el Cross-Site Scripting (XSS), incluyendo:

Validación de entrada: Verificar y validar todas las entradas del usuario antes de incluirlas en una página web. Esto incluye escapar o codificar todas las entradas para evitar que se interpreten como código malicioso.

Sanitización de salida: Escapar o codificar todas las salidas para asegurarse de que no se interpreten como código malicioso.

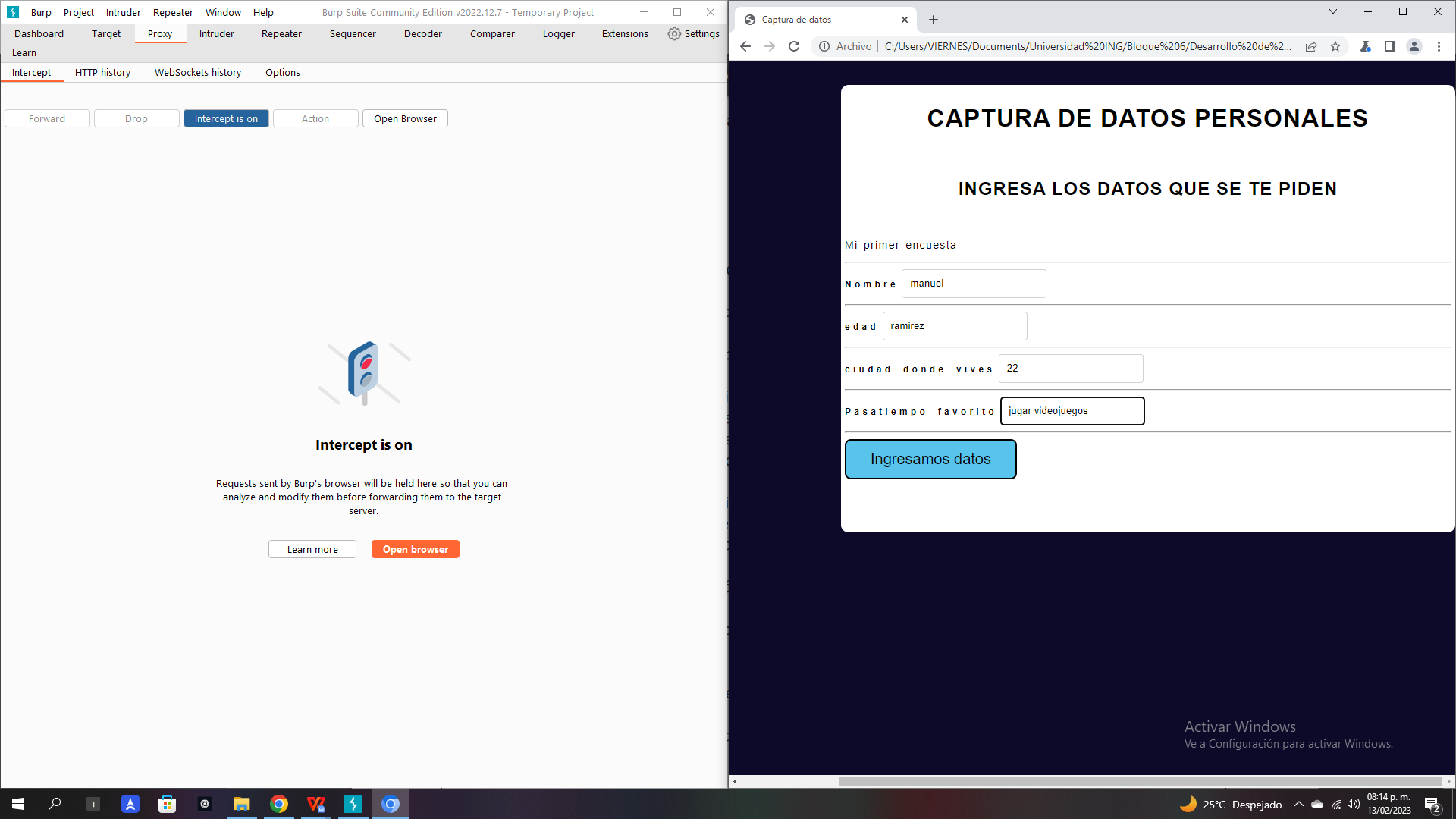
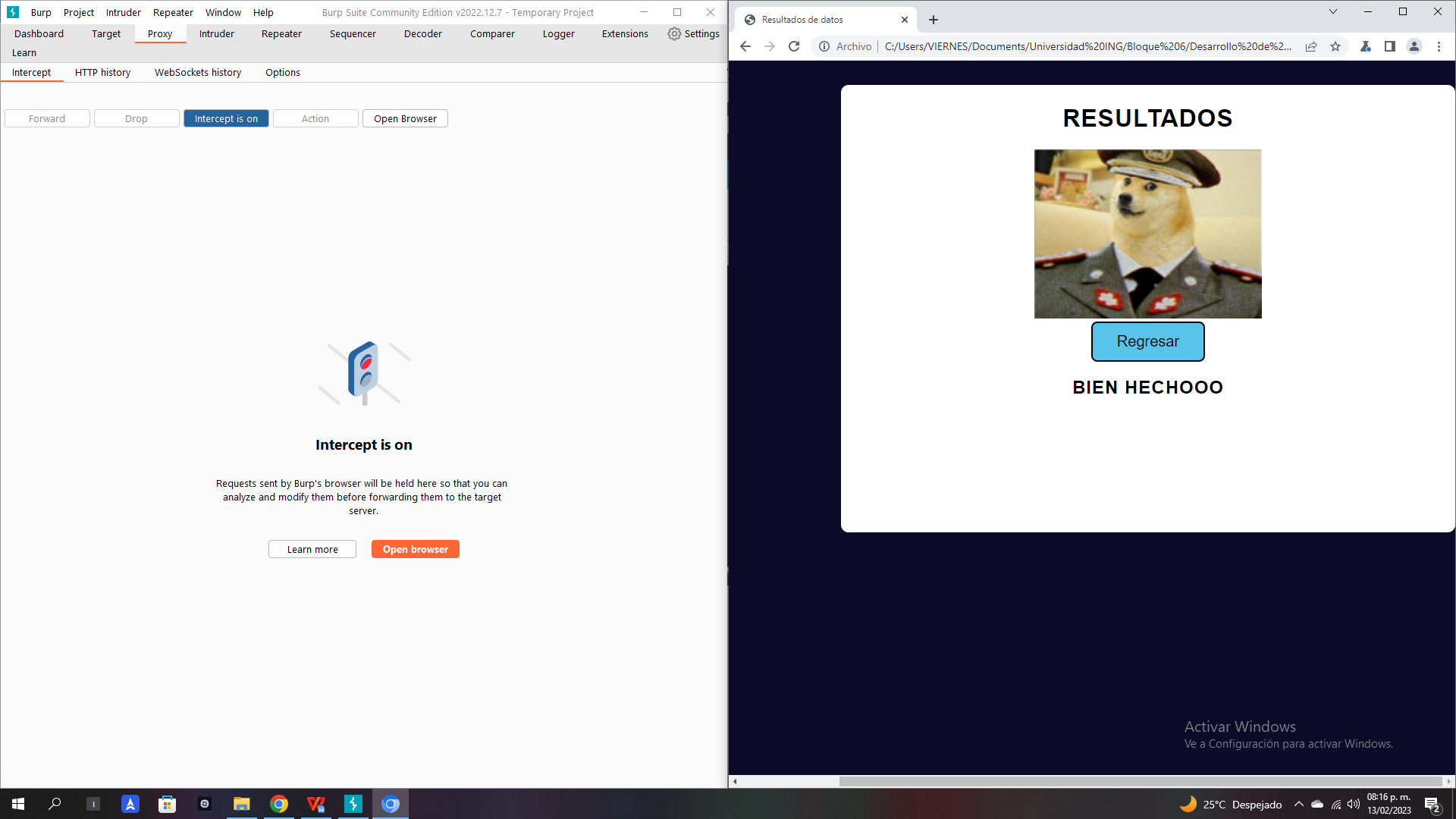
Utilización de políticas de seguridad: Configurar políticas de seguridad, como la política de mismo origen, para limitar la ejecución de scripts en una página web.

Uso de librerías y marcos seguros: Utilizar librerías y marcos que hayan sido diseñados para prevenir automáticamente ataques XSS.

Educación de los desarrolladores: Capacitar a los desarrolladores sobre la importancia de prevenir ataques XSS y proporcionarles herramientas y recursos para hacerlo.

Es importante tener en cuenta que prevenir el XSS es un proceso continuo que requiere una combinación de medidas técnicas y humanas. Además, es fundamental estar atento a las nuevas técnicas y métodos de ataque, y ajustar la prevención en consecuencia.

## Ataque al sitio



# *Conclucion*

En pocas palabras, Cross-Site Scripting (XSS) es un tipo de ataque que usa vulnerabilidades en páginas web para inyectar código malicioso en páginas web legítimas. Dichos ataques pueden tener graves consecuencias para el software y sus usuarios, incluido el robo de información confidencial y la alteración del contenido de las páginas web. La prevención de XSS incluye medidas técnicas como la validación de entrada y la corrección de salida, así como el uso de políticas de seguridad y bibliotecas y marcos de seguridad. Aunque por parte de esta practica no se haya podido realizar correctamente por la manera en que se creo/diseño en su tiempo, se entiende que cada sitio web pagina es única en cuanto su sistema y cada una de ellas puede llegar a tener su propia vulnerabilidad, nuestro deber es saber como corregir y pre-veer las posibles infiltraciones.

# *Referencias*

*Bloquear el XSS y subsanar vulnerabilidades*. (2019, 22 agosto). IONOS Digital Guide. <https://www.ionos.mx/digitalguide/paginas-web/desarrollo-web/que-es-el-xss-o-cross-site-scripting/>

Gómez, P. (2022, 19 mayo). *Qué es un ataque XSS o Cross Site Scripting*. ICM. <https://www.icm.es/2022/05/11/cross-site-scripting-ataque-xss/>

Education, I. S. (2021, 7 enero). *XSS: qué es y cómo funciona el Cross Site Scripting*. Blog de Tecnología - IMF Smart Education. <https://blogs.imf-formacion.com/blog/tecnologia/xss-que-es-y-como-funciona-201805/>