Universidad Corporativa | Programas Académicos

Ingeniería en Desarrollo de Software

Actividad |2| Deserialización Insegura.

Auditoría Informática.

Ingeniería en Desarrollo de Software.

TUTOR: Jessica Hernández Romero.

ALUMNO: Ramón Ernesto Valdez Felix.

FECHA: 24/10/2025.

Introducción.---------- 3

Descripción.---------- 3

Justificación. ---------- 4

Desarrollo.---------- 4

Ataque al sitio.---------- 5

Conclusion. ----------14

Referencias.----------15

Introducción.

En esta segunda actividad de la materia Auditoría Informática, en el marco de una auditoría de seguridad solicitada por una empresa de software, la presente actividad se enfoca en la identificación y explotación de una vulnerabilidad crítica: la deserialización insegura. Esta prueba forma parte de una evaluación exhaustiva a páginas web que carecen de medidas de seguridad robustas.

El objetivo principal es demostrar cómo un atacante puede lograr la escalada de privilegios de un usuario normal a administrador, manipulando las cookies de sesión. La aplicación objetivo utiliza un mecanismo de sesión basado en la serialización de objetos, lo que la hace susceptible a esta falla. Para ejecutar el ataque, emplearemos la herramienta Burp Suite Community Edition sobre un laboratorio simulado de PortSwigger. El ejercicio práctico consiste en iniciar sesión con credenciales básicas (wiener/peter), interceptar el tráfico y editar el objeto serializado dentro de la cookie para obtener acceso administrativo, culminando con la eliminación de la cuenta de "Carlos" para validar el éxito de la prueba.

Descripción.

Esta segunda actividad de Auditoría Informática, se busca realizar una prueba de seguridad de deserialización insegura en una aplicación web, un fallo de diseño que permite la escalada de privilegios. El contexto es una empresa de software que solicita un pentesting a páginas sin medidas de seguridad. El objetivo específico es explotar una vulnerabilidad en el mecanismo de sesión, el cual se basa en la serialización de objetos dentro de una cookie de sesión.

La actividad práctica consiste en utilizar la herramienta Burp Suite Community Edition sobre un laboratorio de la plataforma PortSwigger. Inicialmente, se debe iniciar sesión con credenciales de usuario normal (wiener/peter). Posteriormente, se debe interceptar y modificar la cookie de sesión que contiene el objeto serializado. Editando este objeto para cambiar el rol de usuario normal a administrador, se logra la escalada de privilegios. La prueba culmina al eliminar la cuenta del usuario "Carlos" desde la sesión con privilegios administrativos. Este ataque demuestra el riesgo de la deserialización insegura.

Justificación.

La justificación para realizar esta prueba de deserialización insegura radica en la necesidad crítica de evaluar la postura de seguridad de las aplicaciones de la empresa, especialmente aquellas que carecen de "candados de seguridad". La deserialización insegura es una vulnerabilidad de alto impacto, catalogada en el Top 10 de riesgos, que puede llevar a la ejecución remota de código (RCE) o, como en este caso, a una escalada de privilegios no autorizada.

Al simular un ataque que explota el mecanismo de sesión basado en la serialización mediante la manipulación de cookies con Burp Suite, se demuestra el riesgo real de que un usuario con privilegios mínimos (wiener/peter) pueda obtener acceso de administrador. El éxito al eliminar la cuenta de "Carlos" verifica la vulnerabilidad y proporciona evidencia tangible del fallo. Esta prueba es esencial para justificar la inversión en la implementación de validaciones y mecanismos de serialización seguros, previniendo así un potencial compromiso de datos o control total del sistema.

Desarrollo.

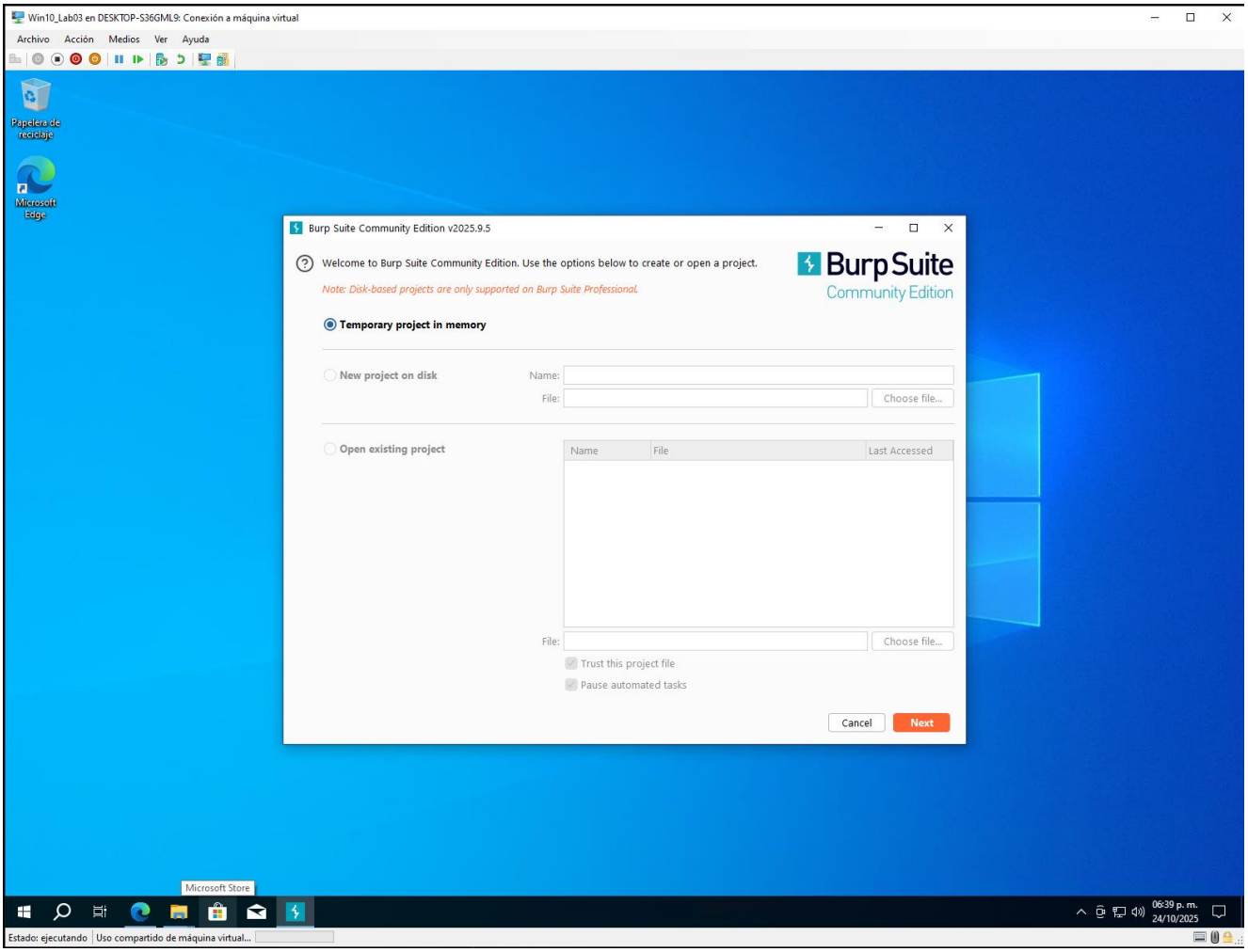
En esta parte de la actividad nos enfocaremos a realizar la actividad y la documentación de cada uno de los pasos a seguir del material de la materia de Auditoría Informática para realizar el ataque al sitio demostrando cómo un atacante puede lograr la escalada de privilegios de un usuario normal a administrador y editar el objeto serializado dentro de la cookie, culminando con la eliminación de la cuenta de "Carlos". A continuación realizaremos la documentación de la evidencia de la actividad donde se dará un breve explicación de cada uno de los pasos que se realizaron, solamente omitiendo la instalación de la herramienta y registro de la misma.

Link: GitHub.

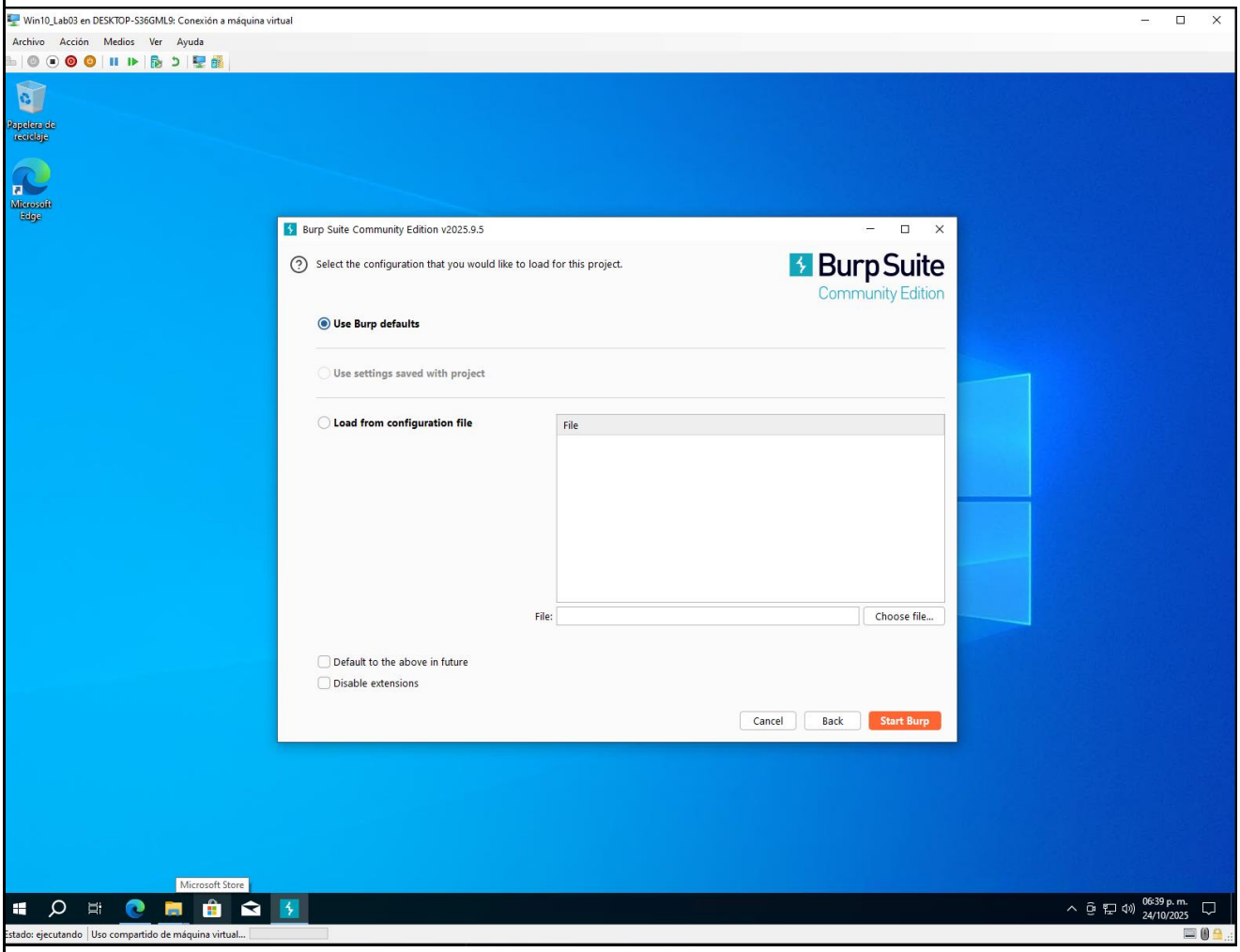
Ataque al sitio.

Antes del ataque del sitio:

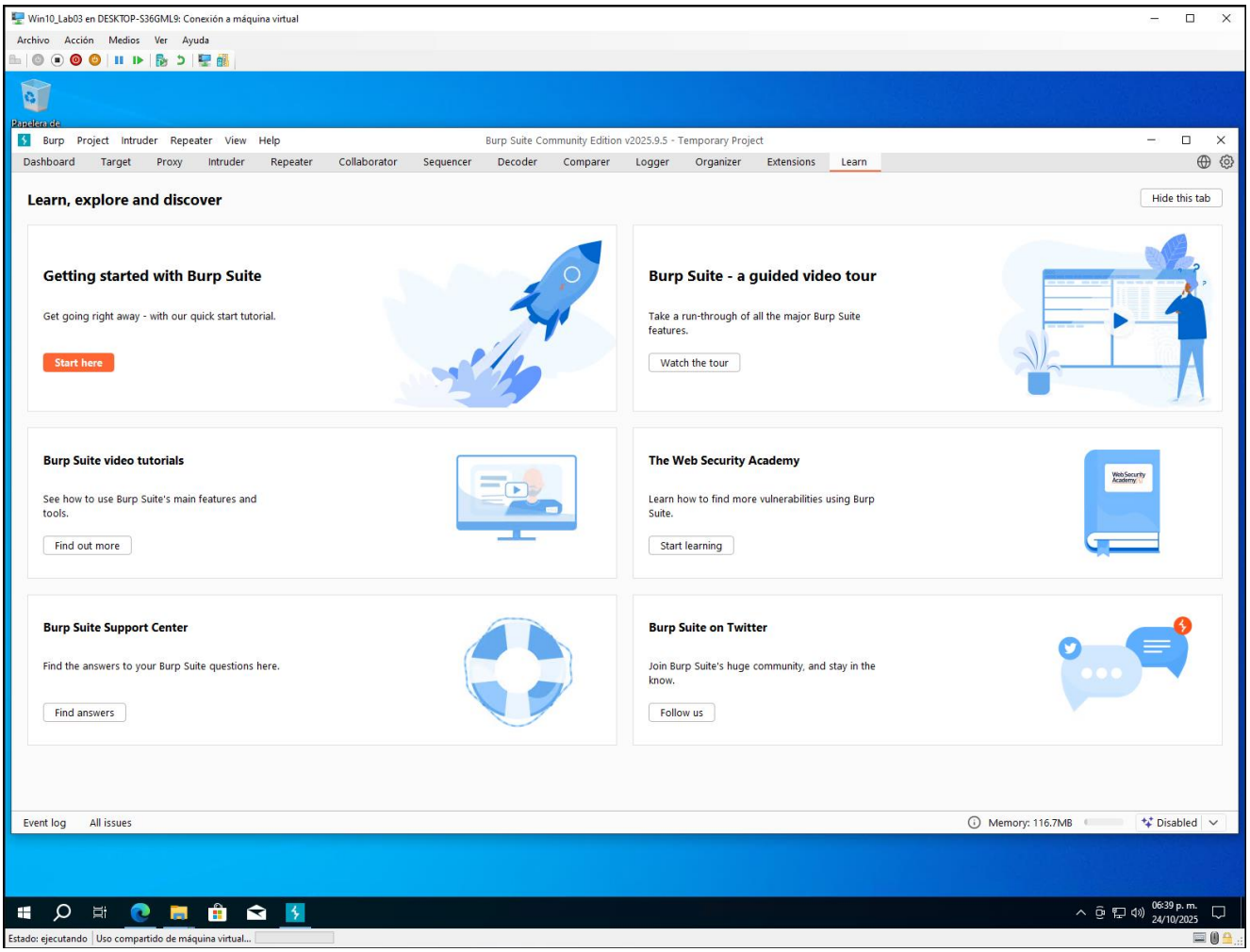
En este punto de la actividad empezamos con la pantalla del proyecto temporal con el que trabajaremos para el ataque del sitio dejándolo con la configuración default.



Continuamos con el punto siguiente donde se muestra la pantalla de use burp default que nos dice que utilizaremos la configuración default y que presionemos el botón de Start burp para iniciar la herramienta.

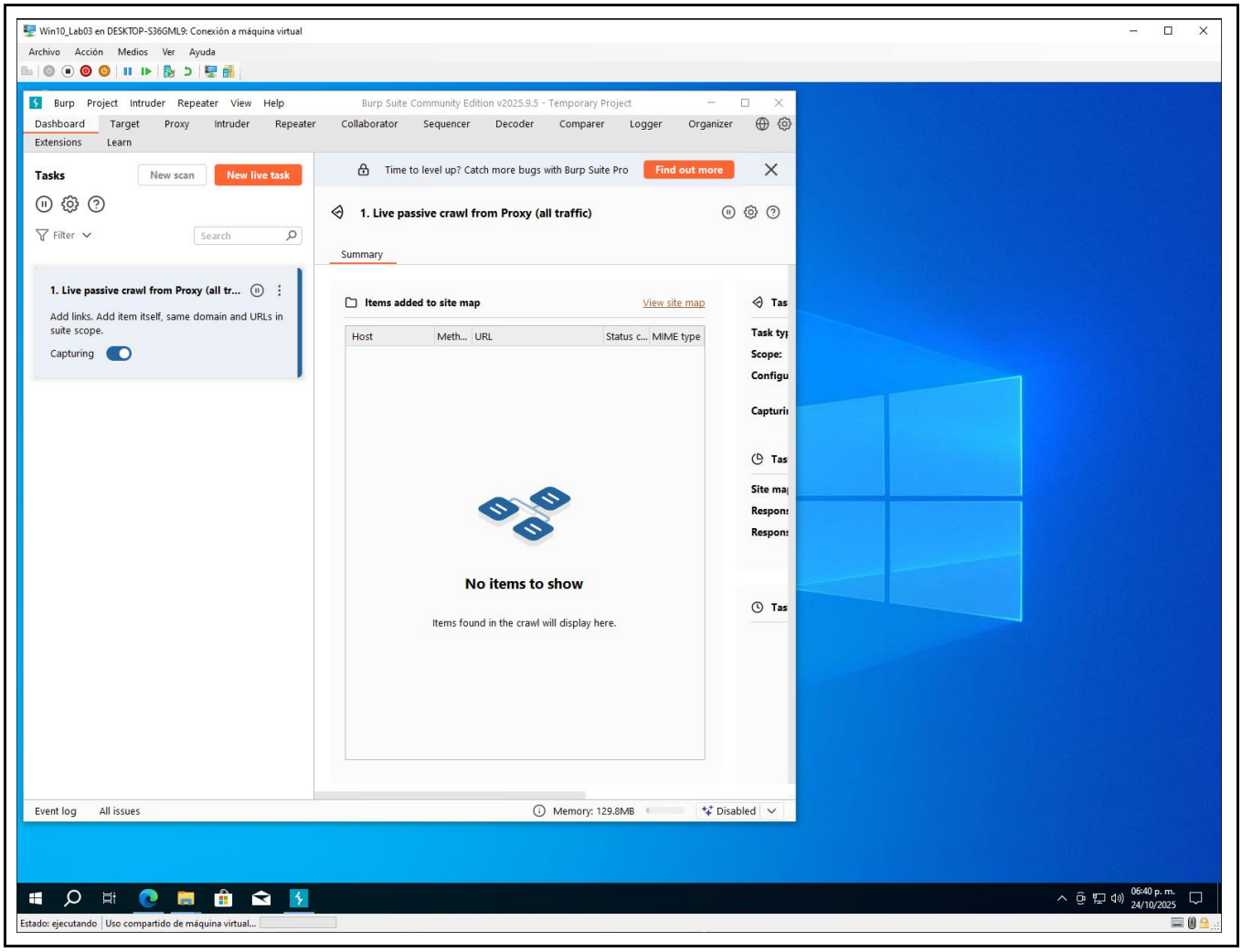


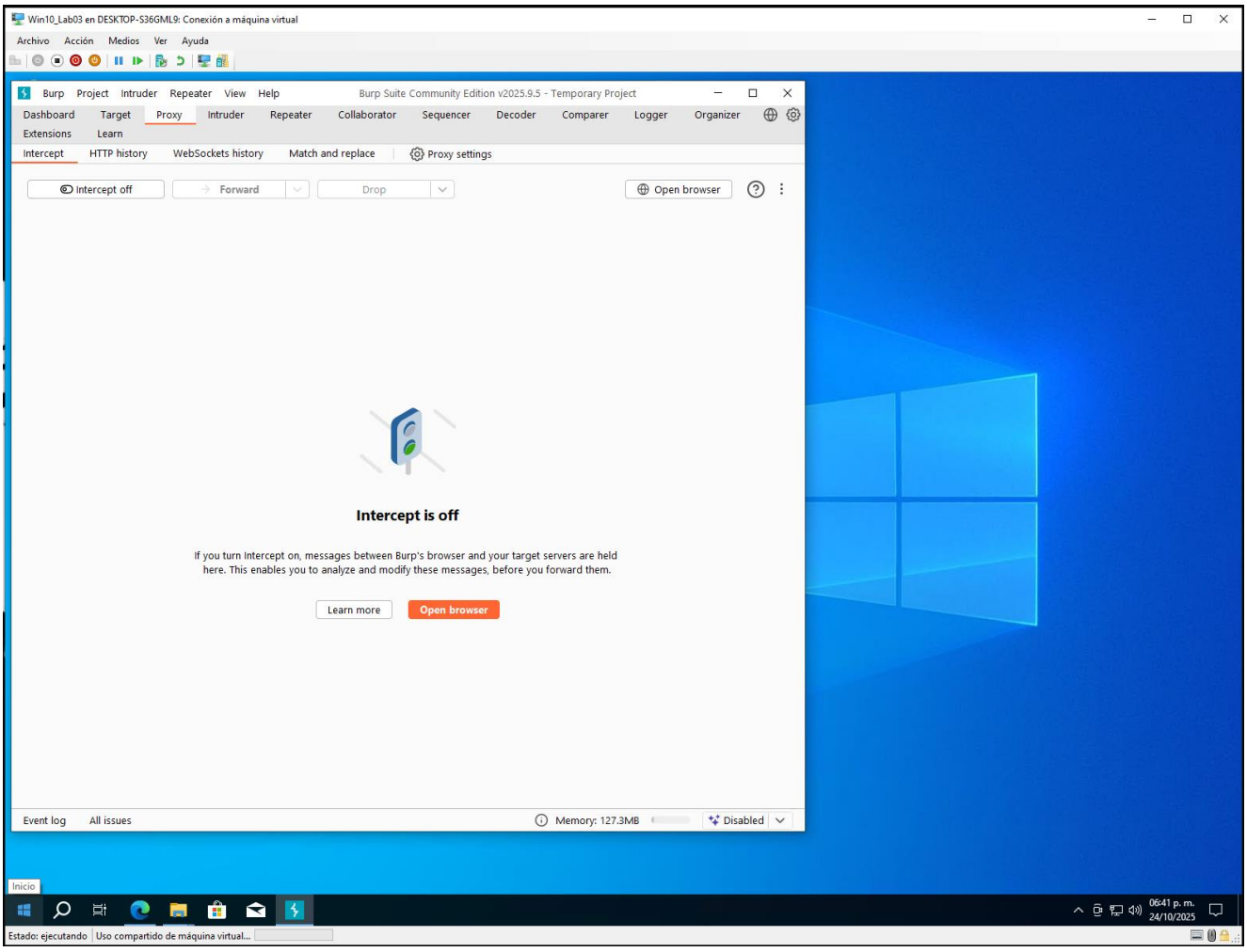
Aquí ya se nos muestra la pantalla principal de la herramienta ya abierta y lista para ser utilizada.



En este punto continuamos con los pasos que se mostraban en la documentación de la actividad donde niciaba con una pantalla de dashboard y después se cambiaba a la opción a utilizar que era la pestaña de proxy y estando en pestaña se mandaba llevar el navegador de la herramienta de burp e ingresamos el sitio del laboratorio.

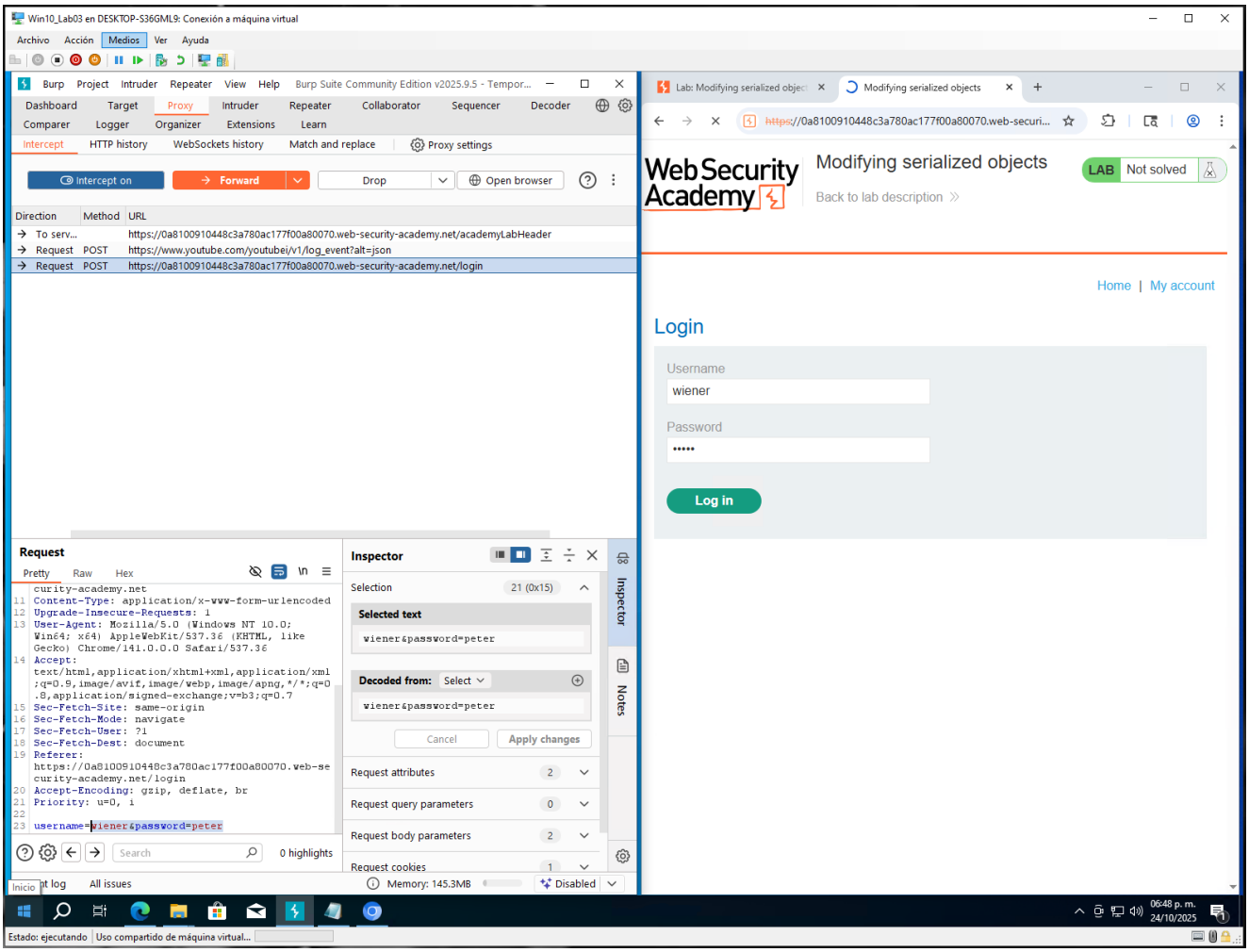
8

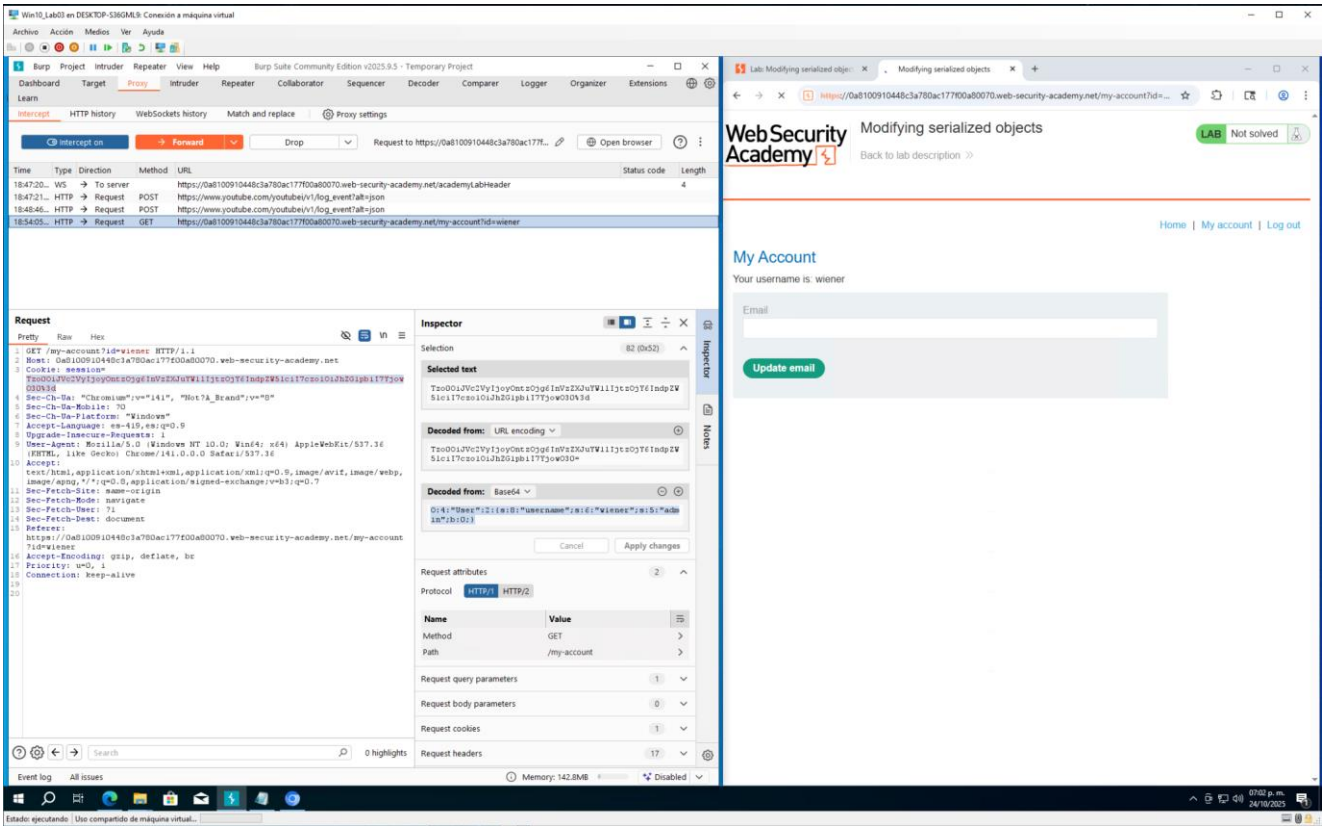

Win10_Lab03 en DESKTOP-S36GML9: Conexión a máquina virtual
Archivo Acción Medios Ver Ayuda
Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.9.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer
Extensions Learn
Tasks
New scan
New live task
Time to level up? Catch more bugs with Burp Suite Pro
Find out more
1. Live passive crawl from Proxy (all traffic)
Filter
Search
Summary
1. Live passive crawl from Proxy (all tr...
Add links. Add item itself, same domain and URLs in suite scope.
Capturing
Items added to site map
View site map
Host
Meth...
URL
Status c...
MIME type
No items to show
Items found in the crawl will display here.
Event log
All issues
Memory: 129.8MB
Disabled
06:40 p. m.
24/10/2025
Estado: ejecutando
Uso compartido de máquina virtual...



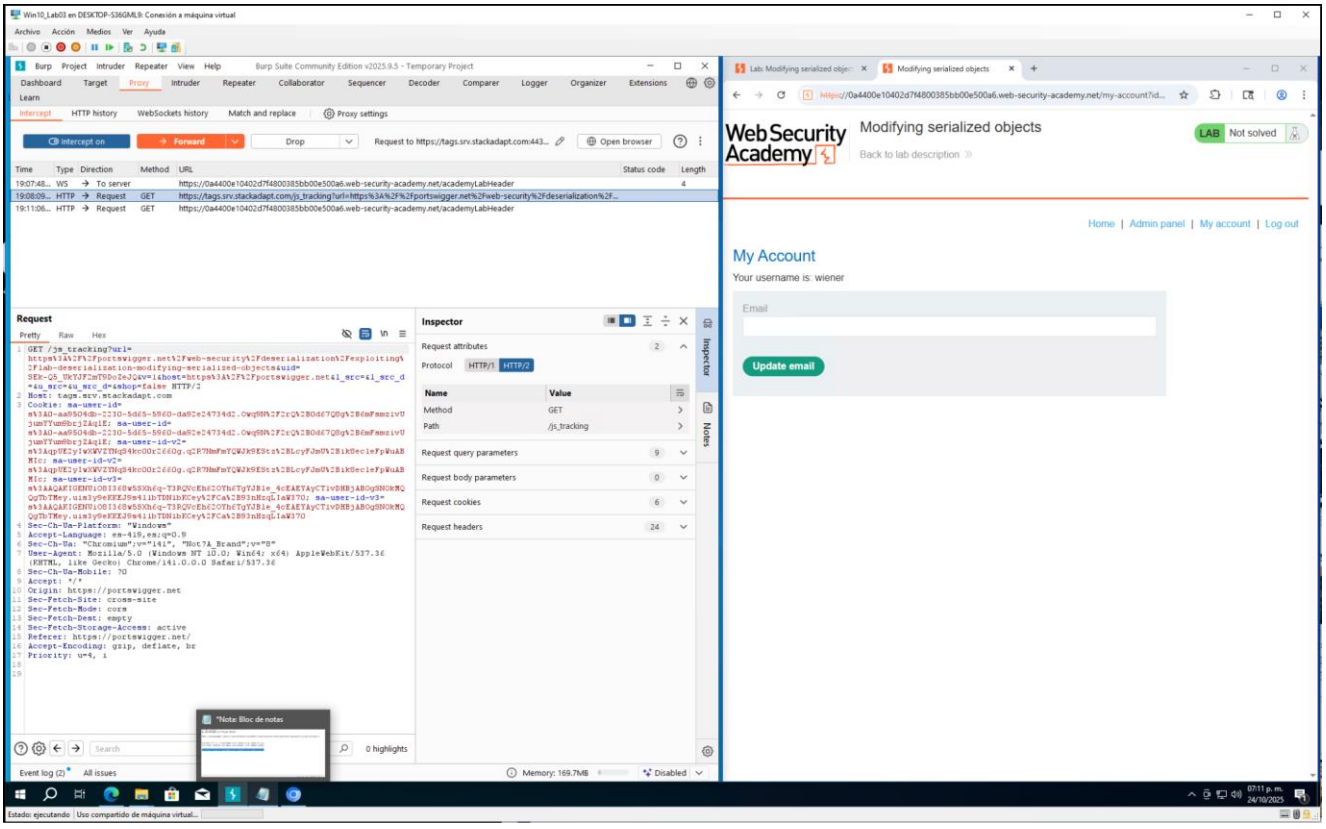
Ataque del sitio:

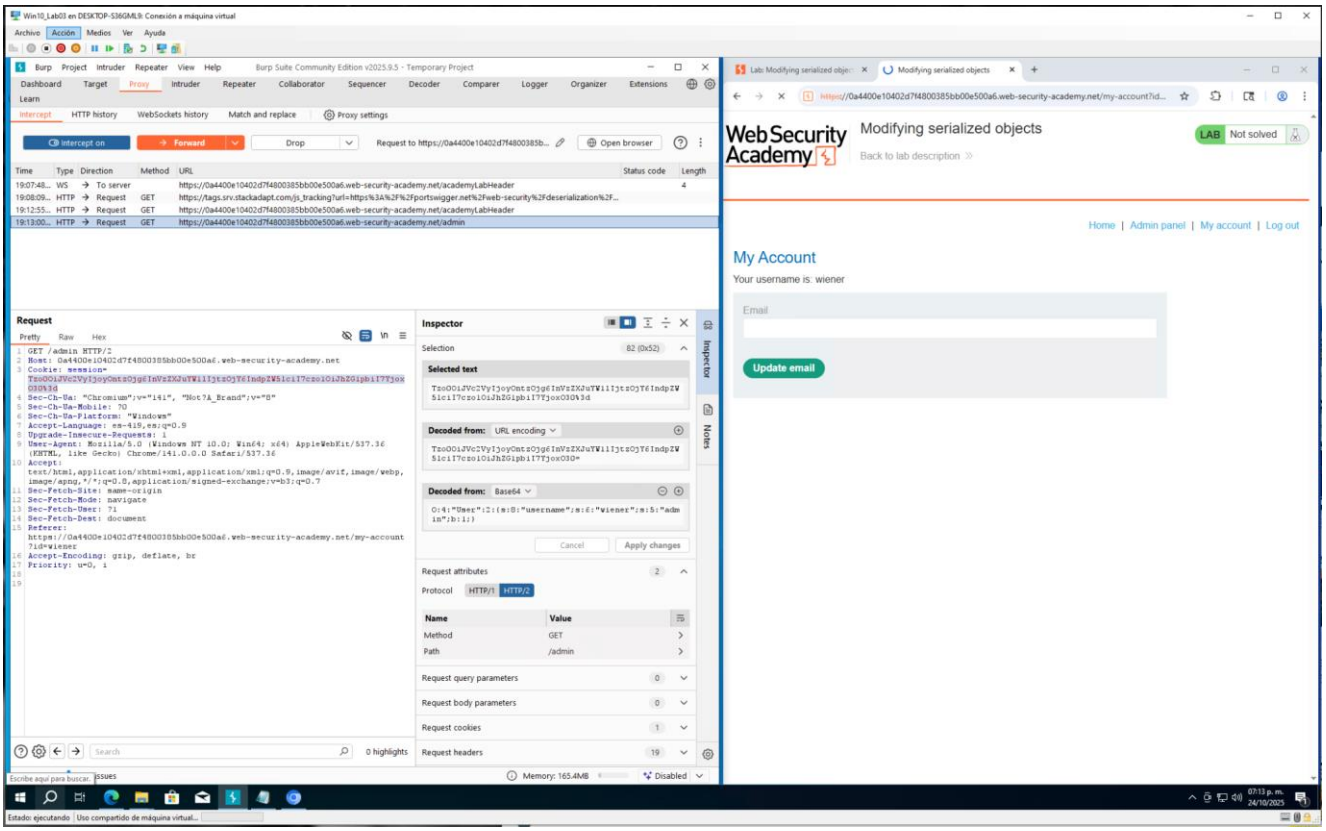
En este punto ya ingresamos al punto donde se presiono el botón de intercept off mostrandose en ntercept on y nos muestra el usuario/clave (wiener/peter) y presionamos el botón de Forward para el nicio de sesión, mostrando la pantalla de my account y mostrando un cuadro de diálogo para asignar una cuenta de email.


Win10_Lab03 en DESKTOP-S36GML9: Conexión a máquina virtual
Archivo Acción Medios Ver Ayuda
Burp Project Intruder Repeater View Help Burp Suite Community Edition v2025.9.5 - Tempor...
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder
Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on Forward Drop Open browser
Direction Method URL
To serv... https://0a8100910448c3a780ac177f00a80070.web-security-academy.net/academyLabHeader
Request POST https://www.youtube.com/youtubei/v1/log_event?alt=json
Request POST https://0a8100910448c3a780ac177f00a80070.web-security-academy.net/login
Request
Pretty Raw Hex
curity-academy.net
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0a8100910448c3a780ac177f00a80070.web-security-academy.net/login
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
username=wiener&password=peter
Search 0 highlights
Inspector
Selection 21 (0x15)
Selected text
wiener&password=peter
Decoded from: Select
wiener&password=peter
Cancel Apply changes
Request attributes 2
Request query parameters 0
Request body parameters 2
Request cookies 1
Inspector Notes
Event log All issues
Memory: 145.3MB Disabled
Lab: Modifying serialized objec
Modifying serialized objects
https://0a8100910448c3a780ac177f00a80070.web-securi...
Web Security Academy
Modifying serialized objects
Back to lab description
LAB Not solved
Home | My account
Login
Username
wiener
Password
Log in
Estado: ejecutando Uso compartido de máquina virtual...

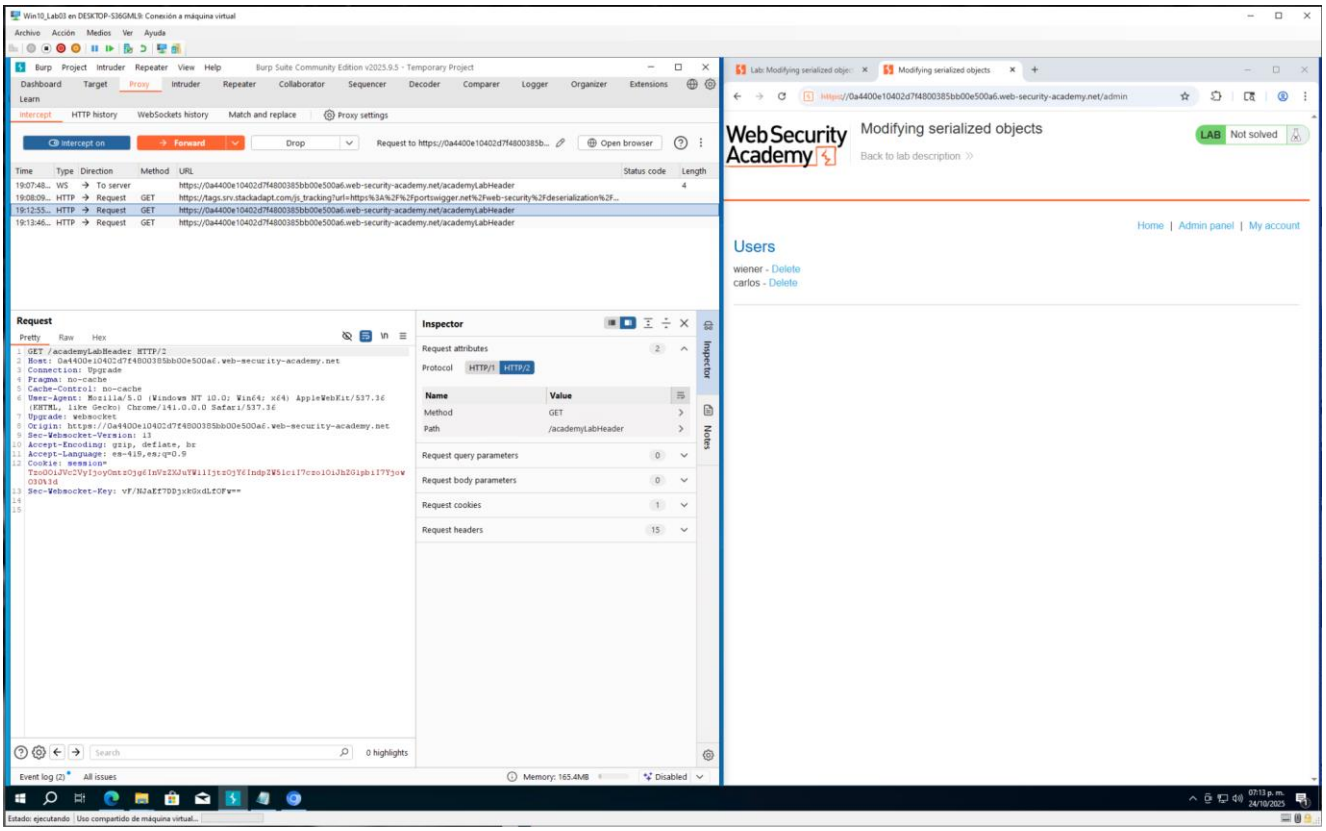

Win10_Lab03 en DESKTOP-S36GML9: Conexión a máquina virtual
Web Security Academy
Modifying serialized objects
Back to lab description
LAB Not solved
Home | My account | Log out
My Account
Your username is: wiener
Email
Update email
Request
Inspector
Selection
Selected text
Decoded from: URL encoding
Decoded from: Base64
Request attributes
Protocol HTTP/1 HTTP/2
Name Value
Method GET
Path /my-account
Request query parameters
Request body parameters
Request cookies
Request headers
Event log All issues
Memory: 142.8MB Disabled
Estado: ejecutando Uso compartido de máquina virtual...

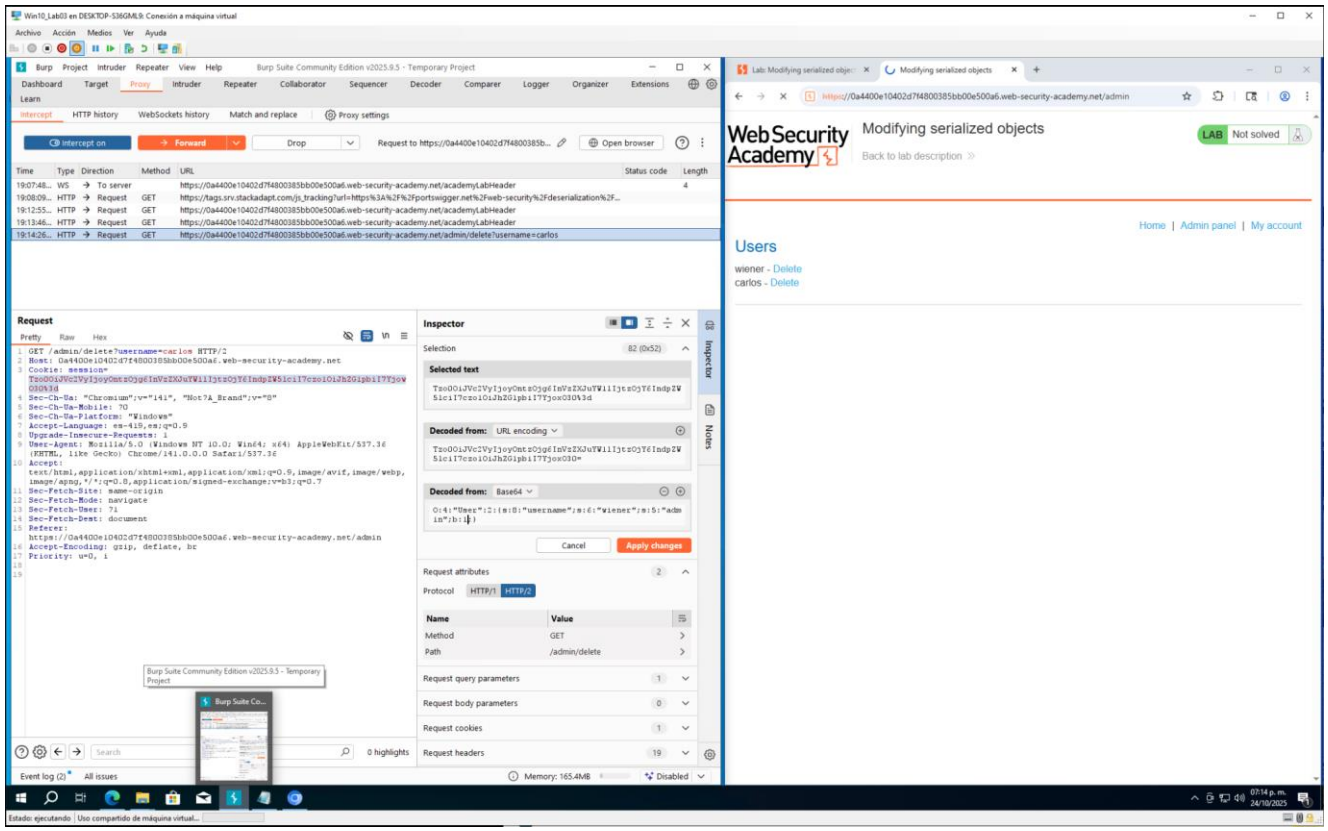
En este punto se elevan los permisos con la cookie para habilitar la opción de Admin panel como se muestra en la imagen siguiente pero sin antes no elevar los privilegios y presionar el botón de forward, así como también se requieren la elevación de los permisos para el ingreso a la opción de admin como se muestra en la segunda image.





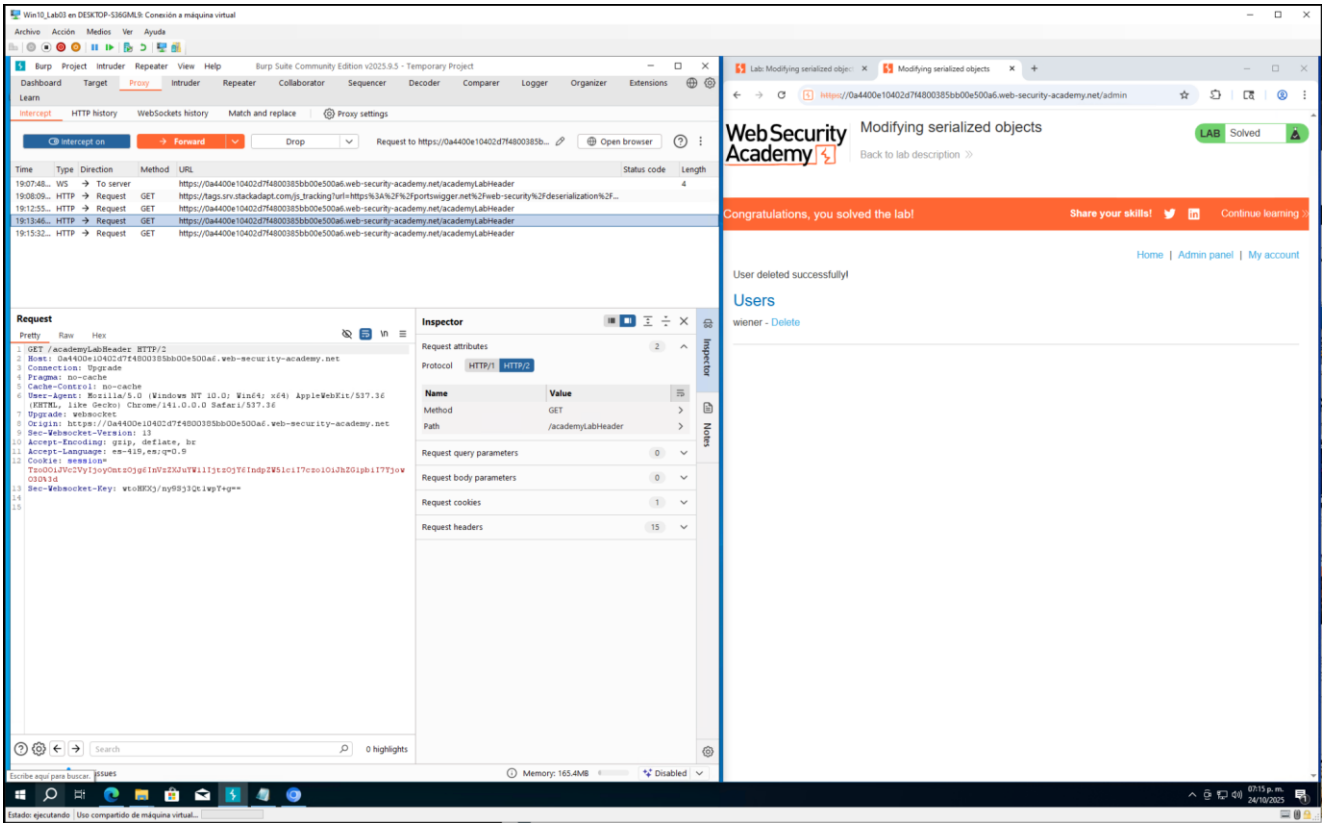
Con los privilegios elevados anteriores en conjunto con el trabajo de la cookie ingresamos al panel de administrador donde se muestran dos cuentas wiener y carlos como se muestra en la imagen siguiente. Después seguimos presionando el botón delete de Carlos y buscamos la cookie para la elevación de privilegios al caviar el número de ID de 0 a 1 aplicamos el cambio y presionamos el botón de forward para su ejecución.





Aquí en la siguiente pantalla nos muestra que el usuario Carlos fue eliminado y el laboratorio fue resuelto al solo mostrarse el usuario wiener como única cuenta en el panel de administrador y así se

culmina con esta actividad.



Conclusion.

En conclusión: La actividad práctica de explotar la Deserialización Insegura ofrece una conclusión fundamental para el campo laboral de la ciberseguridad y la vida cotidiana. Demostrar la escalada de privilegios mediante la manipulación de la cookie de sesión subraya la importancia de una codificación segura. En el campo laboral, este ejercicio evidencia que la confianza implícita en datos serializados provenientes del cliente es una falla crítica. Un pentester o desarrollador debe aplicar validaciones estrictas y usar formatos seguros (como JSON en lugar de serialización nativa) para prevenir el acceso no autorizado y potenciales backdoors. El éxito en la eliminación de la cuenta de "Carlos" justifica la necesidad de auditorías de código regulares.

En la vida cotidiana, esto resalta la fragilidad de la seguridad digital. Como usuarios, aunque no modifiquemos cookies, la existencia de tales vulnerabilidades significa que cualquier aplicación que usemos (bancos, redes sociales) puede ser comprometida, exponiendo datos personales. La lección es

clara: la seguridad comienza con la prevención y el diseño seguro desde la fase inicial del desarrollo.

Referencias.

Gemini - chat to supercharge your ideas. (n.d.). Gemini. Retrieved October 25, 2025, from https://gemini.google.com/

Lab: Modifying serialized objects. (n.d.). Portswigger.net. Retrieved October 25, 2025, from https://portswigger.net/web-security/deserialization/exploiting/lab-deserialization-modifying-serialized-objects

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=*

CyberWorldSec [@CyberWorldSec]. (n.d.). *Lab: Modifying serialized objects | Portswigger | burpsuite* [Video]. Youtube. Retrieved October 25, 2025, from https://www.youtube.com/watch?v=HXMhzXXPJrs