Actividad [#2] – [Deserialización Insegura]

[Auditoria Informática]

Ingeniería en Desarrollo de Software

Tutor: Jessica Hernández Romero

Alumno: Ricardo Rivas Rocha

Fecha: 18-junio-2025

Índice

Introducción

En este segundo escenario de lo que son las vulnerabilidades en sitios web ocuparemos una herramienta que nos ayudara al proceso de desencriptado de credenciales en donde escucharemos los puertos abiertos a través de HTTP con las Cookies de la página web en este caso esta misma cuenta con un laboratorio para poder realizar pruebas de ciberseguridad de manera ética esta misma herramienta me ayudara en esta actividad para cumplir con el objetivo, lo que necesitaremos es de igual manera antes de hacer esta práctica es tener un usuario y una contraseña para facilitar el proceso de realización de esta actividad ya que hoy en día los ataques a sitios web es muy común ya que tanto avanza la tecnología así como de igual manera las vulnerabilidades ya sabiendo este tipo de vulnerabilidades como futuros profesionistas podremos hacer aplicaciones web más seguras y a la vanguardia ante cualquier ciberataque que como lo comento ya es más común en estos tiempos es por ello que debemos estar preparados para todo tipo de ataques que hay en empresas o negocios lideres mundialmente para eso un buen experto en ciberseguridad es lo que buscan hoy en día y es por ello que debemos de alimentarnos de conocimiento y observar el top de vulnerabilidades que hay en el mundo haciendo pruebas de seguridad de igual manera dentro de empresas o negocios así para validad la calidad del sitio.

Descripción

En esta segunda actividad lo que realizaremos es un ataque de deserialización que consiste en tener los privilegios de un administrador web por medio de una vulnerabilidad que en este caso va ser las cookies de la página web que serían las que vamos a explotar con un software llamado Burp Suite con ayuda de la página web de igual manera que viene en nuestro archivo vamos a copiarla para poder hacer esta actividad, primero que nada me registrare en portswigger en donde creare mi usuario y contraseña y accederé de igual manera a la página de laboratorio como lo mencione anteriormente y copiare el enlace de esta página de laboratorio y con la otra aplicación de Burp Suite realizare el ataque de deserialización, en este objetivo de esta actividad es obtener el perfil de Administrador y eliminar al Usuario llamado Carlos para ello en nuestro material viene un video que nos indica como realizar esta actividad para que esta sea un éxito, entenderemos de igual manera como es que funciona esta vulnerabilidad en la vida real de alguna empresa o pequeño negocio ya que la seguridad de la información es vital en estos tiempos entonces estas serían mis herramientas que ocupare y el contexto para realizar esta actividad que de igual manera es interesante que Wireshark ya que son similares pero trabajan diferente en este caso vamos a tomar la vulnerabilidad a través de la cookies de la página proporcionada dentro del laboratorio.

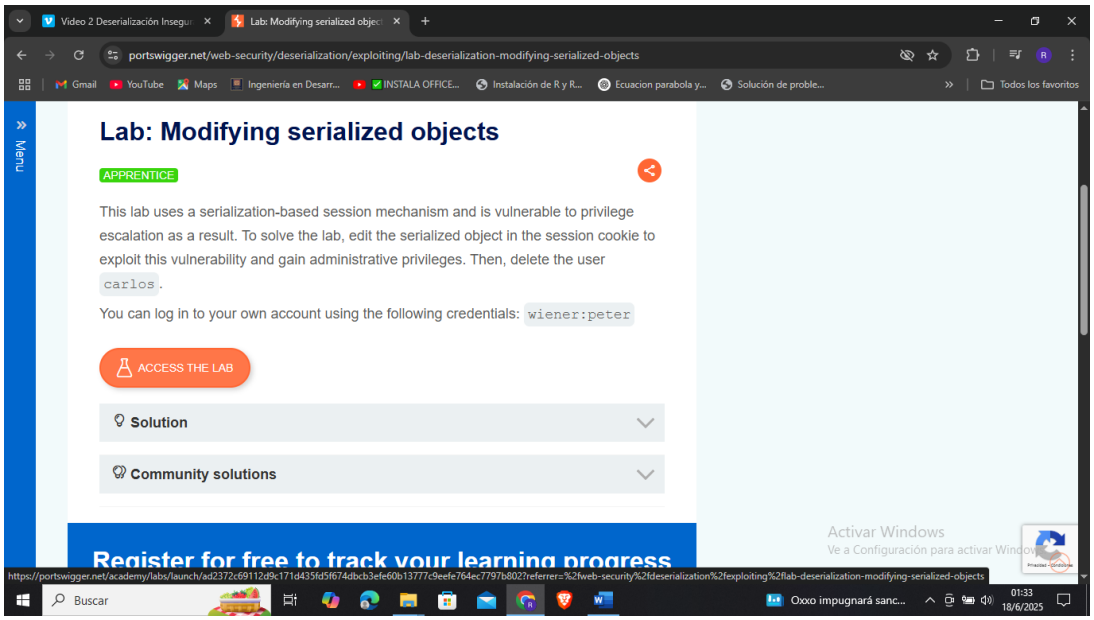
Justificación

Estas acciones nos pueden ayudar a futuro a identificar diversas vulnerabilidades que existen en un ambiente web, porque en la actualidad hay muchas vulnerabilidades aunque tu empresa este totalmente protegida hay nuevas tecnologías tanto para hackers como para empresas como la evaluación de su seguridad en la información por ello es importante se realicen las auditorias de manera en que se detecten diferentes anomalías dentro de la empresa o negocio y así identificarlas, también se pudiera contratar un servicio de inteligencia artificial que ayude a detectar posibles ataques a las redes o sitios de la empresa ya que está en una etapa de conocimiento y esto nutre este mismo pero también no hay que olvidar los bandos que esta pudiera llevar es por ello que con apoyo de esta misma y expertos en ciberseguridad puedan trabajar en conjunto y mitigar amenazas actualmente aunado a ello se tiene que desarrollar los requerimientos de la empresa a través de código ya que de igual manera ayudaría a la empresa en futuros ataques de Hackers y prepararse para algo así como tomando cursos nutriéndose en diferentes formas en las que pudieran atacar en este caso por mi experiencia observe el caso de Coppel y fue una perdida tanto de dinero y tiempo para esta misma porque no se recuperó rápido debido a las grandes bases de datos que esta empresa tiene y yo me imagino que no tenían un protocolo para este tipo de situaciones.

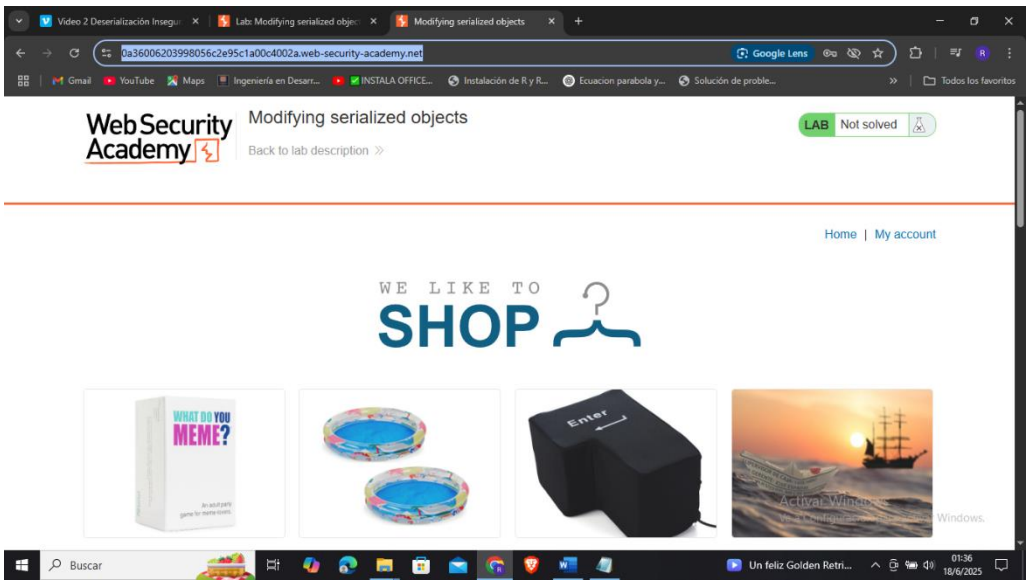
Desarrollo:

- **Ataque Sitio**

En este caso vamos a entrar a la página principal de PortSwigger en donde accederemos al laboratorio de la página web.



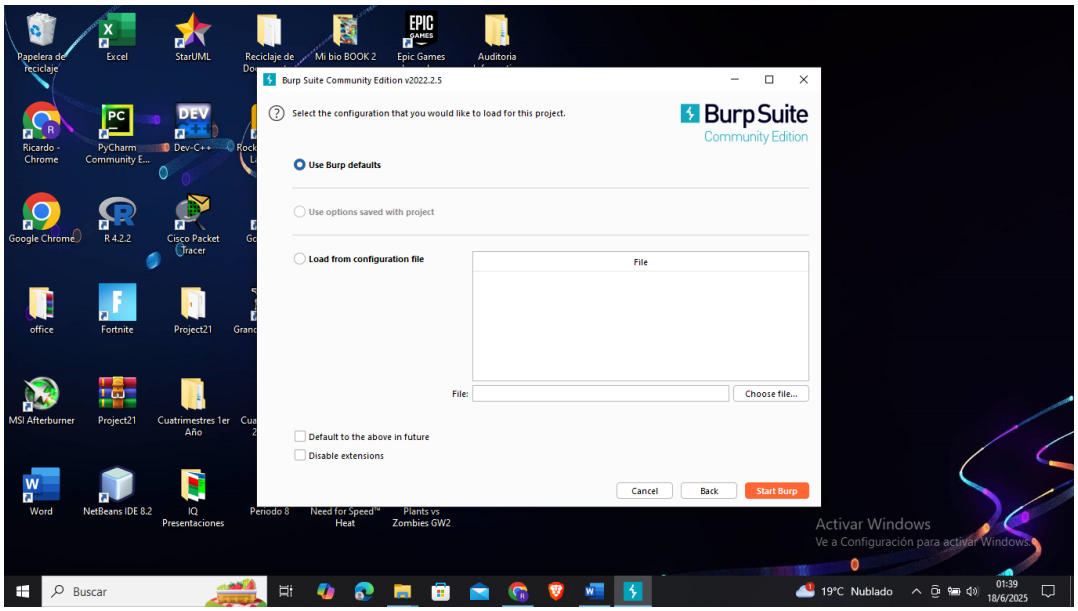
Iniciamos sesión con la cuenta que creamos anteriormente en esta página web para que nos de acceso al laboratorio y copiamos el link de este mismo.



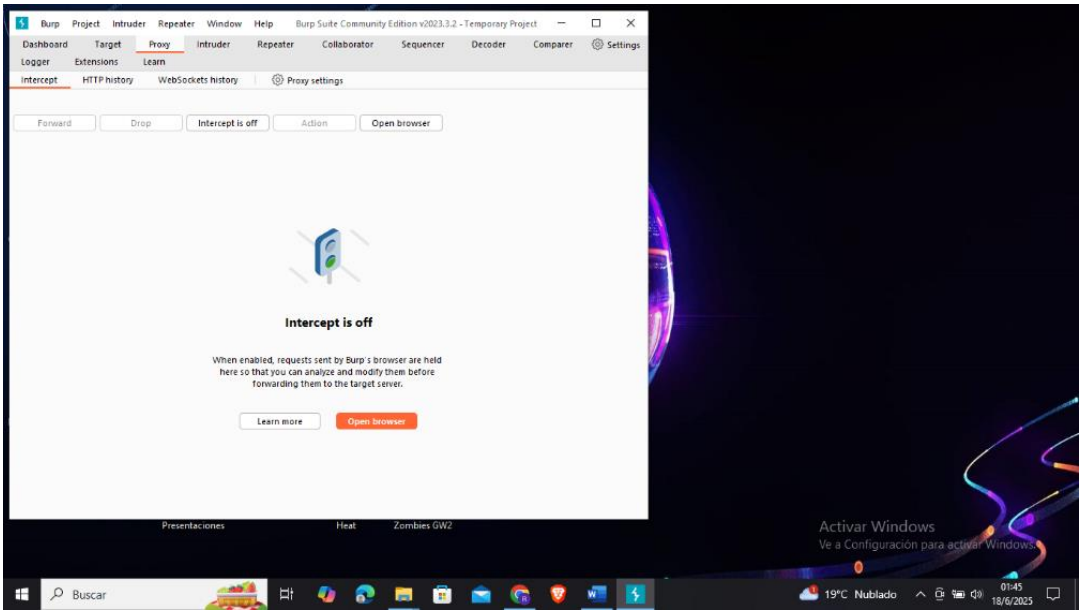
Desarrollo:

- ## Ataque Sitio

Aquí creamos un proyecto temporal en la aplicación de Burp Suite Comunity.



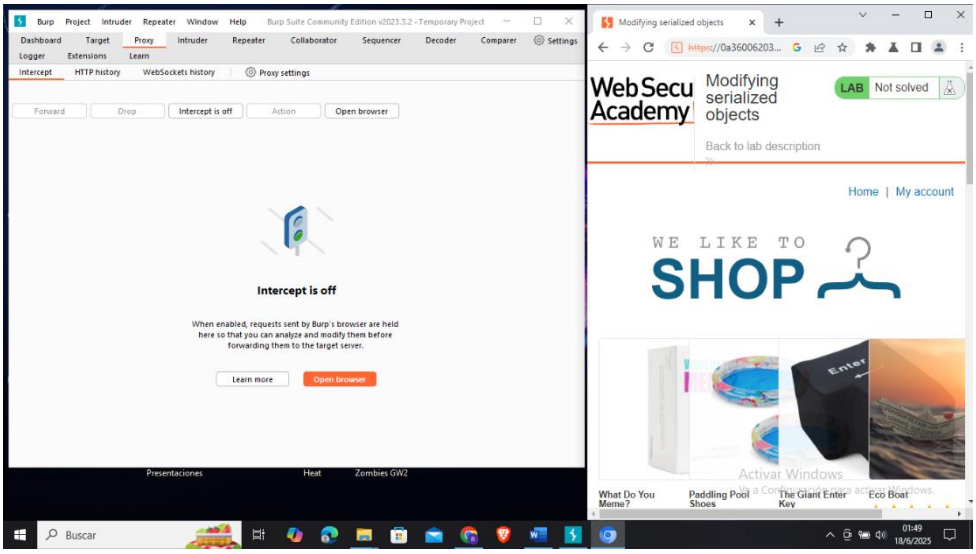
Y nos vamos a la opción de proxy y damos en Open Browser.



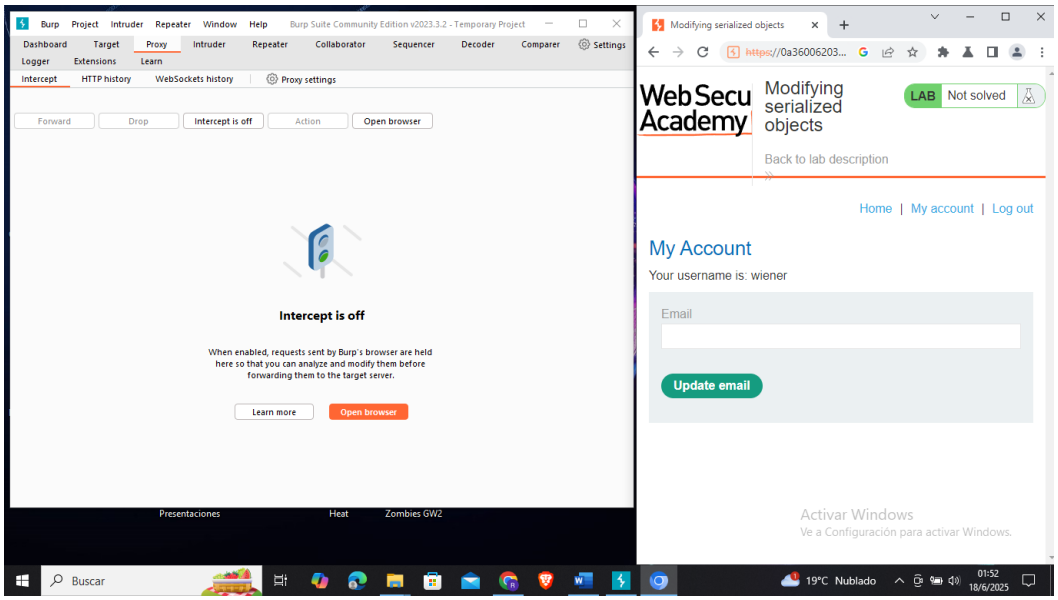
Desarrollo:

- **Ataque Sitio**

Y Pegamos la URL del modo laboratorio que nos dio la pagina en internet normal al navegador de Burp Suite Comunity se nos abrirá la página como podemos observar.



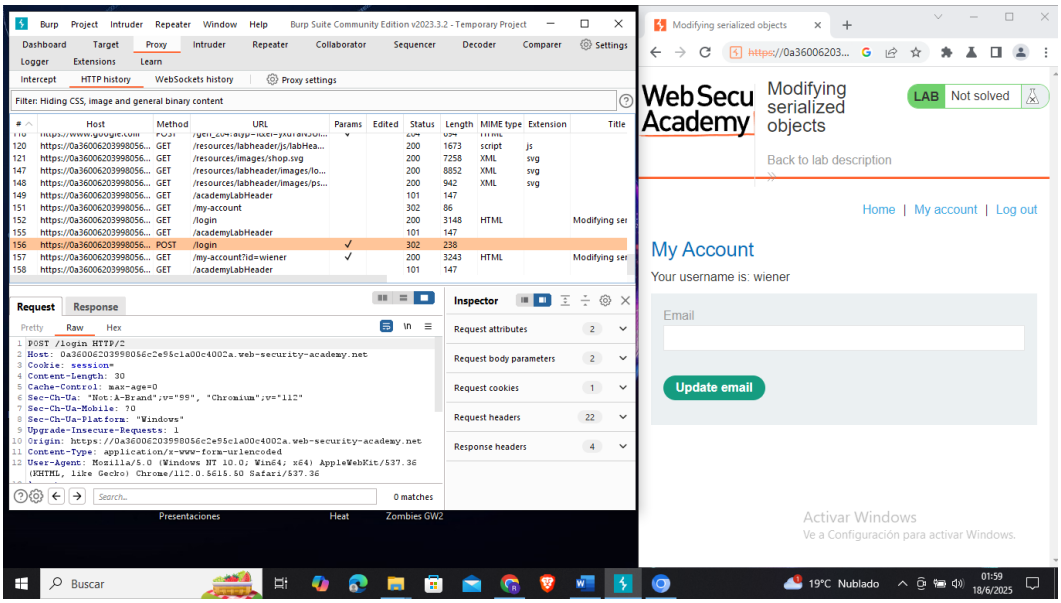
Ahora vamos a iniciar el Usuario de Wiener y Peter desde la sección My Account.



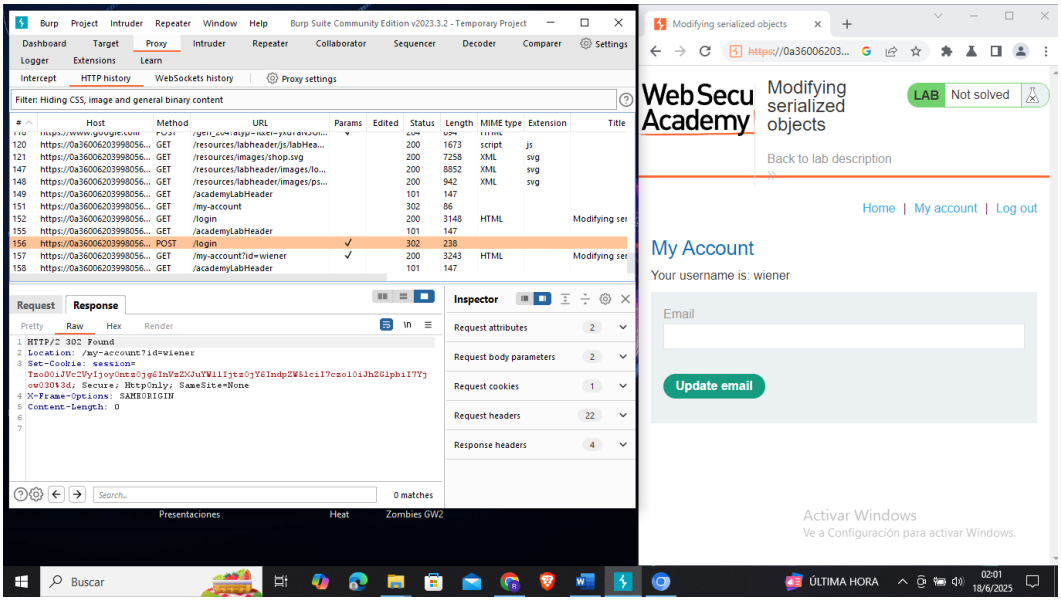
Desarrollo:

- **Ataque Sitio**

Nos vamos a la Opción HTTP history en donde vamos a buscar el método post y /login.



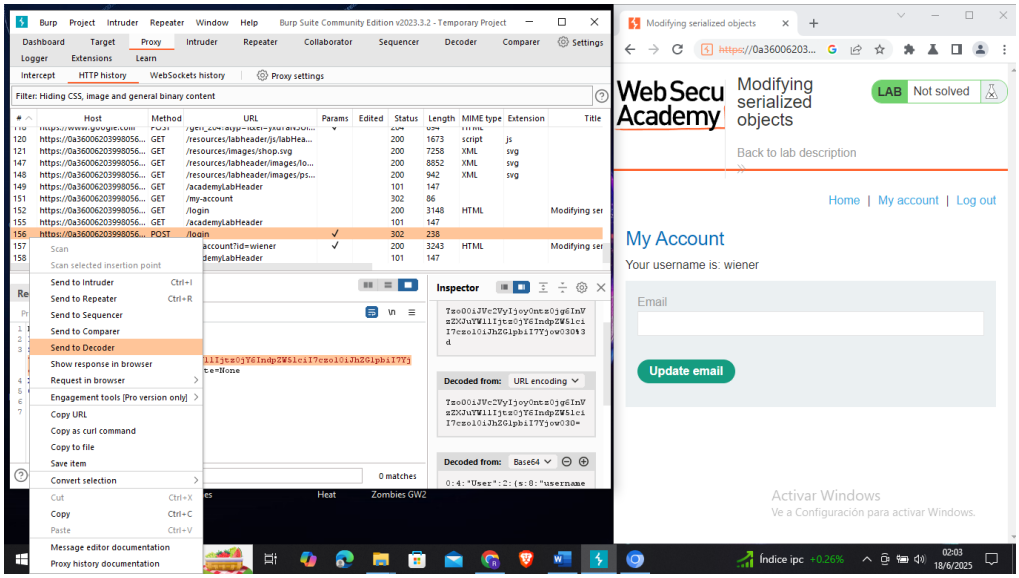
Después de buscarla nos vamos a la pestañita response y en Raw nos aparecerá la cookie sesión.



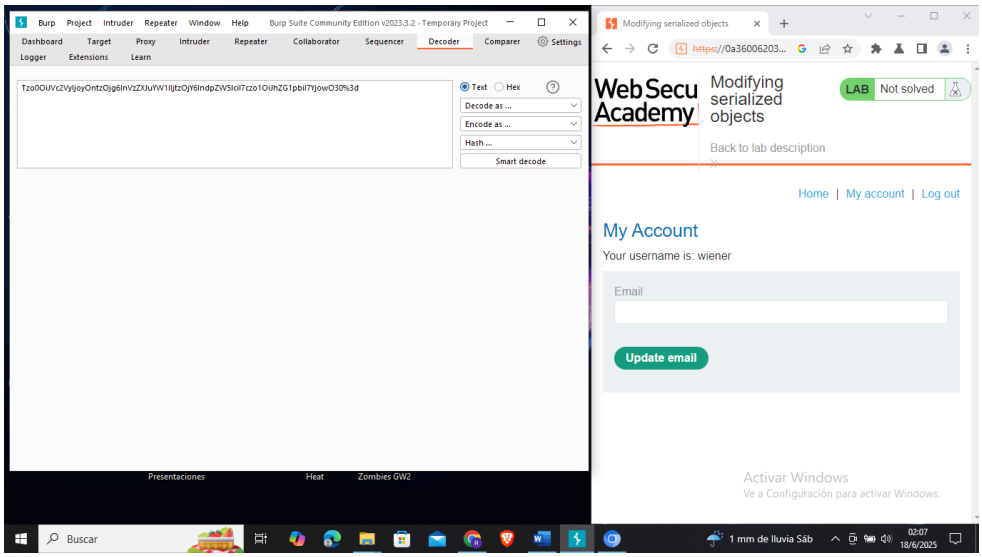
Desarrollo:

- **Ataque Sitio**

Luego seleccionamos la cookie sesión y la mandamos a send decoder.



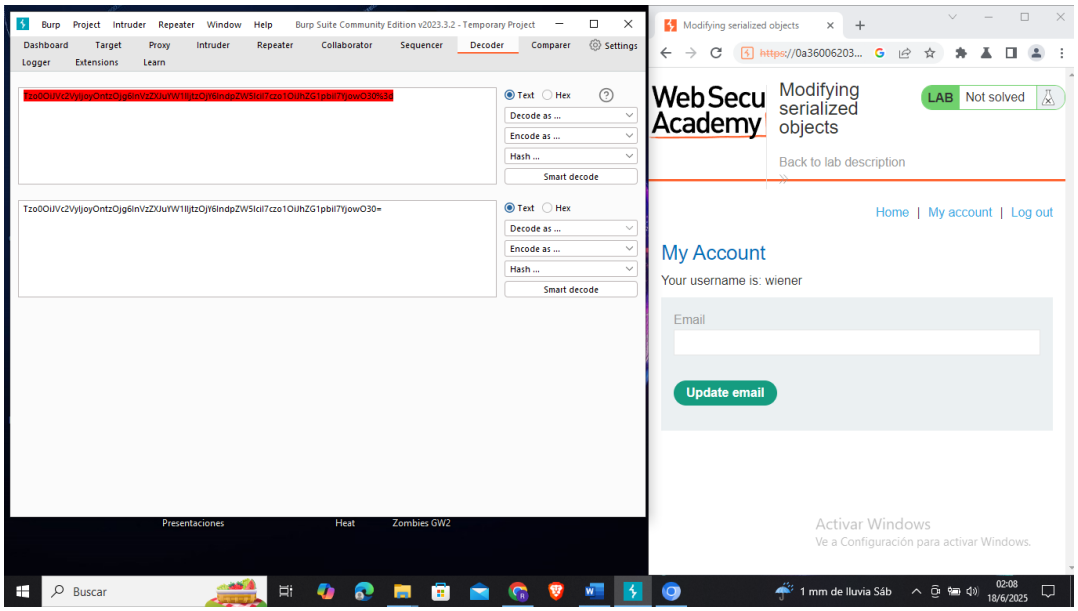
Aquí nos dirigimos en este caso a la opción decoder ya que no me envió automáticamente a la pantallita checando la cookie sesión.

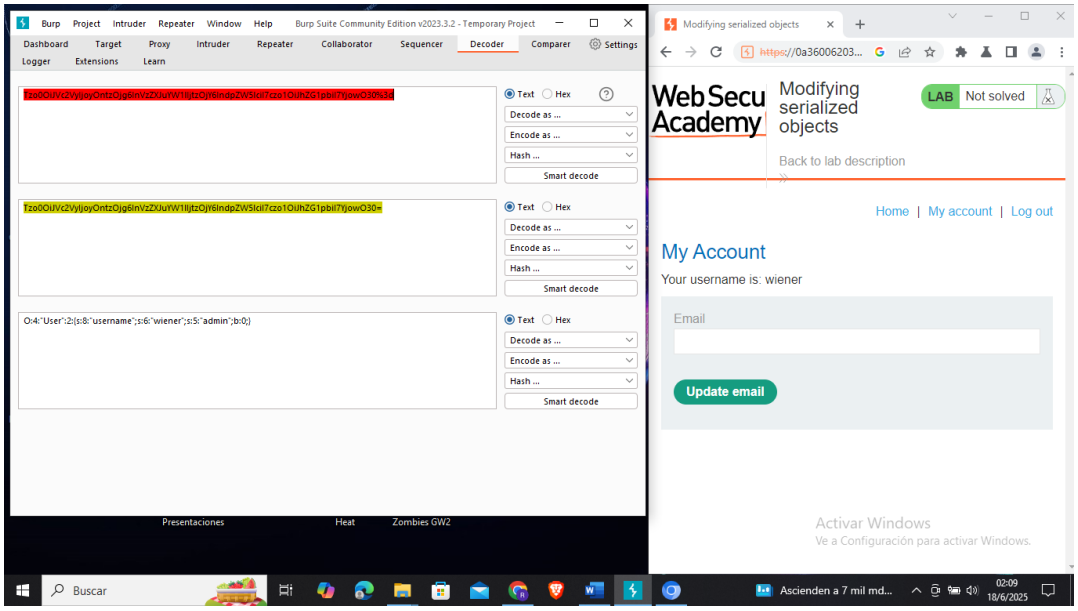


Desarrollo:

- **Ataque Sitio**

La decodificamos a URL para después decodificar a Base64.

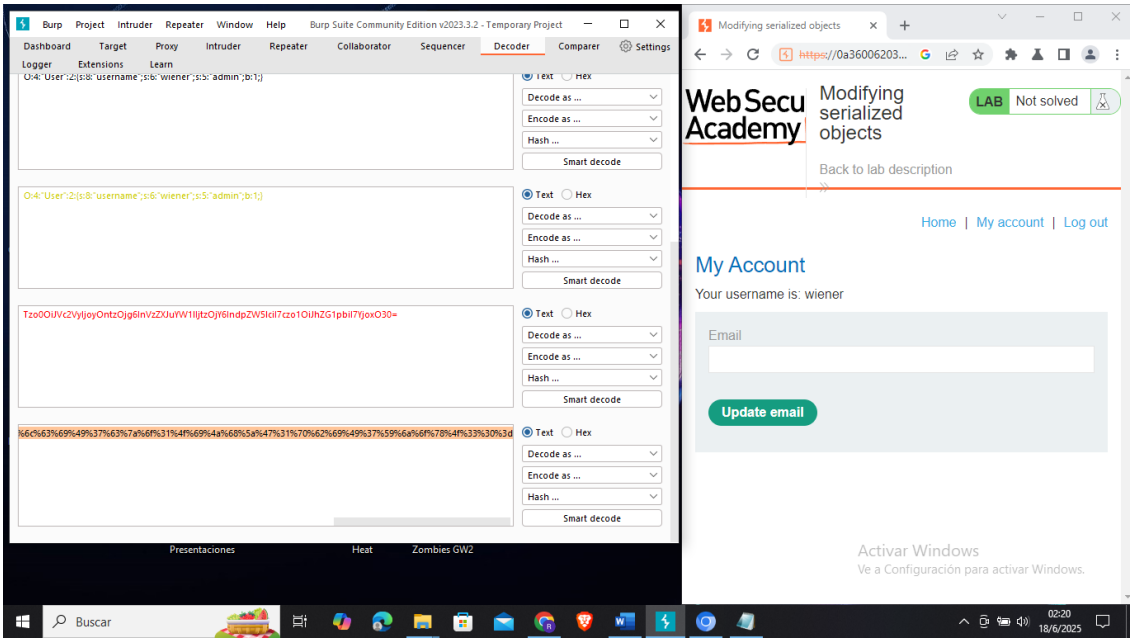




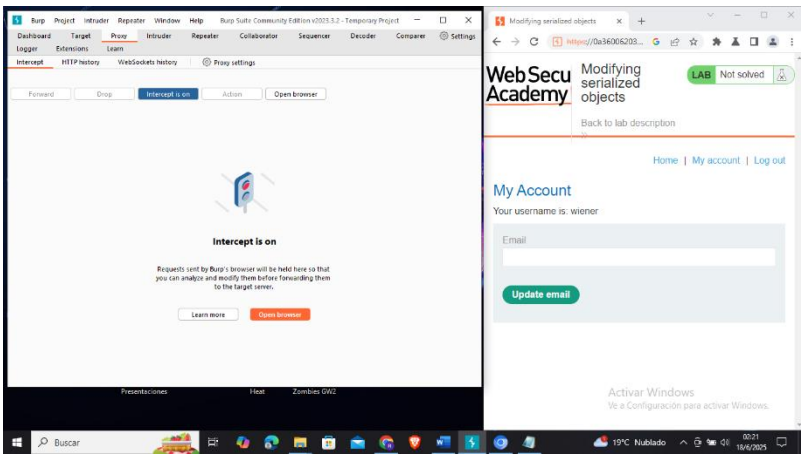
Desarrollo:

- **Ataque Sitio**

Lo mas interesante es cambiarle el 0 a 1 y Ahora al decodificamos a base 64 y por último a URL con este cambio podremos tener acceso con esta cookie para administrar la página.



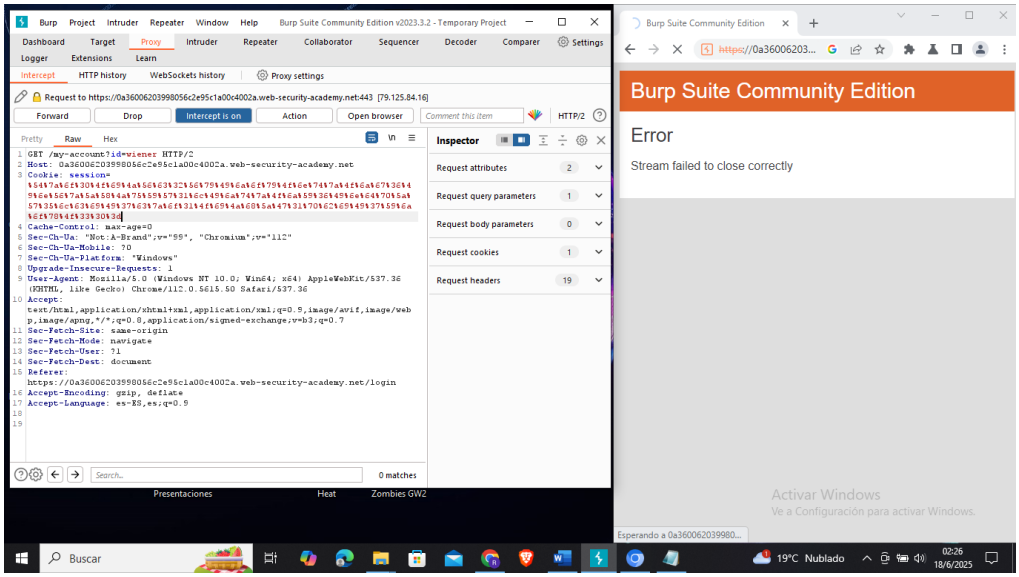
Vamos a Proxy nuevamente y encendemos el interceptor.



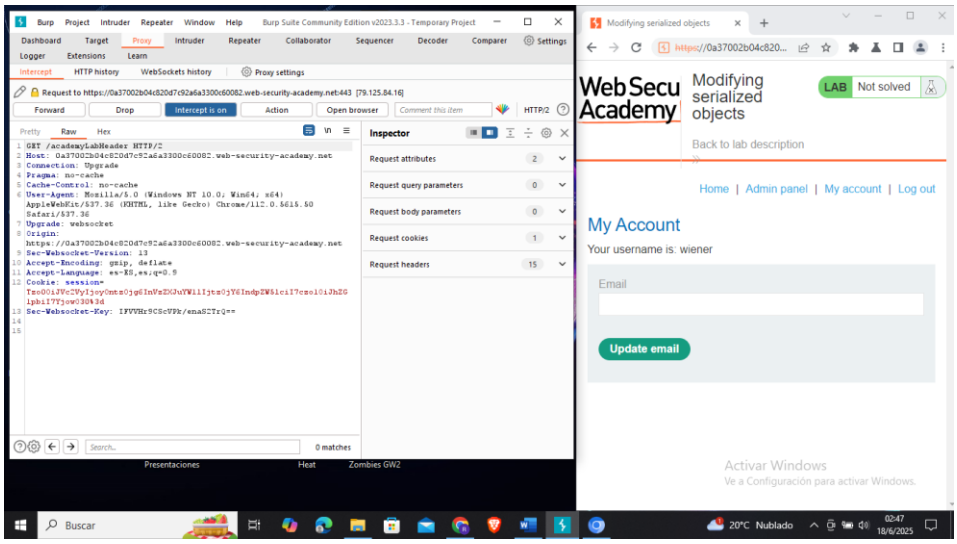
Desarrollo:

- **Ataque Sitio**

Y Refrescamos el sitio en donde realizamos la penetración y cambiamos la información de la cookie por la que se nos generó en el programa de decoder.



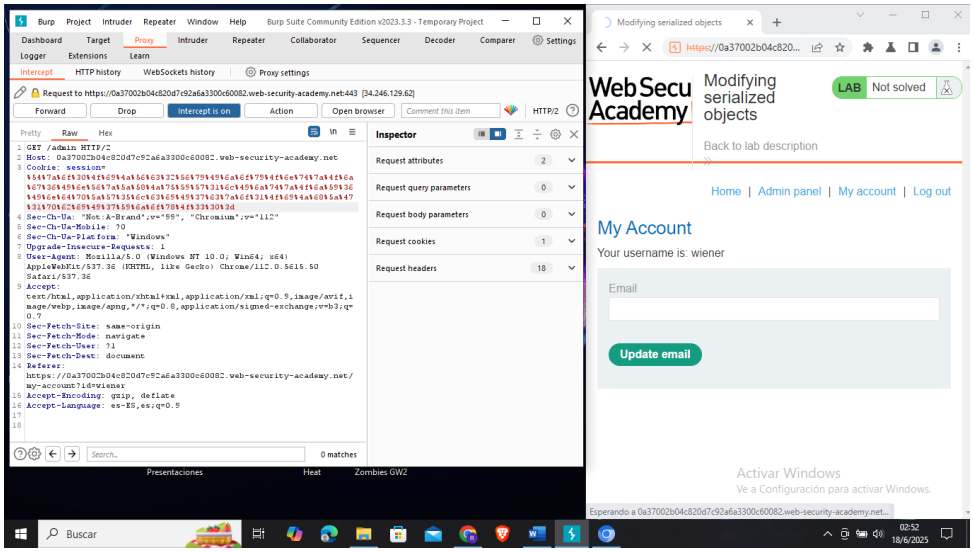
Tuve un errorcillo, pero ya me aparece admin Panel volví a hacer todo el proceso desde el inicio.



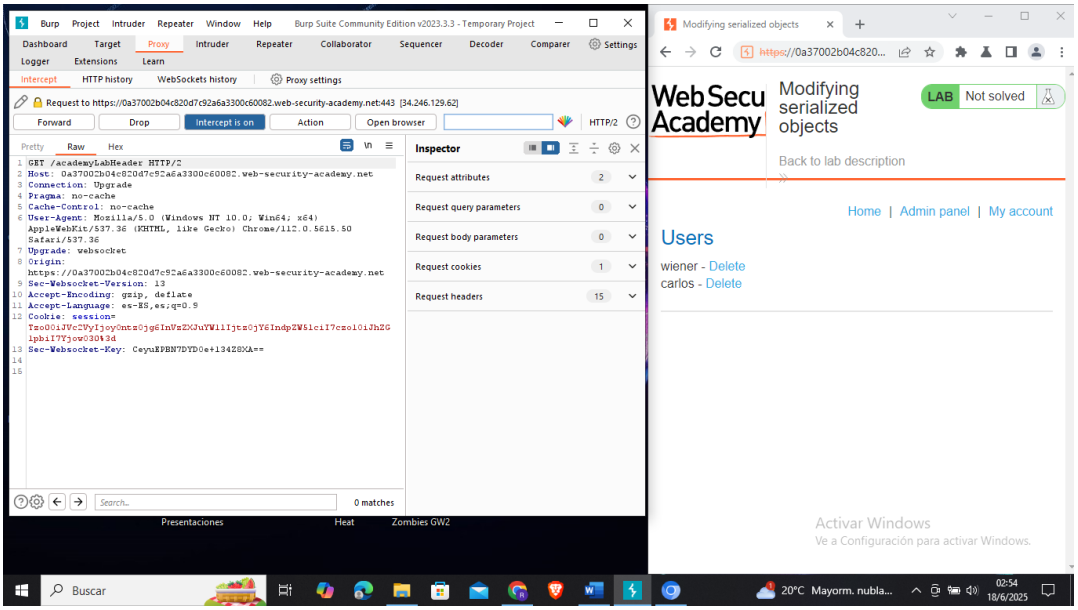
Desarrollo:

- **Ataque Sitio**

Damos clic en Admin panel y se nos abrirá los usuarios registrados en esta ocasión se me paso una captura, pero una antes de esta le cambiamos la cookie por la que desarrollamos en decoder.



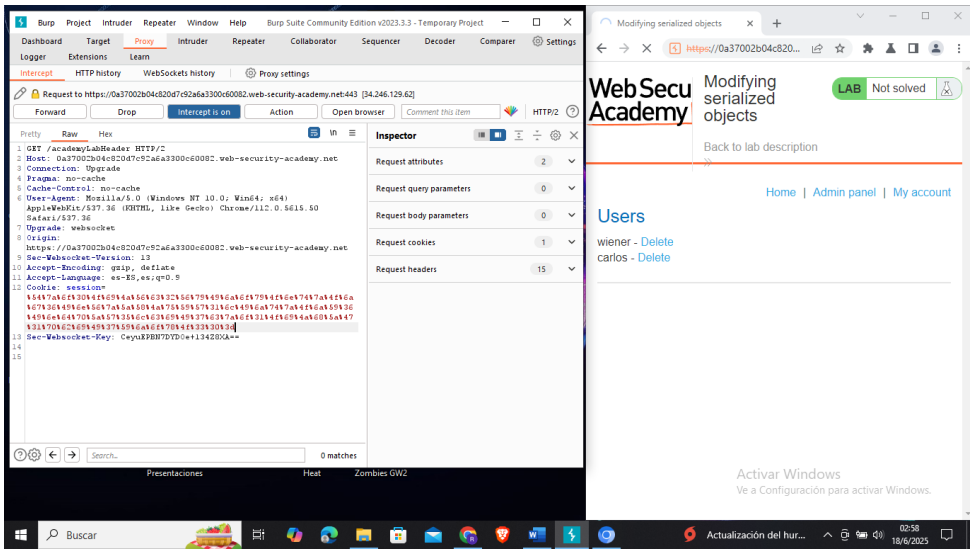
En este caso después de ingresar las cookies que te pide en consola podemos ver la pagina que se actualiza y aparecen los nombres de los Usuarios.



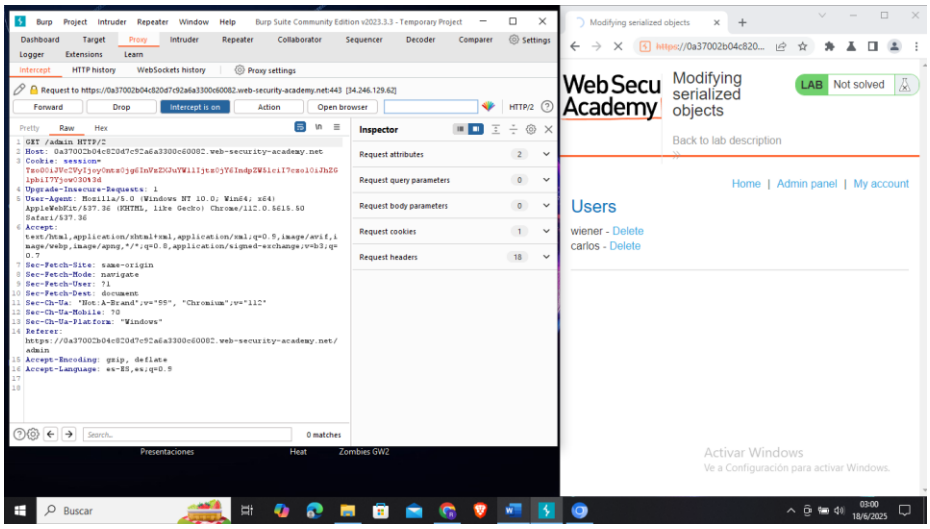
Desarrollo:

- **Ataque Sitio**

Procederemos a eliminar al usuario Carlos le damos clic en delete y en información de la cookie pegamos la ya antes generada en decoder.



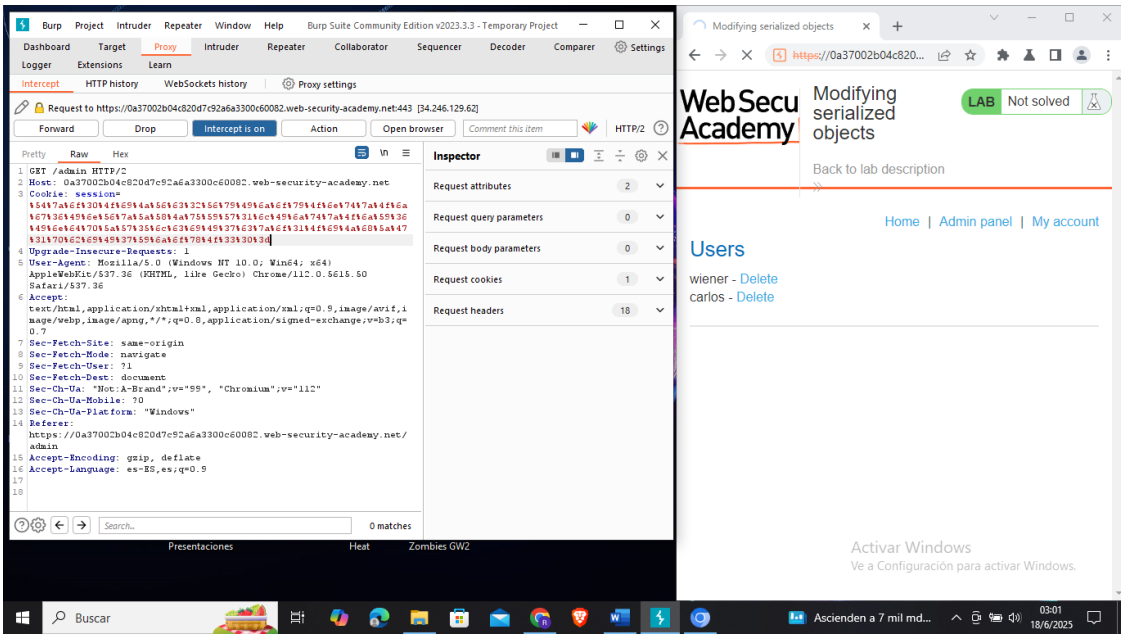
Nos sale otra pagina de consola igual modificamos la cookie igual aquí se me paso una captura y nos salió otra de igual manera modificamos la cookie.



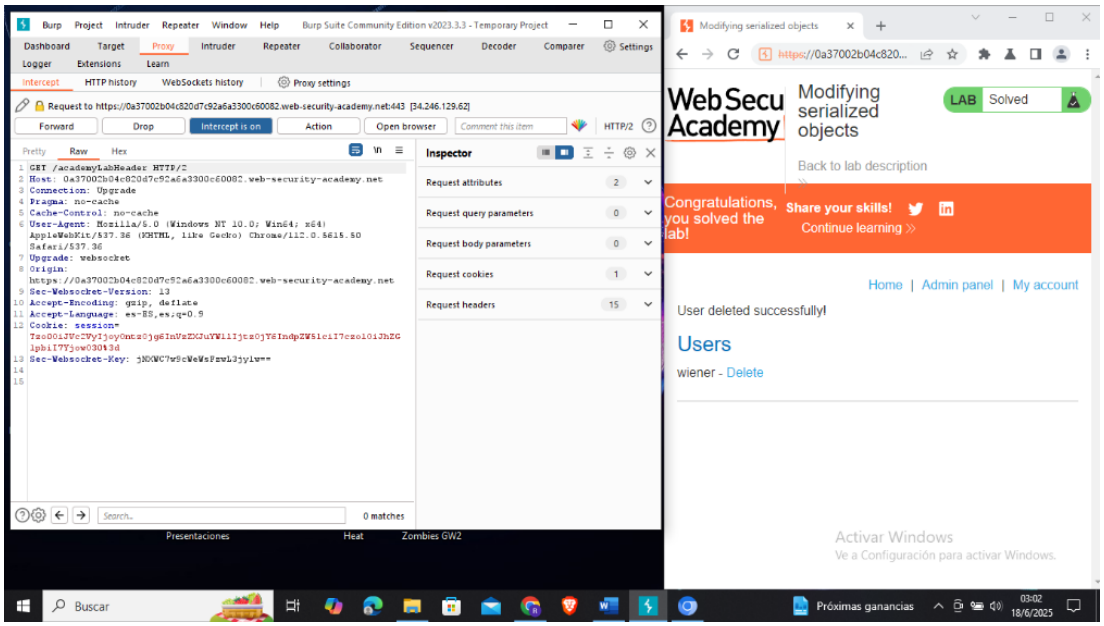
Desarrollo:

- **Ataque Sitio**

Siguiendo la deserialización.



Y finalmente eliminamos al Usuario Carlos Exitosamente **:V** .



Conclusión

Como pudimos observar es muy importante cuidar nuestra información mas que en la actualidad hay muchas cookies para todo esto ya que es un riesgo por que las cookies se trasladan en paquetes de datos http y como ya nos dimos cuenta en la actividad pasada pueden igual robarnos datos como el usuario y la contraseña y en esta segunda practica observamos que tuvimos privilegios como administrador del sitio web por medio de una plataforma de laboratorio esto nos va a servir de aquí en adelante para mantenernos prevenidos al confirmar la cookie o las cookies de la paginas web ya que es muy importante resguardar nuestra información de manera segura ya que en la actualidad tanto los usuarios como grandes empresas enfrentan estos tipos de ataques, con estas actividades comprendemos la importancia de un cifrado seguro y actualizado ya que muchas empresas no quieren pagar por su seguridad hasta que después se lamentan en perdidas tanto económicas y riesgo de su perdida de datos es por ello que tienen que haber respaldos cada cierto tiempo de la información ya que los hackers lo que buscan es afectar a estas mismas ya que les conviene extorsionar para sacarle valor monetario a la empresa o vender la información al mejor postor en este caso se publico la vulnerabilidad en una pagina mexicana la andaban vendiendo al mejor postor en este caso era la información de la empresa en donde trabaje Coppel esto sucedió como lo comente por no llevar un seguimiento a sus protocolos de seguridad es por ello que se necesita reforzar aún más estos mismos.

Link GitHub: https://github.com/Ricardorivas94cr/Auditoria-Inform-tica-UMI

Referencias

Lab: Modifying serialized objects | Web Security Academy. (s. f.). https://portswigger.net/web-security/deserialization/exploiting/lab-deserialization-modifying-serialized-objects

AlanDavidLR. (s. f.). *GitHub - AlanDavidLR/AuditoriaInformatica*. GitHub. https://github.com/AlanDavidLR/AuditoriaInformatica

Video 2 Deserialización Insegura.mp4. (s. f.). Vimeo. https://vimeo.com/711846733/1d604d66b2