Universidad Corporativa Coppel | Programas Académicos

Ingeniería en Desarrollo de Software

Ingeniería en Desarrollo de Software

Actividad: Número 1.

Nombre de la Actividad: Pérdida de autenticación y gestión de sesiones.

Nombre del Curso: Auditoria informática.

Tutor: Jessica Hernández Romero.

Alumno: Omar Juárez Carmona.

Fecha: 26 – Septiembre – 2023.

INDICE

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.

En esta primera etapa, realizar una prueba de la vulnerabilidad de la pérdida de autenticación y gestión de sesiones utilizando el programa WireShark. El objetivo de esta prueba es sacar las credenciales que se ingresaron y estas se puedan mostrar.

Actividad:

Seleccionar un proyecto web realizado anteriormente que cuente con las siguientes características:

- Función de iniciar sesión y de registro de usuarios.
- Conexión con una base de datos.

Subir el proyecto a un servidor web con la base de datos incluida. Una vez que el proyecto esté en Internet, realizar la instalación de WireShark. Este programa permite realizar el ataque. Una vez hecho esto, proceder a realizar el ataque al sitio web aprovechando la vulnerabilidad de falta de SSL o seguridad.

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

En esta primera actividad que estamos empezando referente a la materia de Auditoria informática, estaremos tratando temas relacionados a la vulnerabilidad de los sitios web no seguros.

Como mencionaba en líneas anteriores, la auditoria 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 Wireshark.

En esta primera actividad, se busca identificar posibles vulnerabilidades y riesgos que puedan comprometer la integridad y confidencialidad de la información almacenada en el sistema, así como la privacidad de los usuarios. Además, nos ayuda con el análisis de tráfico de red para inspeccionar las comunicaciones entre el cliente y el servidor. Durante estos procesos es detectar cualquier comportamiento sospechoso o inseguro, ya que en esta auditoria se llevará a cabo en un entorno controlado que simula el funcionamiento real del sistema.

Espero adquirir todos los conocimientos sobre cómo identificar y evaluar las amenazas a la seguridad en los procesos de autenticación y registro de usuario en un sistema, esto incluye como comprender y evaluar la seguridad en los sistemas de autenticación y registros de usuarios, para proteger la integridad de la información y la privacidad de los usuarios en línea.

Aprenderemos a utilizar esta herramienta de trabajo llamada Wireshark en un sitio web no seguro, para así poder visualizar el nombre de usuario y la contraseña con la cual simularemos entrar a la página web y poder robarnos esa información en este sitio vulnerable. Sin más preámbulo, vamos a continuar con nuestra primera actividad y realizar las pruebas necesarias para conocer cómo funciona el hacker de información de un determinado usuario.

JUSTIFICACION

Ahora mismo haremos el análisis del por qué recomendar esta herramienta de trabajo de Wireshark y hacer el uso correcto de este analizador de Auditoria informática para los usuarios, empresas, pero sin antes comencemos por saber que es esta herramienta de trabajo de Wireshark.

Wireshark es una herramienta de análisis de red que permite capturar y examinar el tráfico de red en tiempo real. Algunos de los aspectos importantes de Wireshark son:

Licencia GPL:

Wireshark es un software de código abierto y se distribuye bajo la licencia GPL.

Robustez:

Es muy robusto tanto en modo promiscuo como en modo no promiscuo.

Captura de datos:

Puede capturar datos de la red o leer datos almacenados en un archivo.

Basado en librería Pcap:

Wireshark está basado en la librería Pcap, que proporciona una interfaz para capturar paquetes de red.

Interfaz flexible:

Tiene una interfaz muy flexible que permite personalizar su apariencia y disposición.

Gran capacidad de filtrado:

Wireshark tiene una gran capacidad de filtrado, lo que permite analizar y visualizar solo los paquetes relevantes.

Formato estándar de archivos tcpdump:

Admite el formato estándar de archivos tcpdump, lo que facilita el intercambio de capturas con otras herramientas.

Reconstrucción de sesiones TCP:

Wireshark puede reconstruir sesiones TCP y mostrar el flujo completo de datos entre dos hosts.

Wireshark es una herramienta ampliamente utilizada por profesionales de redes y seguridad para diagnosticar problemas, analizar el tráfico de red, detectar anomalías y realizar investigaciones forenses2. Su capacidad para capturar y analizar datos en tiempo real lo convierte en una herramienta valiosa para administradores de redes, ingenieros de seguridad y otros profesionales del campo.

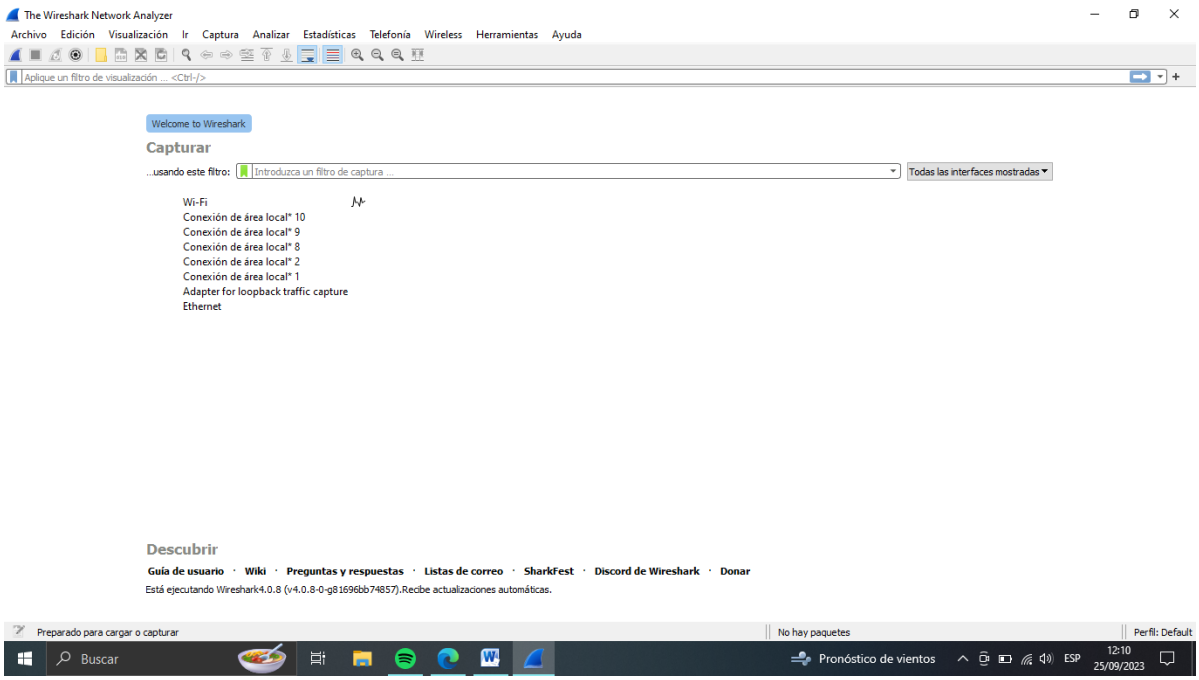
DESCRIPCION DEL SITIO WEB

Sitio web oficial llamado CELFI, donde el principal objetivo se refiere a Ministerio de Ciencia Tecnología Innovación Argentina, donde tiene vulnerabilidad y con una leyenda de modo no seguro del sitio web que es acá en donde haremos nuestra primera prueba utilizando la herramienta de trabajo de Wireshark.

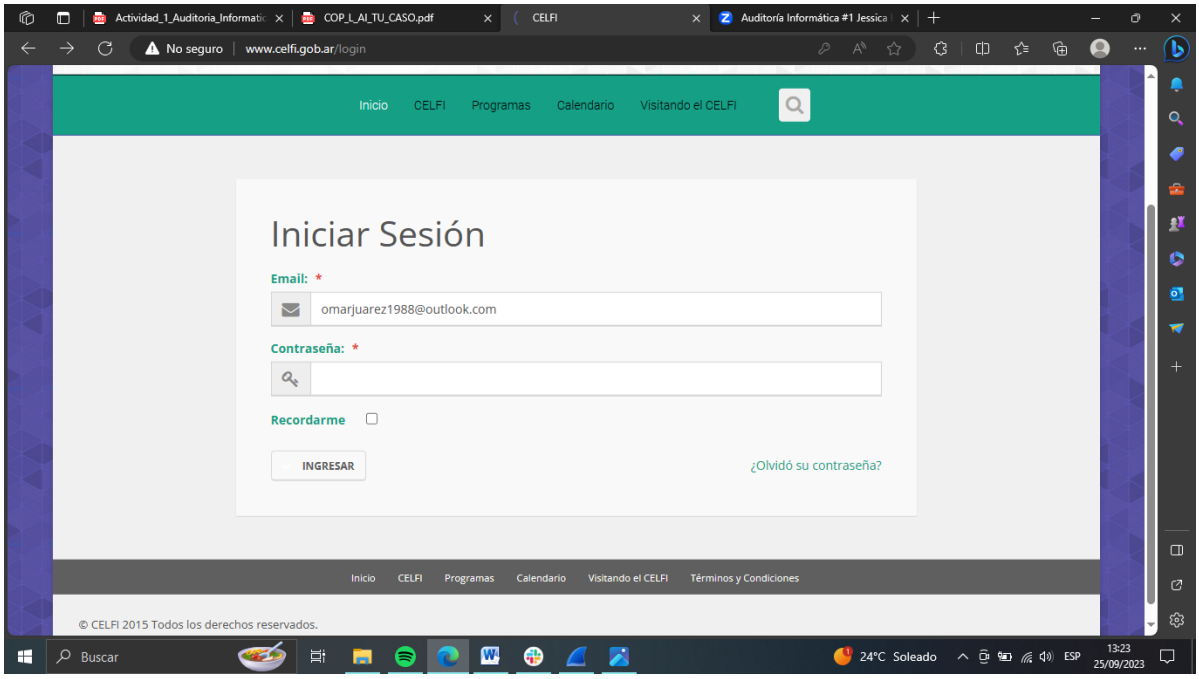
Daremos a detalle cómo se realiza el hacker, ya que el protocolo de transferencia de hipertexto es muy vulnerable, hoy en día las páginas que lo llegan a usar son demasiado vulnerables al ataque y robo de datos, para comprobar que se utilizó un analizador de paquetes llamado Wireshark. Nos introduciremos en una página web de http, para poder observar lo fácil que es extraer los datos del usuario. Cabe recalcar que esto funciona solo si el usuario al cual extraeremos sus datos, debe estar conectado a la misma red que nosotros, es decir que para poder extraer datos del usuario con un analizador de paquetes. Ambos, tanto el como yo debemos de estar conectado a la misma red.

ATAQUE AL SITIO WEB

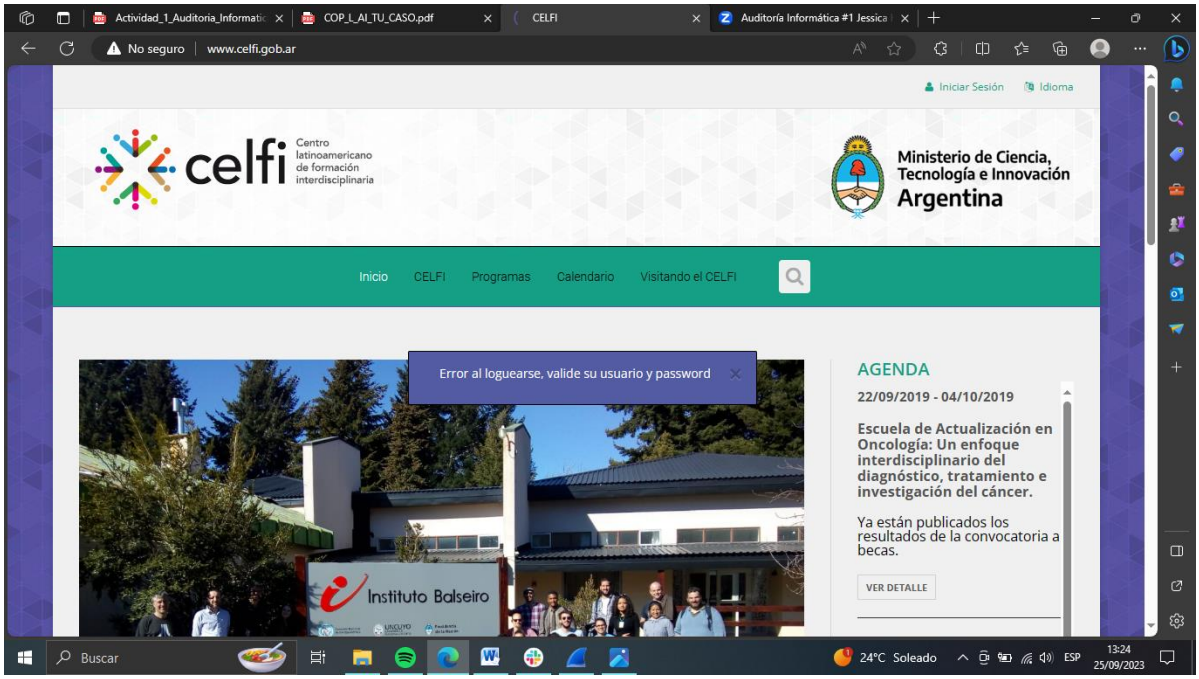
Página principal de herramienta de trabajo Wireshark.



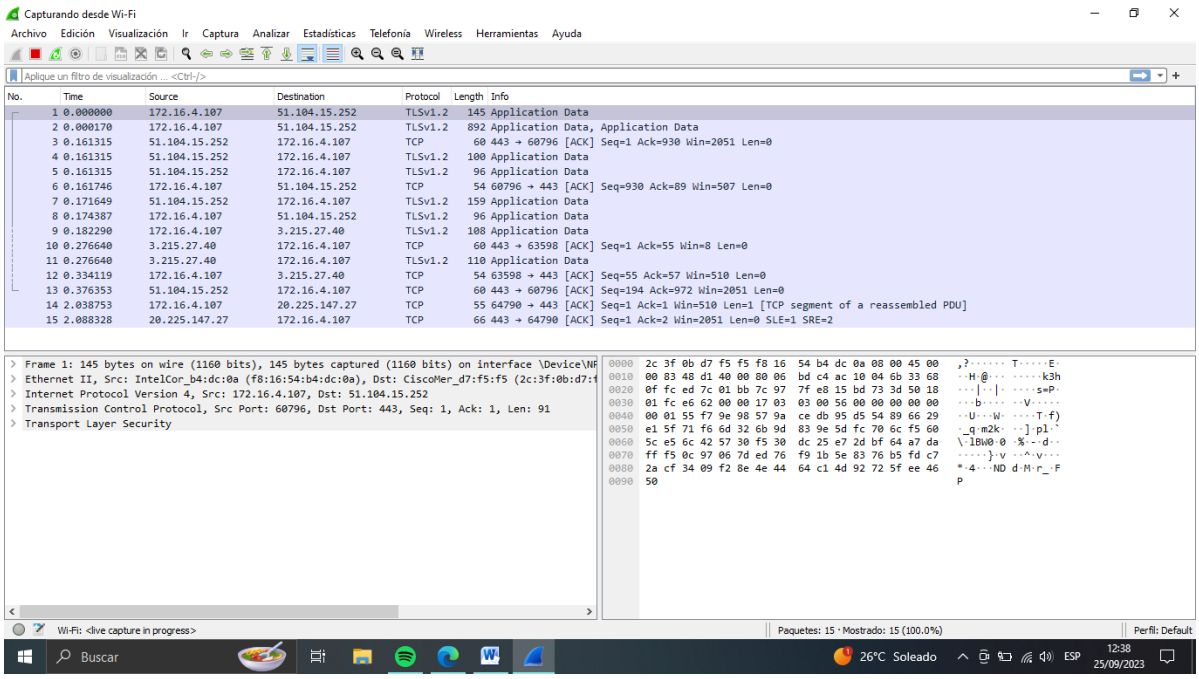
Página celfi no segura para loguearnos.



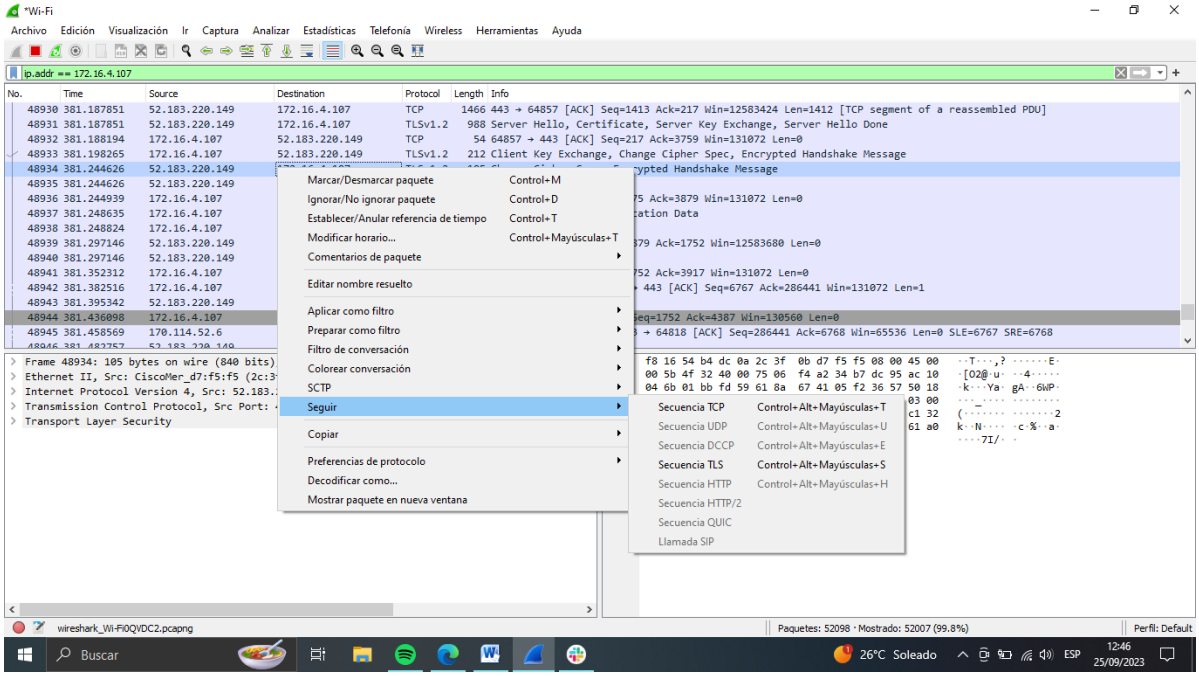
Página celfi logueada con nuestro usuario y contraseña.



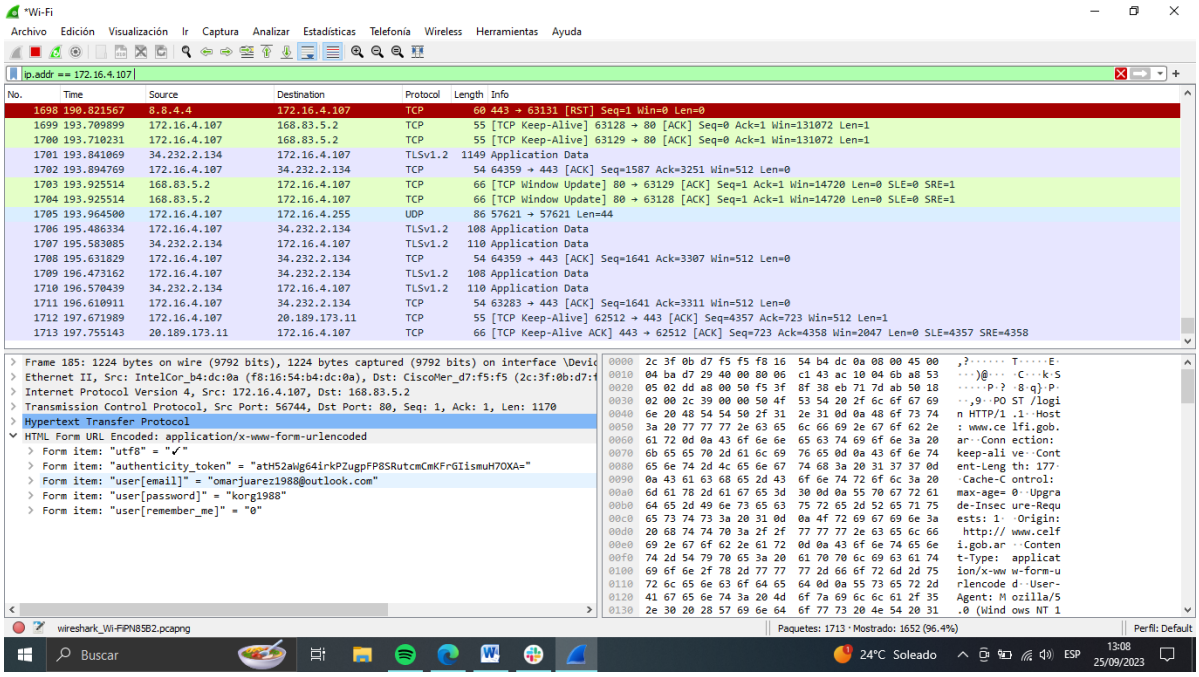
Comenzando a ejecutar nuestra herramienta de trabajo Wireshark modo wi-fi.



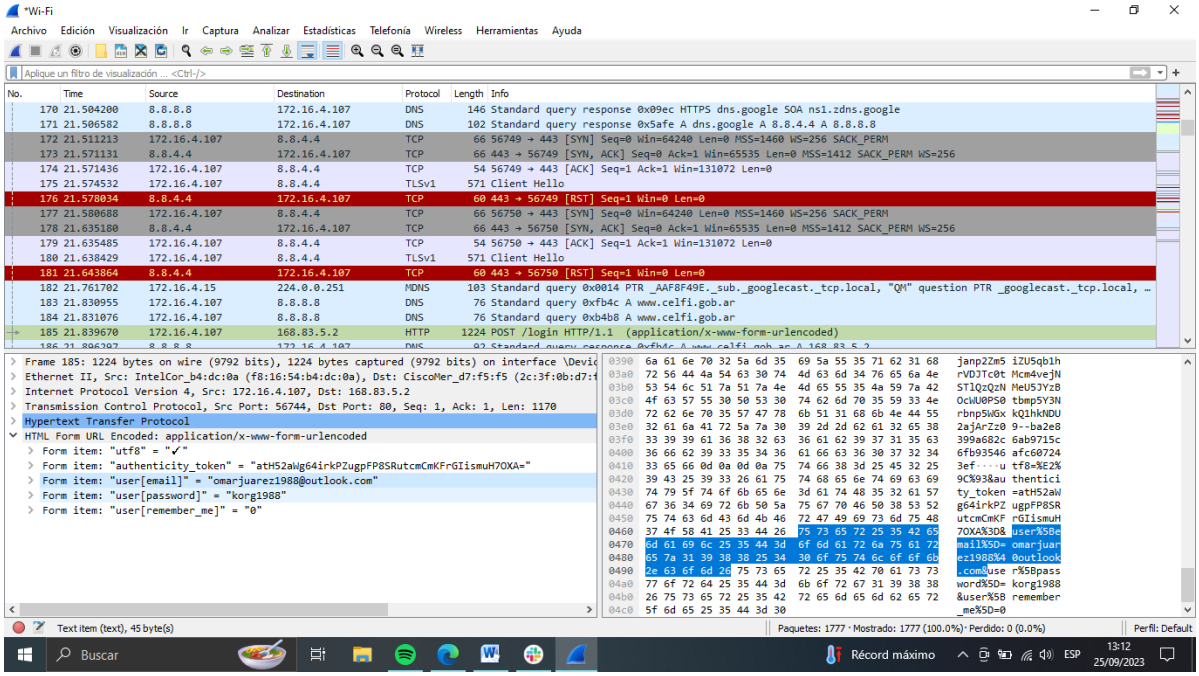
Utilizando comando ip.add == dirección IP para saber usuario y contraseña de usuario.



Resultado obtenido correctamente de usuario y contraseña con Wireshark.



Resultados obtenidos correctamente al saber usuario y contraseña de página web.



CONCLUSION

Casi todas las aplicaciones web mantienen el perfil de los usuarios por separado pata así poder garantizar sus servicios y comunicaciones. No obstante, el problema de la autenticación rota y gestión de sesiones representa dos de los principales impedimentos para confirmar la confidencialidad de la aplicación web en la actualidad. Por lo tanto, hay que implementar medidas que logren mitigarlos.

Por lo anterior, es de gran importancia realizar auditorías de seguridad para así poder verificar la protección de los datos y evitar que cualquier tipo de malware pueda ingresar a nuestro equipo a través de las vulnerabilidades de los sitios web a los que les proporcionamos los datos confidenciales.

Debemos de entender y conocer que existen 2 tipos de vulnerabilidades, estas dos vulnerabilidades establecidas por OWASP en sus top 10, nos pueden ayudar a identificarlas en nuestras aplicaciones o sitios web. A su vez podremos saber que estrategias de seguridad podemos implementar para evitar que nuestro software tenga vulnerabilidades y los datos puedan ser robados con gran facilidad de nuestras máquinas.

En definitiva, para lograrlo, es vital saber cómo realizar auditorías que nos permitan verificar la calidad y seguridad del programa o sitio web en cuestión, así como identificar qué tipo de vulnerabilidad pudiéramos tener.

En esta primera actividad aprendimos a usar la herramienta de trabajo de Wireshark en una página web con login y así poder identificar las vulnerabilidades que tienen los sitios web no seguros (http).

Pudimos intentar acceder a esa página web con un nombre de usuario y una contraseña de un correo x y poder robarnos esa información confidencial con la misma herramienta de trabajo. En sí, hackeamos al usuario sus datos personales.

REFERENCIAS

Wireshark · go deep. (n.d.). Wireshark. Retrieved September 21, 2023, from https://www.wireshark.org/

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/

Altube, R. (2021, January 7). Wireshark: Qué es y ejemplos de uso. *Openwebinars.net*. https://openwebinars.net/blog/wireshark-que-es-y-ejemplos-de-uso/

Molina, L. P. [@LuisPeraltaMolina]. (2021, August 2). *Como descargar e instalar Wireshark*. Youtube. https://www.youtube.com/watch?v=L07PeLPtvPo

CELFI. (n.d.). Gob.Ar. Retrieved September 25, 2023, from http://www.celfi.gob.ar/

LINK DE GITHUB

Omarsitho1988 (github.com)