Universidad Corporativa | Programas Académicos

Ingeniería en Desarrollo de Software

Actividad 1 - Pérdida de autenticación y gestión de sesiones

Auditoria Informática

Ingeniería en Desarrollo de Software

Tutor: Mtra. Jessica Hernández Romero

Alumno: Fernando Pedraza Garate

Fecha: 14 de octubre del 2024

Índice

Etapa 1 – Gestión de sesiones.

Introducción

La gestión de sesiones y la pérdida de autenticación son términos comunes en el contexto de seguridad informática, particularmente cuando se trabaja con aplicaciones web o servicios que requieren autenticación de usuarios, donde la sesión representa un período en el que el sistema y el usuario están conectados de manera autenticada, y la gestión, se refiere al control y mantenimiento de la sesión del usuario, una vez que ha sido autenticado, se crea una sesión única para identificarlo y asociar sus acciones en el sistema, en donde los sistemas suelen almacenar una "cookie", o un token para identificar al usuario en cada solicitud sin tener que pedir credenciales repetidamente, estas sesiones suelen tener un tiempo de vida limitado, si un usuario está inactivo durante mucho tiempo o si se cumplen ciertas condiciones, la sesión puede expirar y necesitará autenticarse de nuevo, el sistema debe permitir al usuario cerrar la sesión de manera segura cuando ya no necesite estar autenticado.

La pérdida de autenticación ocurre cuando un usuario pierde el acceso a su sesión autenticada por algún motivo, lo que puede requerir que se autentique nuevamente, y si la sesión tiene un tiempo de vida predeterminado y el usuario ha estado inactivo demasiado tiempo, el sistema cerrará la sesión automáticamente, en algunos casos, un administrador del sistema puede revocar las sesiones activas, en aplicaciones como escritorios remotos o servicios basados en la nube, una interrupción en la conexión puede causar pérdida de autenticación, obligando al usuario a volver a iniciar sesión y si los tokens de autenticación se invalidan o son manipulados (por ejemplo, en ataques de seguridad), el usuario perderá su autenticación.

Descripción.

Una empresa de software esta solicitando realizar varias pruebas de seguridad en páginas web que no cuentan con los candados de seguridad, y para la primera etapa, requiere se realice una prueba de la vulnerabilidad de la pérdida de autenticación y gestión de sesiones utilizando el programa WireShark con el objetivo de obtener las credenciales que se ingresaron y que estas se puedan mostrar

Posteriormente se deberá seleccionar un proyecto web que se haya realizado anteriormente y que cuente con las características de la función de inicio de sesión y de registro de usuarios, que cuente con conexión con una base de datos y subir el proyecto a un servidor web con la base de datos incluida.

Una vez que el proyecto esté en Internet, se realizará la instalación de WireShark, donde este programa permitirá realizar el ataque al sitio web, aprovechando la vulnerabilidad de falta de SSL o seguridad.

Justificación.

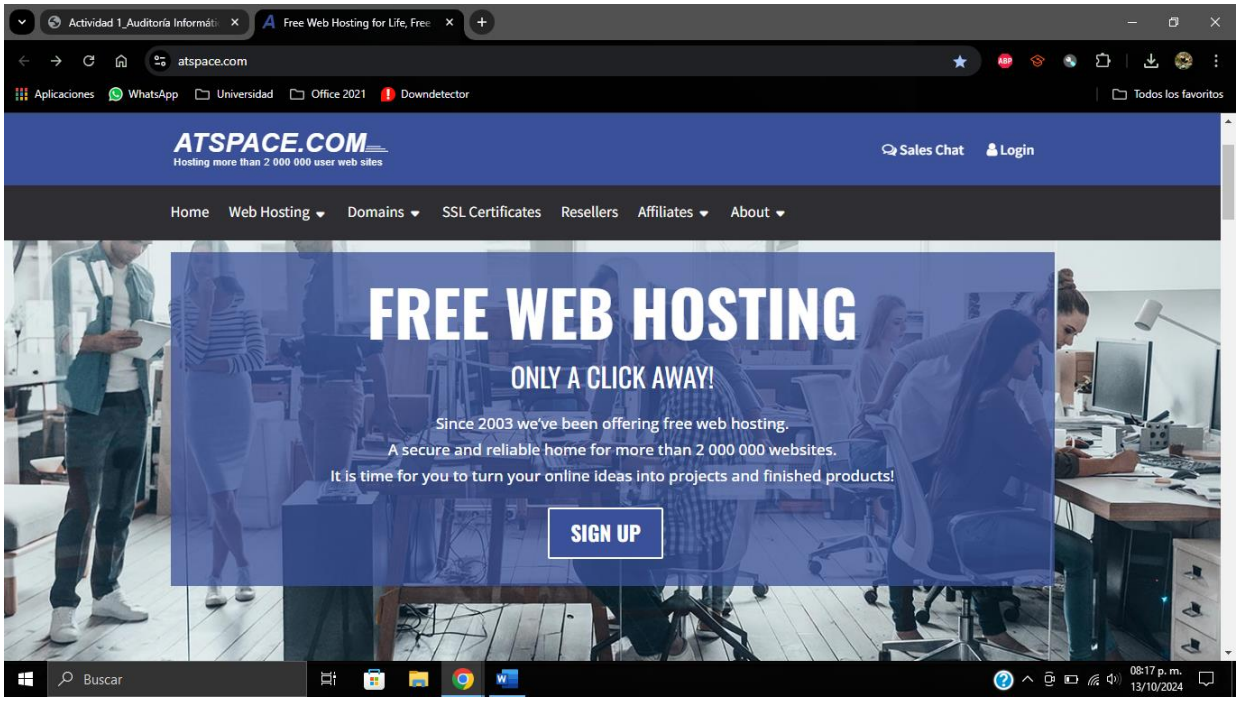
La gestión de sesiones es crucial en el diseño de sistemas que involucran la autenticación de usuarios y el acceso a recursos privados o sensibles, algunas de las razones por las que la gestión adecuada de sesiones es fundamental, es asegurar que el sistema pueda identificar y controlar quién está interactuando con él de manera continua, protegiendo así los datos sensibles de los usuarios, y al mantener controlada la sesión se evitaran situaciones de acceso no autorizado que pueden ser aprovechados por terceros malintencionados que accedan al dispositivo del usuario o intercepten su sesión, ayudando a mitigar ataques comunes como el hijacking de sesión (secuestrar una sesión activa) o la falsificación de solicitudes entre sitios (CSRF), situaciones donde el atacante utiliza una sesión activa para realizar acciones en nombre del usuario sin su consentimiento.

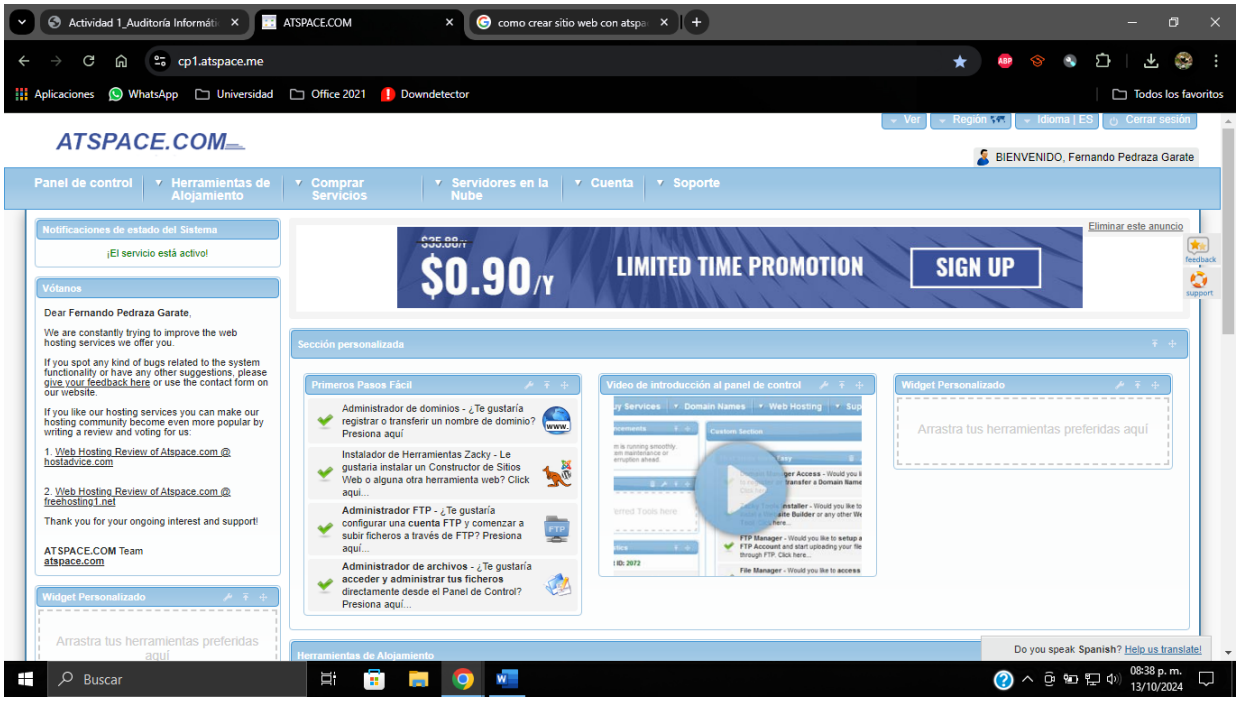
Un sistema bien gestionado en cuanto a sesiones puede mejorar la experiencia del usuario al evitar interrupciones innecesarias, cuando la sesión expira, el sistema puede pedir que el usuario vuelva a iniciar sesión de manera segura y controlada, minimizando los inconvenientes, permitiendo que los usuarios puedan retomar actividades donde las dejaron, si se implementan funcionalidades como "sesión persistente".

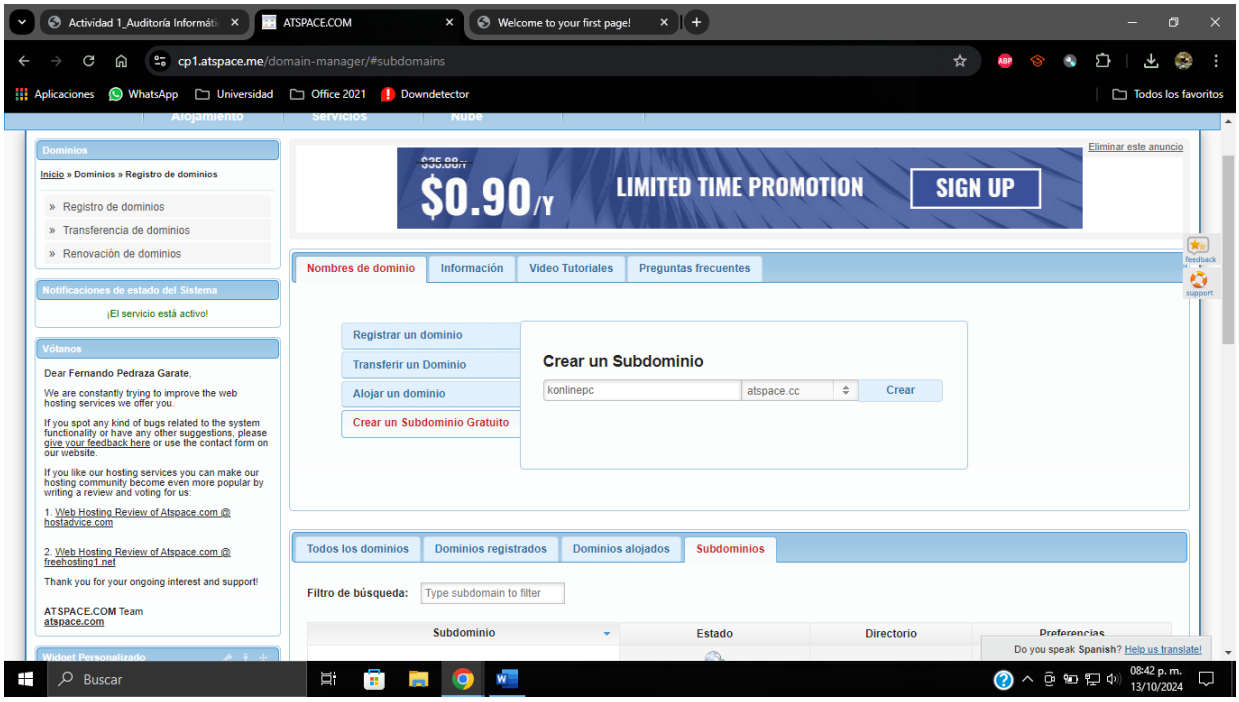
Muchos sectores (como el financiero, médico o gubernamental) están sujetos a normativas de protección de datos y seguridad (como el Reglamento General de Protección de Datos (GDPR) o la Ley de Portabilidad y Responsabilidad de los Seguros de Salud (HIPAA) en EE.UU.), y las sesiones deben ser gestionadas de forma que se pueda garantizar que solo los usuarios autenticados tienen acceso a ciertos recursos o datos, siendo necesario saber quién accedió a qué, cuándo, y desde dónde, y esto solo se puede hacer correctamente si las sesiones son gestionadas y registradas, impactando en la eficiencia y el rendimiento del sistema, liberando recursos, lo que es importante en sistemas de gran escala, previniendo sobrecarga por mantener demasiadas sesiones simultáneas abiertas innecesariamente.

Las políticas de seguridad internas de las empresas o instituciones muchas veces requieren una gestión de sesiones robusta para cumplir con los estándares de la industria como una autenticación multifactor (MFA), y bloqueo automático si se detectan actividades inusuales o cambios en el entorno de seguridad del sistema protegiendo al usuario contra ataques o accesos no autorizados.

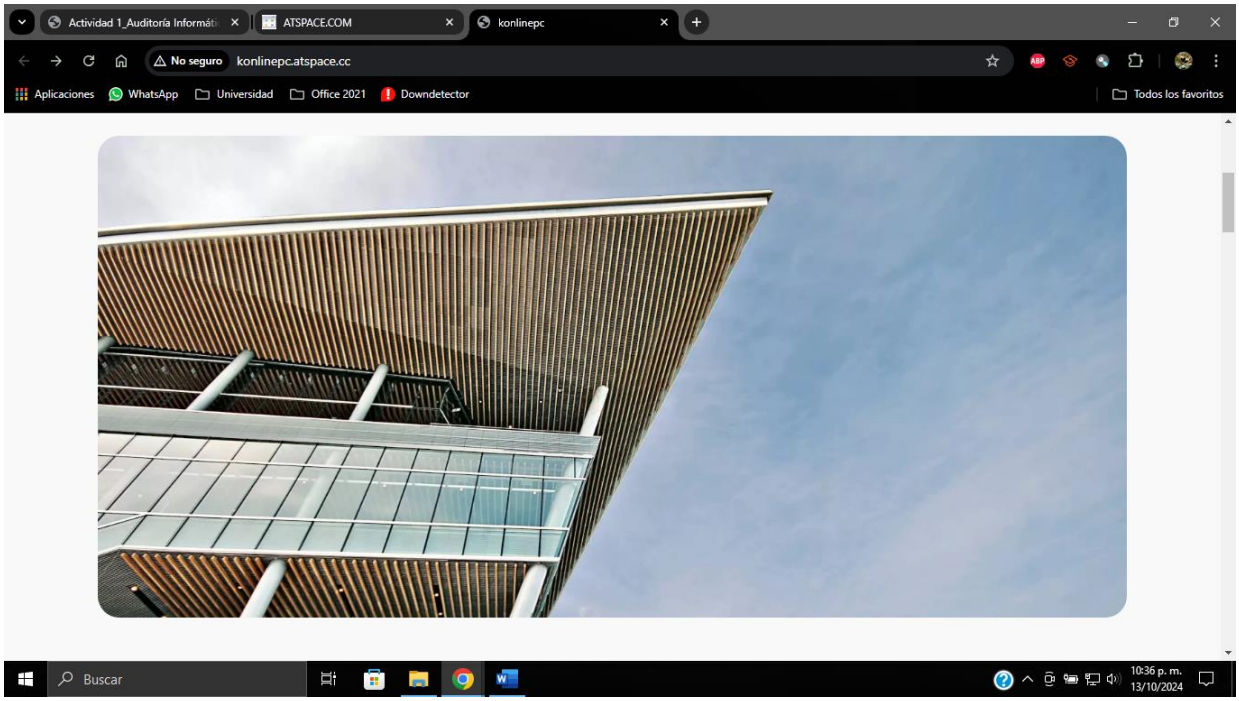
Desarrollo.

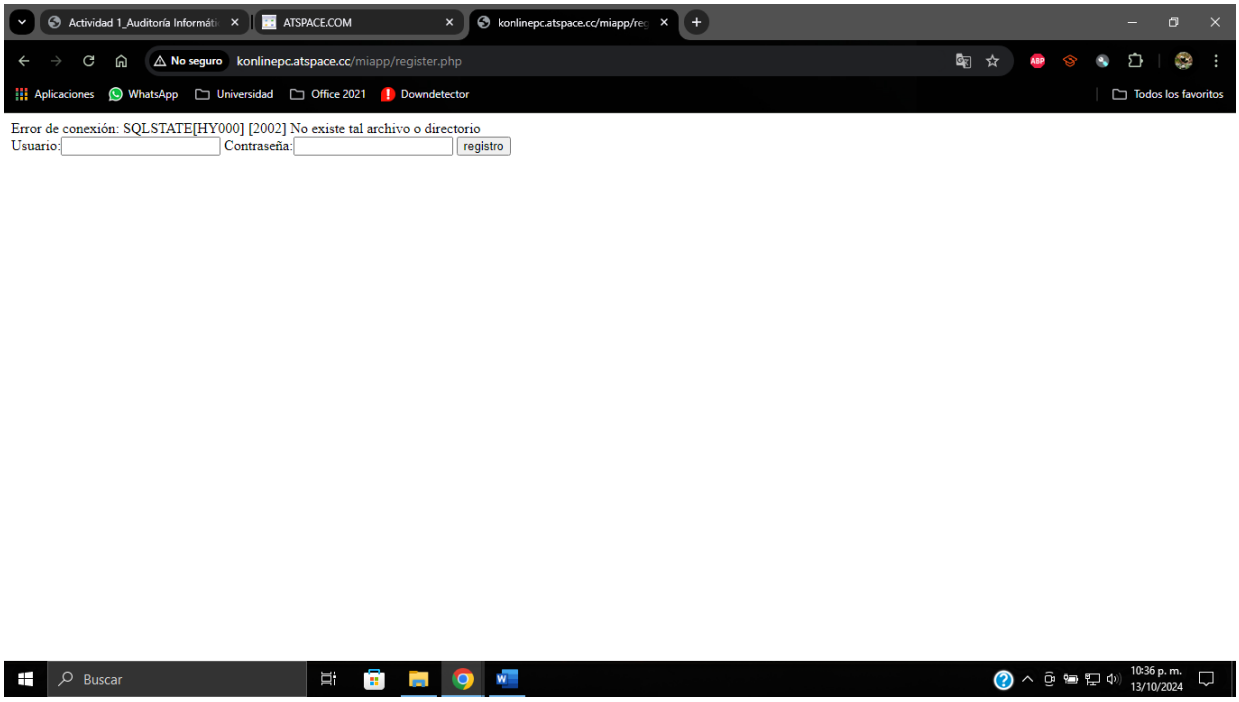

Actividad 1_Auditoría Informáti
Free Web Hosting for Life, Free
atspace.com
Aplicaciones
WhatsApp
Universidad
Office 2021
Downdetector
Todos los favoritos
ATSPACE.COM
Hosting more than 2 000 000 user web sites
Sales Chat
Login
Home
Web Hosting
Domains
SSL Certificates
Resellers
Affiliates
About
FREE WEB HOSTING
ONLY A CLICK AWAY!
Since 2003 we've been offering free web hosting.
A secure and reliable home for more than 2 000 000 websites.
It is time for you to turn your online ideas into projects and finished products!
SIGN UP
Buscar
08:17 p. m.
13/10/2024


Actividad 1_Auditoría Informáti
ATSPACE.COM
como crear sitio web con atspa
cp1.atspace.me
Aplicaciones
WhatsApp
Universidad
Office 2021
Downdetector
Todos los favoritos
ATSPACE.COM
Ver
Región
Idioma | ES
Cerrar sesión
BIENVENIDO, Fernando Pedraza Garate
Panel de control
Herramientas de Alojamiento
Comprar Servicios
Servidores en la Nube
Cuenta
Soporte
Notificaciones de estado del Sistema
¡El servicio está activo!
Vótanos
Dear Fernando Pedraza Garate,
We are constantly trying to improve the web hosting services we offer you.
If you spot any kind of bugs related to the system functionality or have any other suggestions, please give your feedback here or use the contact form on our website.
If you like our hosting services you can make our hosting community become even more popular by writing a review and voting for us:
1. Web Hosting Review of Atspace.com @ hostadvice.com
2. Web Hosting Review of Atspace.com @ freehosting1.net
Thank you for your ongoing interest and support!
ATSPACE.COM Team
atspace.com
Widget Personalizado
Arrastra tus herramientas preferidas aquí
$0.90/Y
LIMITED TIME PROMOTION
SIGN UP
Eliminar este anuncio
Sección personalizada
Primeros Pasos Fácil
Administrador de dominios - ¿Te gustaría registrar o transferir un nombre de dominio? Presiona aquí
Instalador de Herramientas Zacky - Le gustaría instalar un Constructor de Sitios Web o alguna otra herramienta web? Click aquí...
Administrador FTP - ¿Te gustaría configurar una cuenta FTP y comenzar a subir ficheros a través de FTP? Presiona aquí...
Administrador de archivos - ¿Te gustaría acceder y administrar tus ficheros directamente desde el Panel de Control? Presiona aquí...
Video de introducción al panel de control
Widget Personalizado
Arrastra tus herramientas preferidas aquí
Herramientas de Alojamiento
Do you speak Spanish? Help us translate!
Buscar
08:38 p. m.
13/10/2024

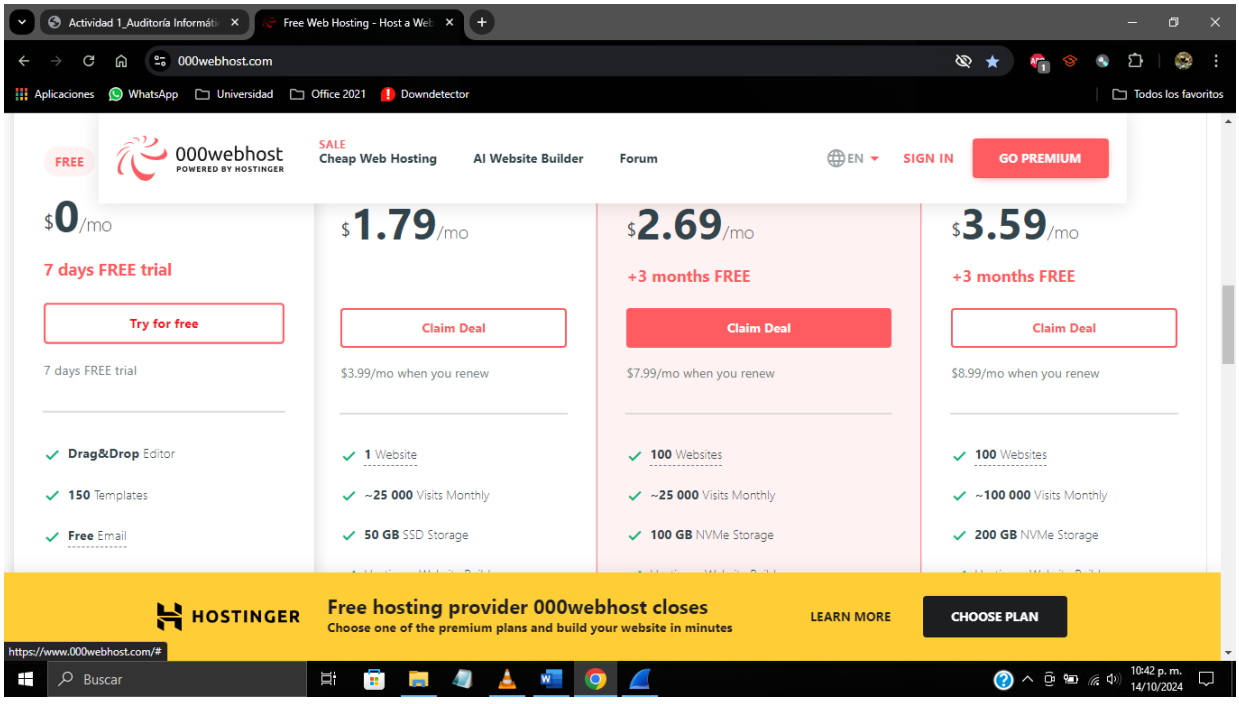


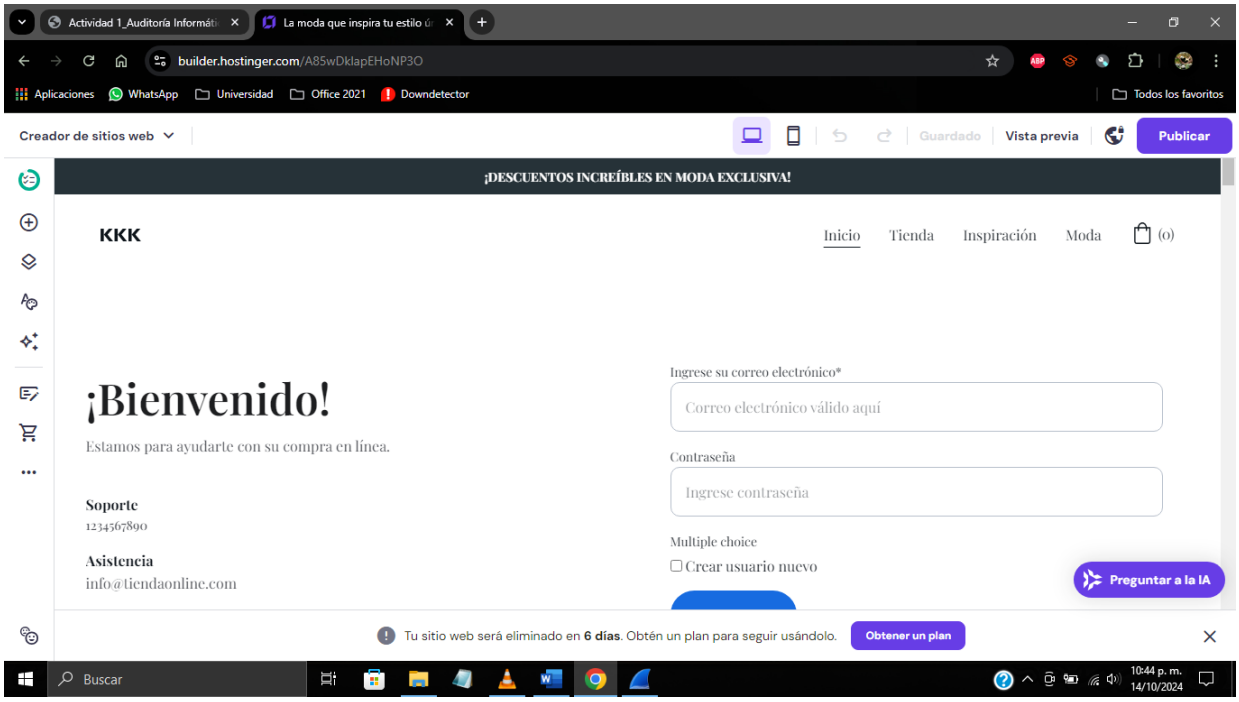
Se carga el proyecto donde se creó la página a monitorear con wireshark



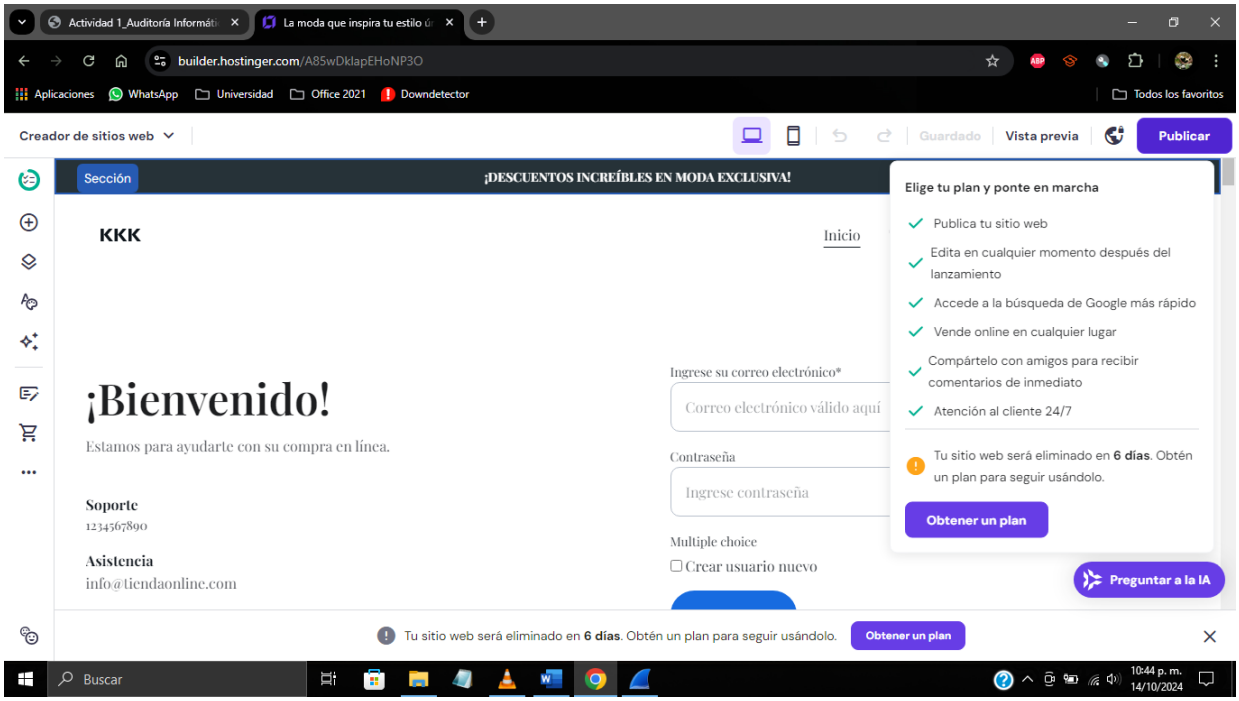


Sin poder cargar el dominio internet en la versión gratuita

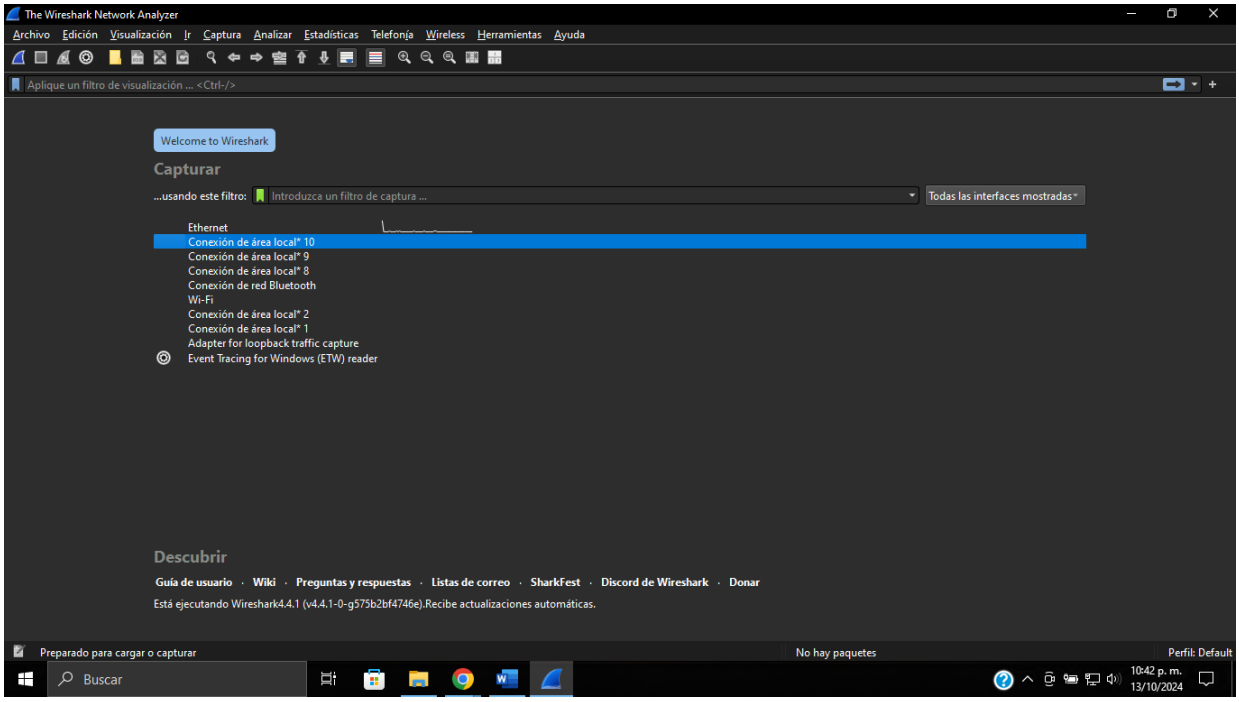


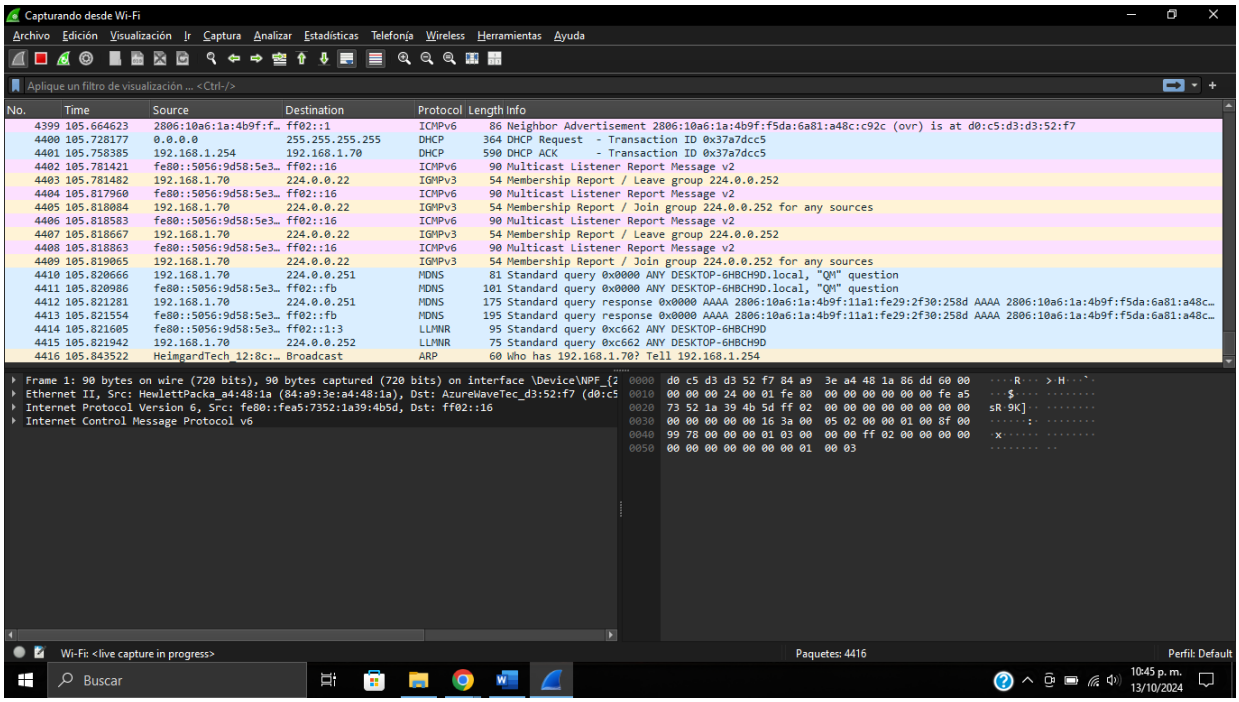


Intentando con Hostinger, obteniendo el mismo resultado



Se instala y se abre wireshark





Se ingresa al apartado de WiFi para monitorear el tráfico de red

Enlace de GitHub: https://github.com/Chifer888/Auditoria-informatica.git

Conclusión.

En conclusión, ambos conceptos son importantes para garantizar la seguridad y la usabilidad en sistemas que manejan sesiones de usuario y acceso a recursos sensibles, y se justifica como una práctica esencial para garantizar la seguridad, la experiencia del usuario, el cumplimiento de normativas, la eficiencia del sistema y la implementación de políticas de seguridad adecuadas.

¿Qué aprendo?

Que aún tengo mucho por aprender para poder gestionar el funcionamiento de las redes y poder detectar las intrusiones ajenas a mis equipos, que es sumamente importante establecer el tipo de seguridad que deben tener nuestros diseños para garantizar la seguridad y evitar que los datos de los usuarios sean interferidos por terceros al momento de autenticarse e ingresar a los sitios seleccionados que requieran de un inicio de sesión, aun cuando en la actualidad ya se contempla desde el momento de la elaboración de los diseños, al no permitir publicar las paginas sin establecer el tipo de seguridad a menos de requerir alguna remuneración de suscripción para poder publicarlas.

Referencias

ChatGPT. (n.d.). https://chatgpt.com/c/670afc6c-da4c-8003-83b6-7c97e3dd35fa

Wireshark · Go Deep. (n.d.). Wireshark. https://www.wireshark.org/

Luis Peralta Molina. (2021, August 2). *Como descargar e instalar Wireshark* [Video]. YouTube. https://www.youtube.com/watch?v=L07PeLPtvPo

Abel Albuez. (2018, June 26). *Subir pagina con PHP + Base de datos (MYSQL) a un Hosting* [Video]. YouTube. https://www.youtube.com/watch?v=5tXxoRKdCWo

000webhost. (n.d.). *Mejor Hosting Gratis de Mexico 2020 | Hosting Gratuito*. Free Web Hosting. https://mex.000webhost.com/