
# Actividad [#1] – [Pérdida de Autenticación y Gestión de Sesiones]

## [Auditoría Informática]

## Ingeniería en Desarrollo de Software

**Tutor: Lic. Jessica Hernández Romero**

**Alumno: Alan David López Rojas**

**Fecha:/09/2023**

# Índice

Introducción…….…..……. pág. 3

Descripción…….……..…. ……..…pág. 4

Justificación…….……..……. pág. 5

Descripción del sitio web…….……..……..…… pág. 6

Ataque al sitio……..……..……..……...…. pág. 8

Conclusión…….....…….…. pág. 13

Bibliografía…….……. pág. 14

## Introducción

La pérdida de autenticación y la gestión inadecuada de sesiones en la web representan una amenaza seria en el mundo digital que afecta a un amplio espectro de usuarios de Internet. Estas vulnerabilidades se producen cuando los sitios web no implementan medidas de seguridad sólidas, como la falta de cifrado SSL/TLS, exponiendo a las personas a riesgos considerables en línea. La importancia de esta cuestión se extiende a cualquier individuo que utilice la web para actividades como compras, comunicación, transacciones financieras o acceso a servicios en línea.

La pérdida de autenticación puede resultar en la captura de credenciales de inicio de sesión, lo que expone las cuentas en línea de los usuarios a amenazas. Esto puede dar lugar a situaciones de suplantación de identidad, donde los atacantes se hacen pasar por usuarios legítimos, poniendo en peligro la privacidad y los datos personales de las víctimas.

Además, la gestión deficiente de sesiones puede permitir a los atacantes acceder a cuentas y servicios sin autorización, lo que puede resultar en la pérdida de datos, la exposición de información financiera y la violación de la privacidad. Estas vulnerabilidades también pueden erosionar la confianza de los usuarios en la seguridad en línea y en los servicios que utilizan, lo que socava la adopción generalizada de tecnologías digitales.

**Descripción**

Espero comprender en profundidad cómo funcionan las vulnerabilidades de pérdida de autenticación y gestión de sesiones en los sitios web. Quiero aprender los conceptos subyacentes, cómo se explotan y cuáles son sus implicaciones para la seguridad en línea. Esto incluye comprender cómo se pueden robar credenciales de inicio de sesión y cómo se puede acceder a cuentas de usuarios sin autorización.

Además, espero adquirir habilidades prácticas en el uso de herramientas como WireShark para llevar a cabo pruebas de seguridad y evaluar la vulnerabilidad de los sitios web. Quiero aprender a identificar patrones y comportamientos sospechosos en el tráfico de red y a comprender cómo se pueden detectar estos problemas de seguridad.

También espero comprender la importancia del cifrado y de las mejores prácticas de seguridad en la web, como el uso de SSL/TLS. Deseo aprender cómo las implementaciones adecuadas de seguridad pueden prevenir estas vulnerabilidades y proteger la información confidencial de los usuarios.

En última instancia, espero que esta actividad me brinde un conjunto de habilidades valiosas en el campo de la seguridad cibernética y la evaluación de riesgos en línea. Quiero ser capaz de aplicar lo que aprenda en esta actividad para protegerme mejor en línea y, potencialmente, contribuir a la seguridad en línea en mi futuro profesional.

**Justificación**

La realización de pruebas de seguridad, como la prueba de vulnerabilidad de pérdida de autenticación y gestión de sesiones, es fundamental en el mundo actual en el que la información en línea y la interacción digital son partes esenciales de nuestras vidas. Esta justificación se centra en la importancia de llevar a cabo pruebas de este tipo de ataque.

En primer lugar, estas pruebas son cruciales para evaluar la seguridad de los sistemas en línea. En un momento en que los delincuentes cibernéticos están constantemente buscando vulnerabilidades para explotar, es esencial que las organizaciones y los individuos comprendan sus propias debilidades en términos de autenticación y gestión de sesiones. Estas pruebas proporcionan información valiosa sobre los posibles puntos débiles que los atacantes podrían aprovechar, lo que permite a las organizaciones tomar medidas preventivas antes de que ocurra un ataque real.

Además, estas pruebas son un componente esencial de la mejora continua de la seguridad en línea. La tecnología y las tácticas de los delincuentes cibernéticos evolucionan constantemente, por lo que las organizaciones deben estar un paso adelante. Al llevar a cabo pruebas de pérdida de autenticación y gestión de sesiones, las empresas pueden identificar y abordar las nuevas amenazas de seguridad a medida que surgen.

La realización de estas pruebas también demuestra el compromiso de una organización con la seguridad de los datos y la privacidad de los usuarios. Los clientes y usuarios confían en que sus datos personales y financieros están protegidos al interactuar en línea, y las pruebas de seguridad son una forma de respaldar esa confianza al mostrar un esfuerzo continuo por garantizar la seguridad.

**Descripción del sitio web**

**http://papeleria.free.nf/index.php**
**https://github.com/AlanDavidLR/AuditoriaInformatica.git**

Nombre de la Página Web: Papelería Acuario.

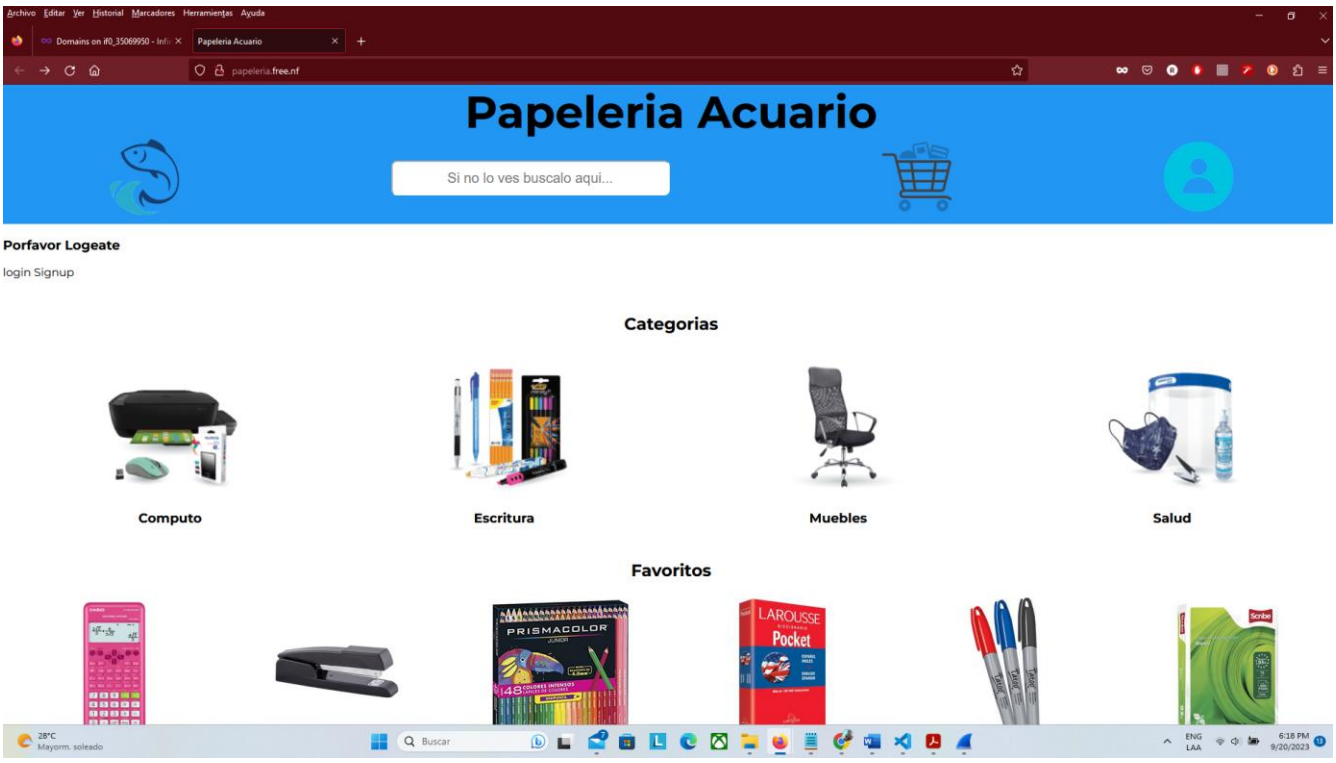
La página web es una aplicación web de e-comerce , enfocada a productos de una papelería, esta tiene funcionalidades de registro y acceso para usuarios. A continuación, se describe lo que hace:

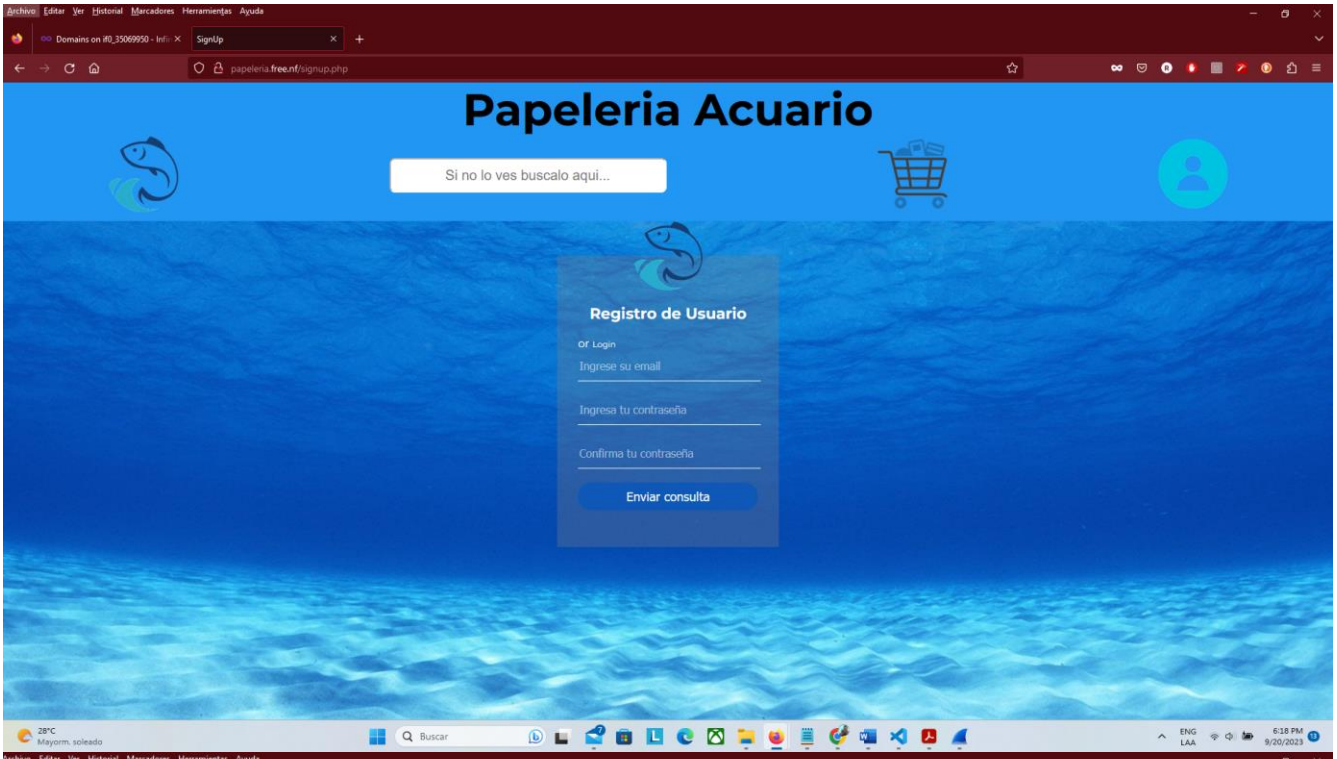
Registro de Usuarios: La página web permite a los usuarios registrarse proporcionando un correo electrónico y una contraseña. Además, deben confirmar su contraseña para garantizar que coincida con la contraseña original.

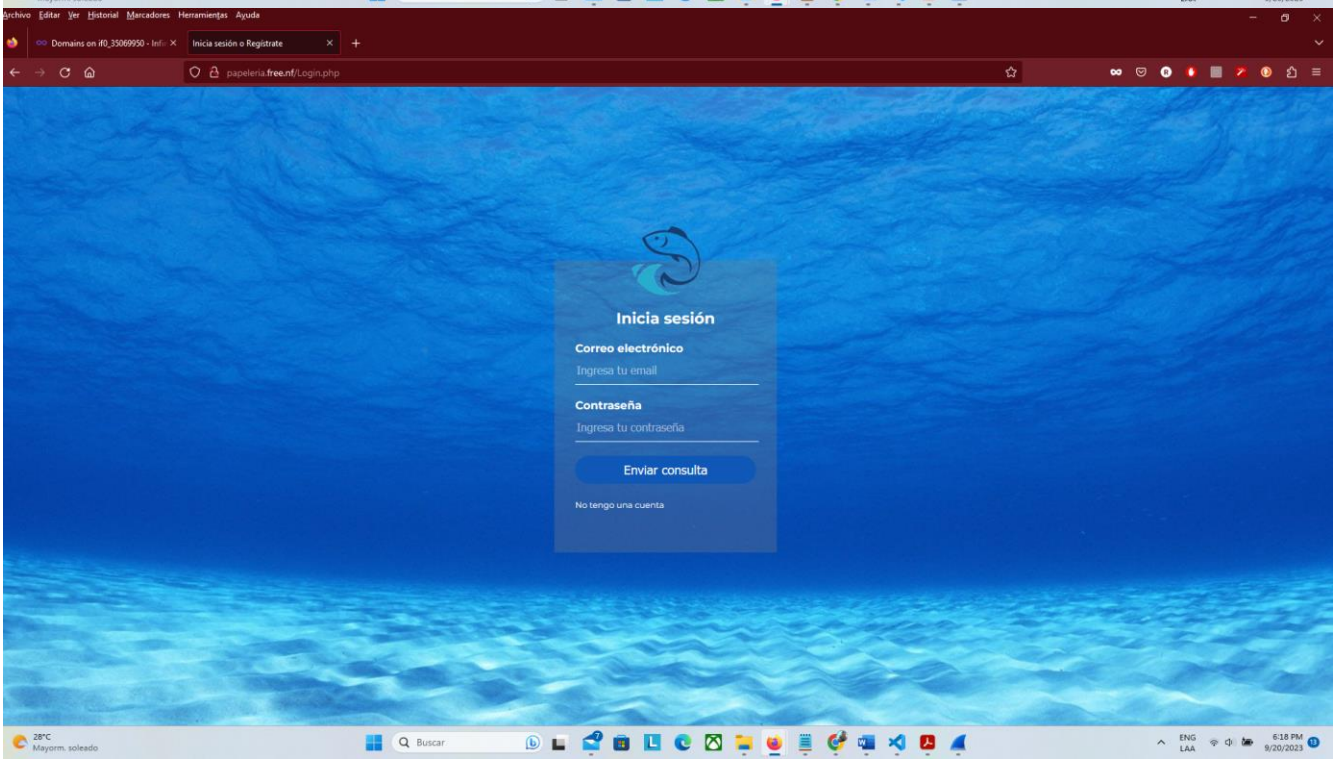
Inicio de Sesión: Después del registro, los usuarios pueden iniciar sesión en la página web utilizando su correo electrónico y contraseña registrados. Si los datos de inicio de sesión son correctos, se le redirige a la página principal.

Mensajes de Confirmación: La página web muestra mensajes de confirmación después de realizar acciones importantes, como el registro exitoso de un usuario o intentos de inicio de sesión fallidos.

Base de Datos: La página web se conecta a una base de datos MySQL, para guardar los usuarios y se encripta con bcrypt.

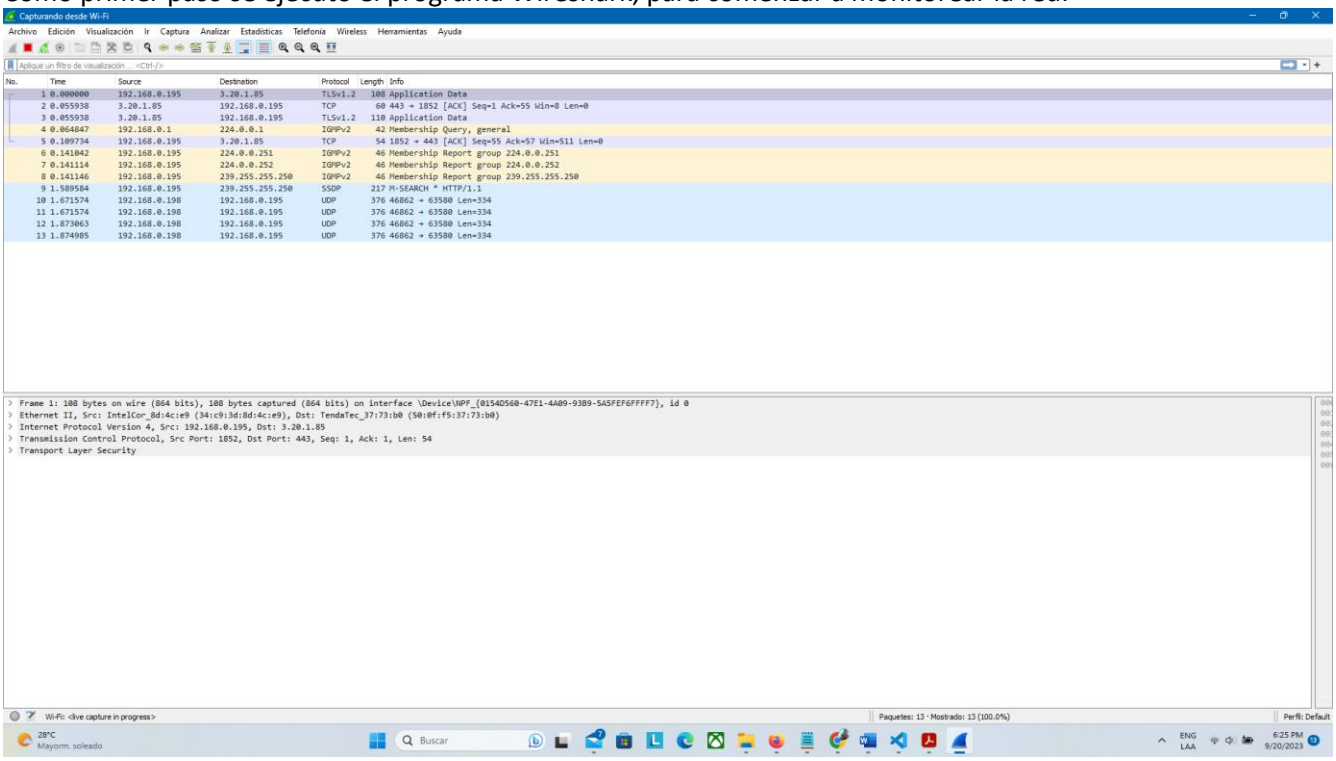



Archivo Editar Ver Historial Marcadores Herramientas Ayuda
Domains on if0_35069950 - Infi
SignUp
papeleria.free.nf/signup.php
Papeleria Acuario
Si no lo ves buscalo aqui...
Registro de Usuario
Or Login
Ingrese su email
Ingresa tu contraseña
Confirma tu contraseña
Enviar consulta
28°C
Mayorm. soleado
Buscar
ENG
LAA
6:18 PM
9/20/2023

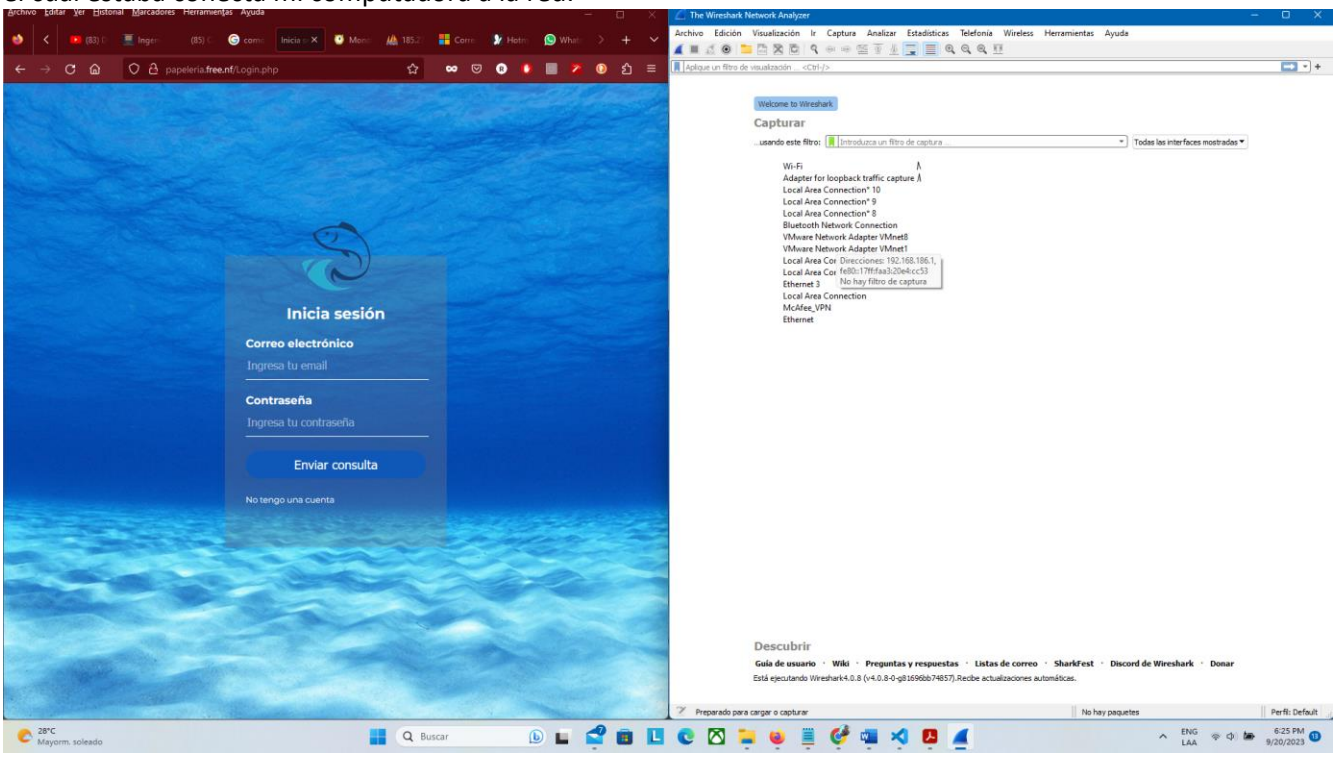

Archivo Editar Ver Historial Marcadores Herramientas Ayuda
Domains on if0_35069950 - Infi
Inicia sesión o Registrate
papeleria.free.nf/Login.php
Inicia sesión
Correo electrónico
Ingresa tu email
Contraseña
Ingresa tu contraseña
Enviar consulta
No tengo una cuenta
28°C
Mayorm. soleado
Buscar
ENG
LAA
6:18 PM
9/20/2023

## Ataque al sitio

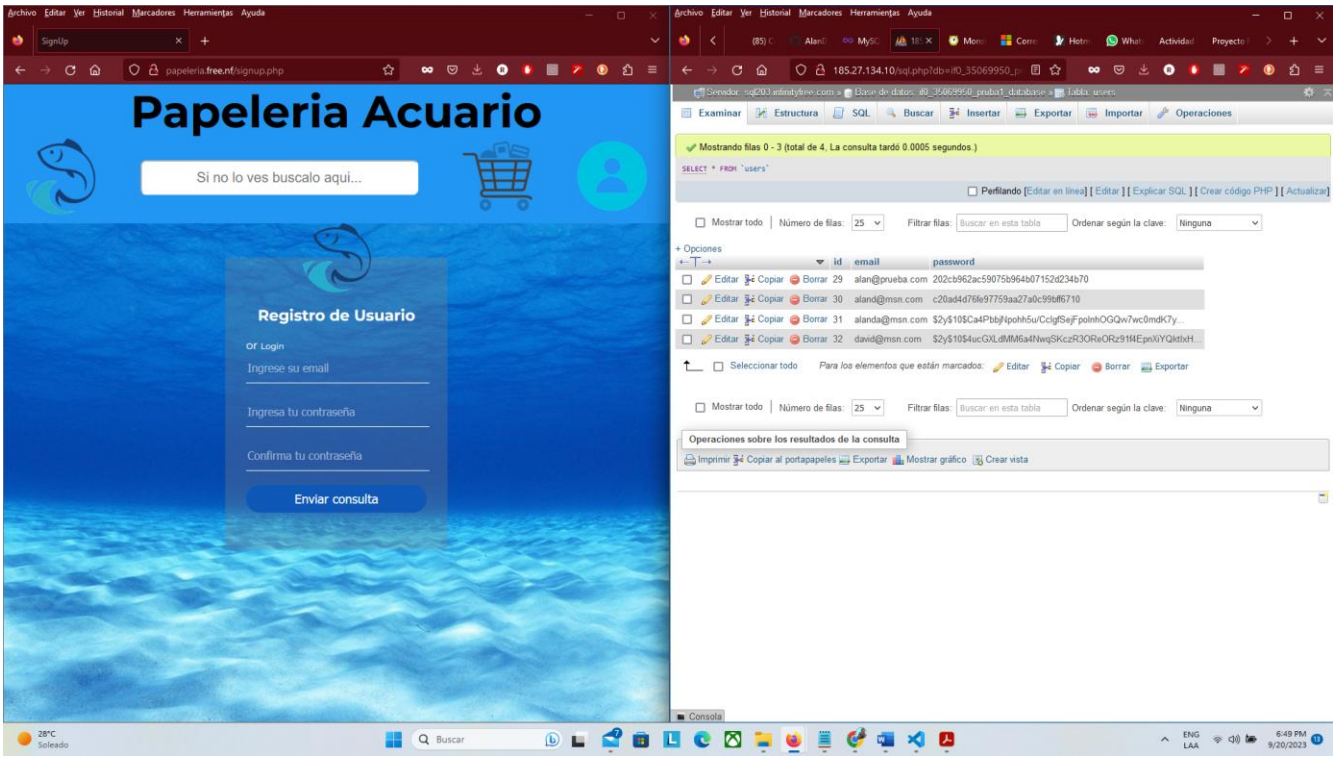
Como primer paso se ejecutó el programa Wireshark, para comenzar a monitorear la red.



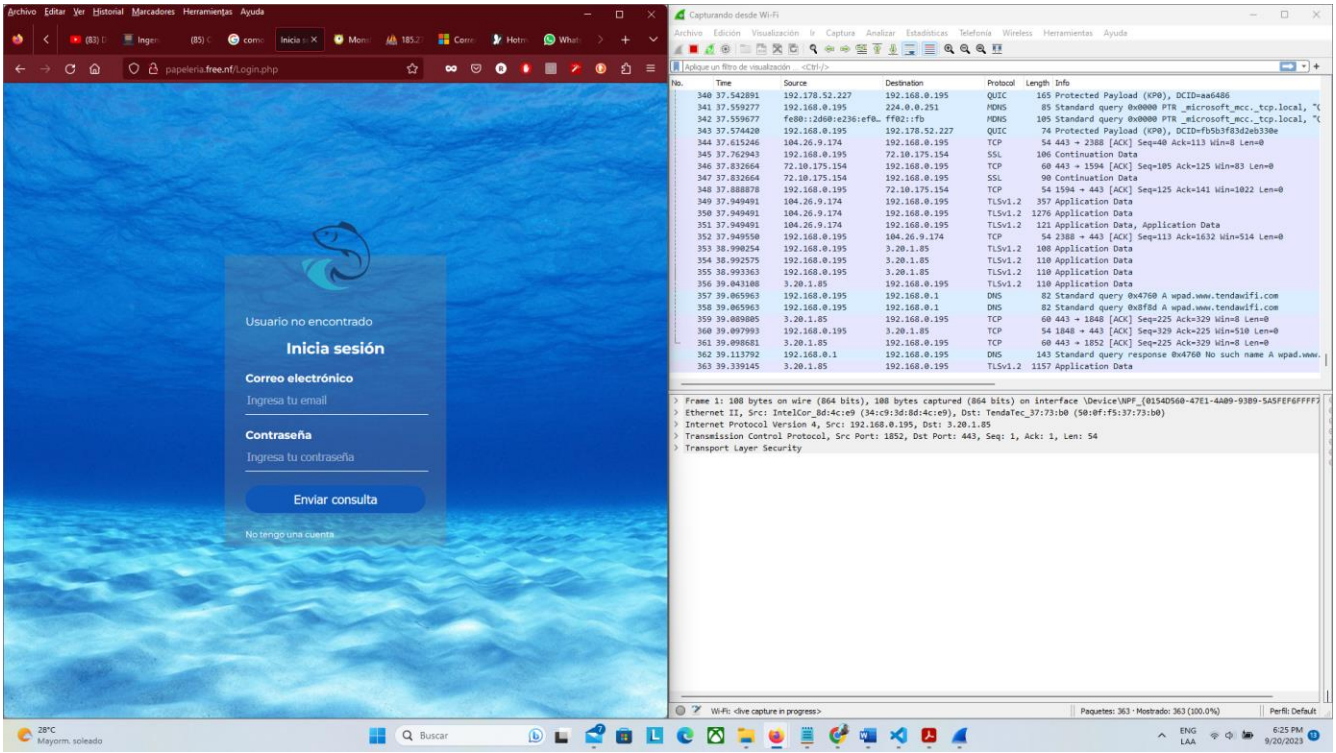

Ya estando activo se abrió el navegador Firefox, en el cual se accedió a la pagina ya creada con anterioridad desde los servidores de infinity free y en el programa se accedió al apartado de WIFI ya que por este medio es el cual estaba conecta mi computadora a la red.



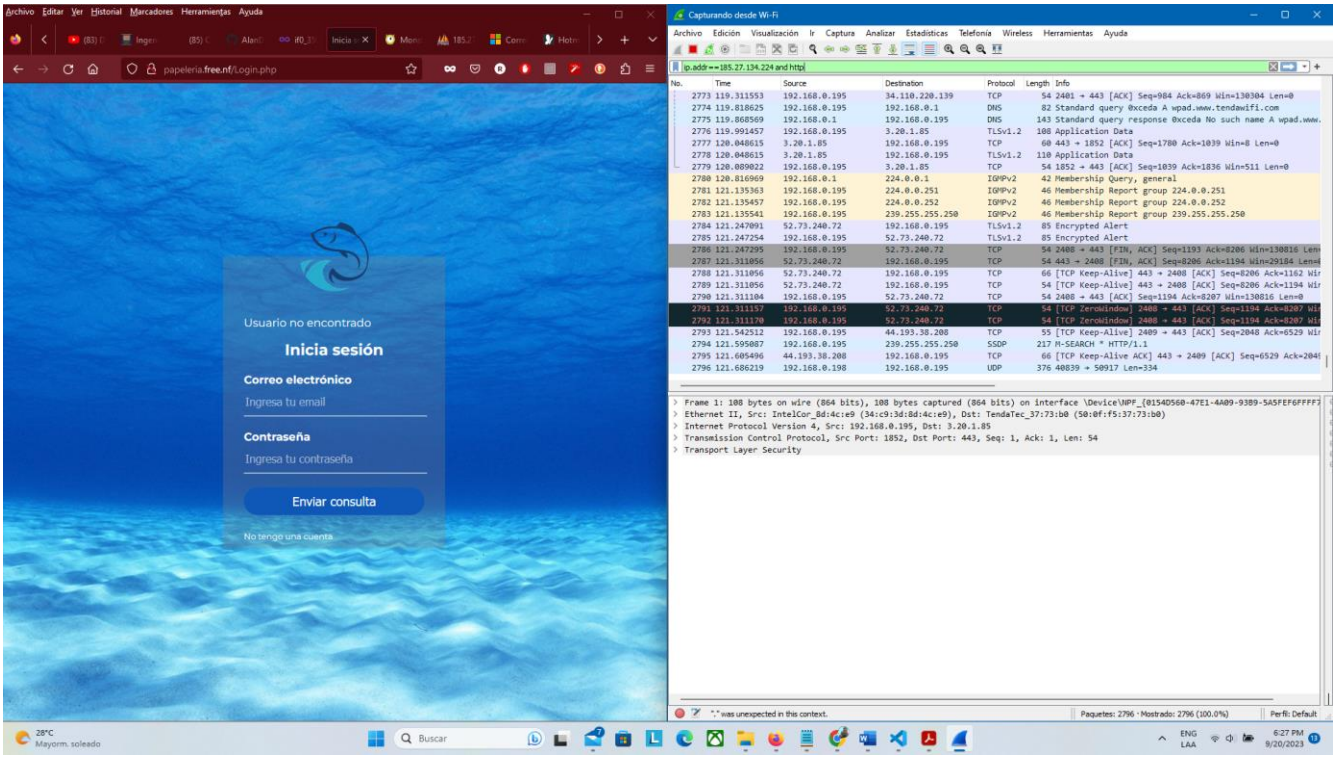
Previamente se había creado un usuario con el correo david@msn.com y una contraseña 123.



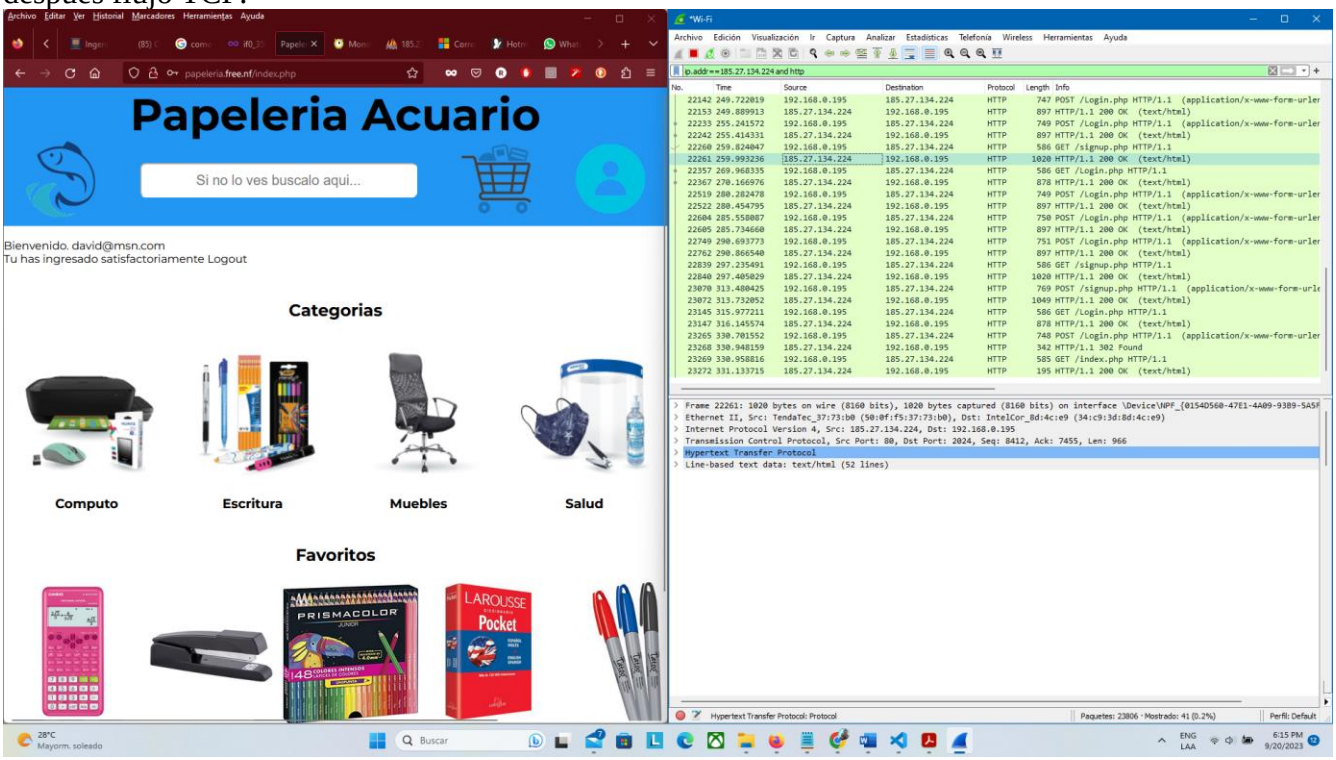

En el Login de mi página se ingresaron datos incorrectos para el correo.



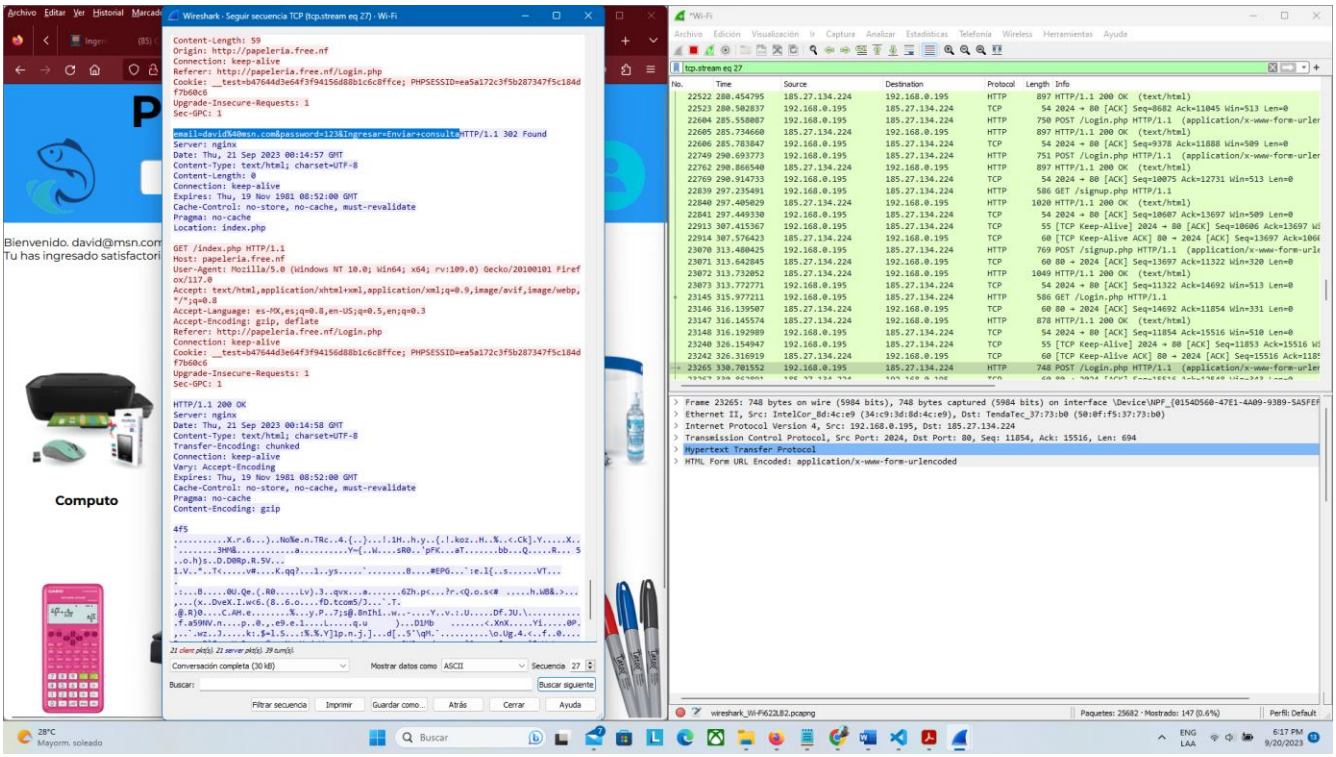
Una vez hecho se procedió a colocar el comando ip.add== con el ip de mi pagina y se realizo la búsqueda, el recuadro se marco con verde indicando que se encontró.




Se realizo nuevamente el ingreso de usuario esta vez con los datos correctos y se ingresó exitosamente, después en el ultimo registro con HTTP se dio clic con  el botón derecho y en la opción seguir y después flujo TCP.



**Abriendo una nueva ventana con los datos que se recopilaron, se marco con azul los datos que se obtuvieron que son el email y la contraseña.**



**Conclusión**

Habiendo completado la actividad que implicó la realización de pruebas de seguridad en páginas web con el enfoque en la vulnerabilidad de pérdida de autenticación y gestión de sesiones, puedo afirmar que esta experiencia ha tenido un impacto significativo en mi comprensión de la seguridad cibernética y su relevancia en mi campo laboral y vida cotidiana.

En mi campo laboral, esta actividad ha demostrado ser invaluable. Como profesional que trabaja en el desarrollo y mantenimiento de aplicaciones web y sistemas en línea, ahora tengo un conocimiento mucho más profundo sobre los riesgos que enfrentan las organizaciones y los usuarios en términos de seguridad en línea. Comprender cómo los atacantes pueden aprovechar las vulnerabilidades de autenticación y gestión de sesiones me ha convertido en un defensor más efectivo de la seguridad cibernética en mi lugar de trabajo. Puedo aplicar medidas preventivas proactivas y participar en la educación de mi equipo sobre las mejores prácticas de seguridad en el desarrollo de software.

Además, en mi vida cotidiana, esta actividad me ha dotado de una mayor conciencia y vigilancia en línea. Ahora tendré más cautela al interactuar con sitios web y servicios en línea, y tengo la capacidad de reconocer señales de advertencia de posibles amenazas de seguridad. Esto me permite tomar medidas para proteger mi propia información personal y financiera en línea, lo que es esencial en un mundo donde la privacidad y la seguridad son cada vez más importantes.

# Bibliografía

Borja Merino Febrero, Análisis De Tráfico Con Wireshark,  febrero 2011, INTECO-CERT, En línea: https://ns2.elhacker.net/timofonica/manuales/cert_inf_seguridad_analisis_trafico_wireshark.pdf

Mario Gerardo Piattini Velthuis, Emilio del Peso Navarro, Auditoría Informática Un enfoque práctico, 2.a edición ampliada y revisada, 2001 ALFAOMEGA Grupo Editor, S.A. de C.V. , En línea: http://cotana.informatica.edu.bo/downloads/ld-Auditoria-informatica-un-enfoque-practico-Mario-Piattini-pdf.pdf