Nombre:

Lirys Nayely Zambrano Salazar

NAO ID

3127

Fecha

18/08/2024

Nombre de la trayectoria

Integridad y autenticidad de la información

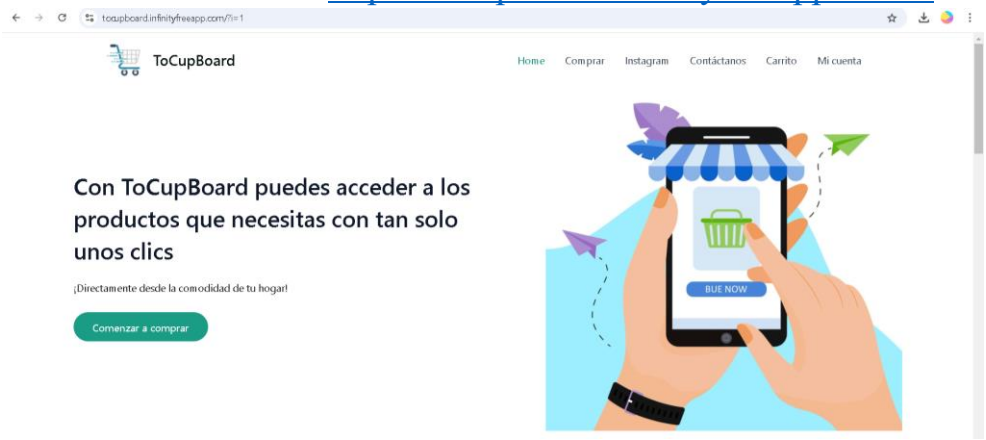
Título del Reto

Protocolos de seguridad con pentesting y criptografía

Reporte Técnico

1. Instrucciones para Acceder y Navegar por el Sitio Web

1.1 URL del Sitio Web: https://tocupboard.infinityfreeapp.com/#



1.2 Proceso de Acceso:

Desde la página de inicio, los usuarios pueden explorar las categorías de productos y seleccionar los artículos que desean adquirir.

- Navegación a través de las pestañas principales:
  Inicio: Muestra un poco de los servicios que presenta ToCupBoard.
  Comprar: Lista completa de productos.
  Instagram: Acceso directo al Instagram de la empresa
  Carrito: Los productos seleccionados por el usuario para compra.
  Contacto: Información para comunicarse con la empresa.
  Mi cuenta: Cuenta para poder acceder a realizar la compra

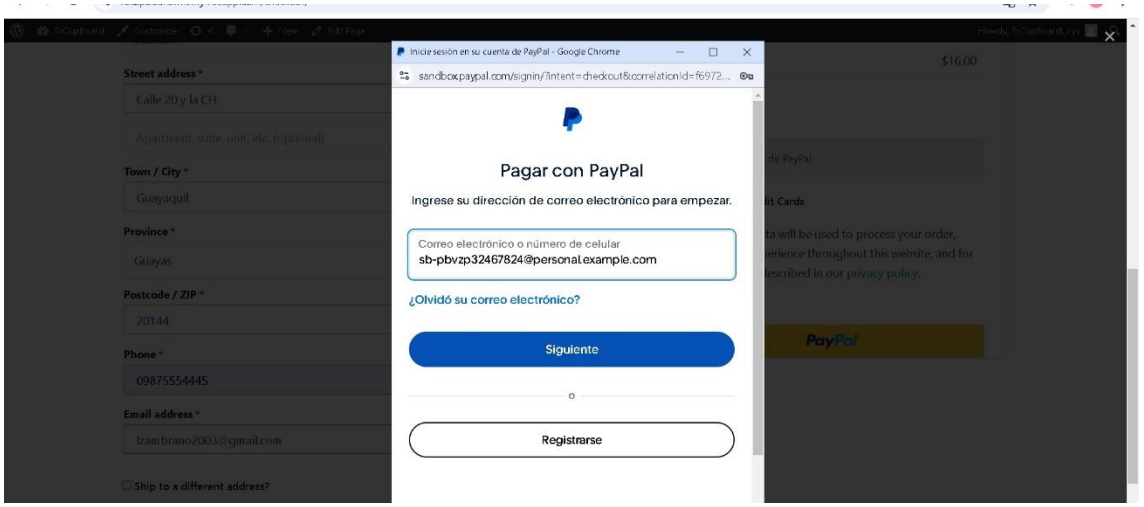
Proceso de Compra:

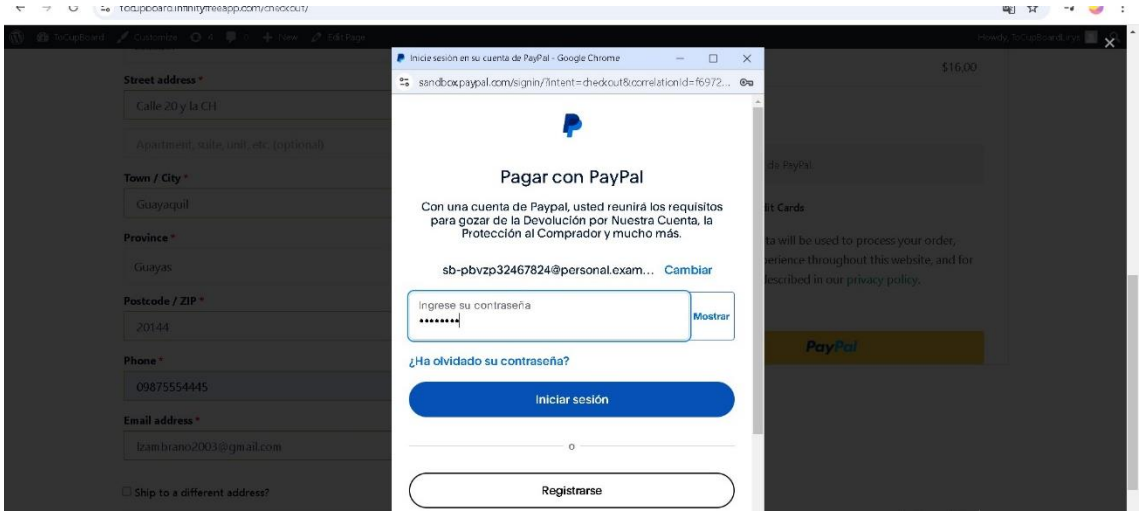
- Los usuarios pueden añadir productos al carrito y continuar con la simulación de compra, que incluye la pasarela de pagos integrada con PayPal (usando el entorno de pruebas Sandbox).

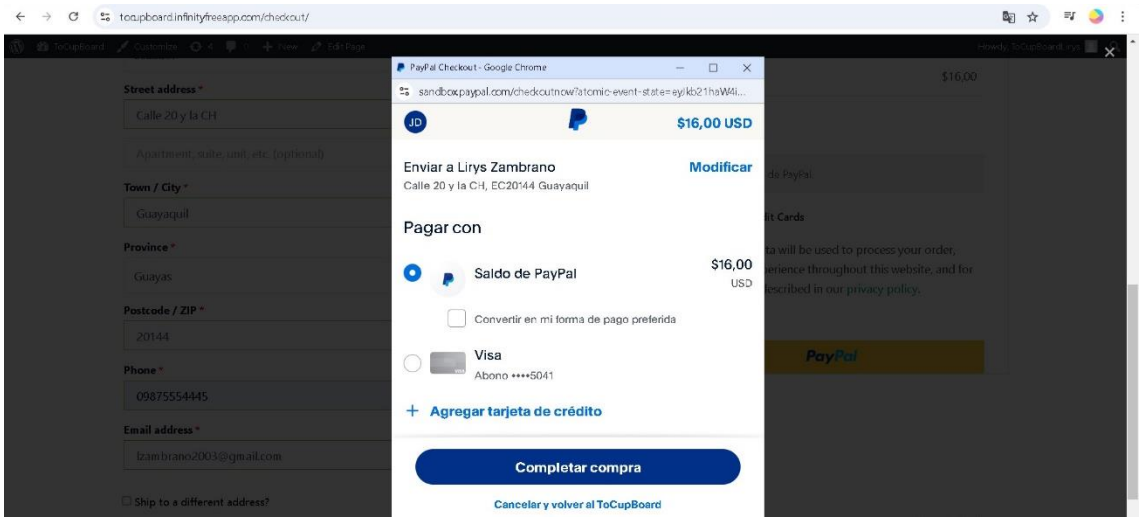
2. Descripción de las Llamadas a la API Implementadas

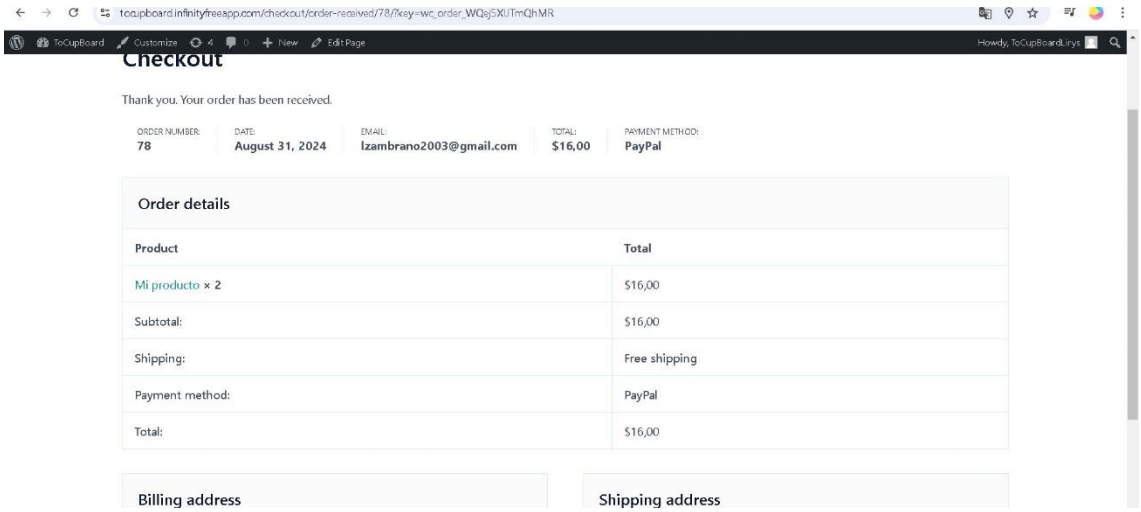
2.1 API de PayPal

Implementada para realizar el proceso de simulación de pagos a través de WooCommerce, que se conecta a la API de PayPal.
Se utilizó el entorno PayPal Sandbox para realizar pruebas seguras de los flujos de pago. Esta API permite gestionar los pagos de manera simulada para verificar el funcionamiento sin procesar transacciones reales.
Seguridad: Los pagos están autenticados utilizando un token de acceso que asegura la conexión y evita accesos no autorizados.


Inicie sesión en su cuenta de PayPal - Google Chrome
sandbox.paypal.com/signin/?intent=checkout&correlationId=f6972...
Pagar con PayPal
Ingrese su dirección de correo electrónico para empezar.
Correo electrónico o número de celular
sb-pbvzp32467824@personal.example.com
¿Olvidó su correo electrónico?
Siguiente
o
Registrarse
Street address *
Calle 20 y la CH
Town / City *
Guayaquil
Province *
Guayas
Postcode / ZIP *
20144
Phone *
09875554445
Email address *
lzambrano2003@gmail.com
Ship to a different address?
$16,00
PayPal


Inicie sesión en su cuenta de PayPal - Google Chrome
sandbox.paypal.com/signin/?intent=checkout&correlationId=f6972...
Pagar con PayPal
Con una cuenta de Paypal, usted reunirá los requisitos para gozar de la Devolución por Nuestra Cuenta, la Protección al Comprador y mucho más.
sb-pbvzp32467824@personal.exam... Cambiar
Ingrese su contraseña
Mostrar
¿Ha olvidado su contraseña?
Iniciar sesión
o
Registrarse
Street address *
Calle 20 y la CH
Town / City *
Guayaquil
Province *
Guayas
Postcode / ZIP *
20144
Phone *
09875554445
Email address *
lzambrano2003@gmail.com
Ship to a different address?
$16,00
PayPal


tocupboard.infinityfreeapp.com/checkout/
PayPal Checkout - Google Chrome
sandbox.paypal.com/checkoutnow?atomic-event-state=eyJkb21haW4i...
JD
$16,00 USD
Enviar a Lirys Zambrano
Modificar
Calle 20 y la CH, EC20144 Guayaquil
Pagar con
Saldo de PayPal
$16,00
USD
Convertir en mi forma de pago preferida
Visa
Abono ••••5041
Agregar tarjeta de crédito
Completar compra
Cancelar y volver al ToCupBoard
Street address *
Calle 20 y la CH
Town / City *
Guayaquil
Province *
Guayas
Postcode / ZIP *
20144
Phone *
09875554445
Email address *
lzambrano2003@gmail.com
Ship to a different address?
$16,00
PayPal

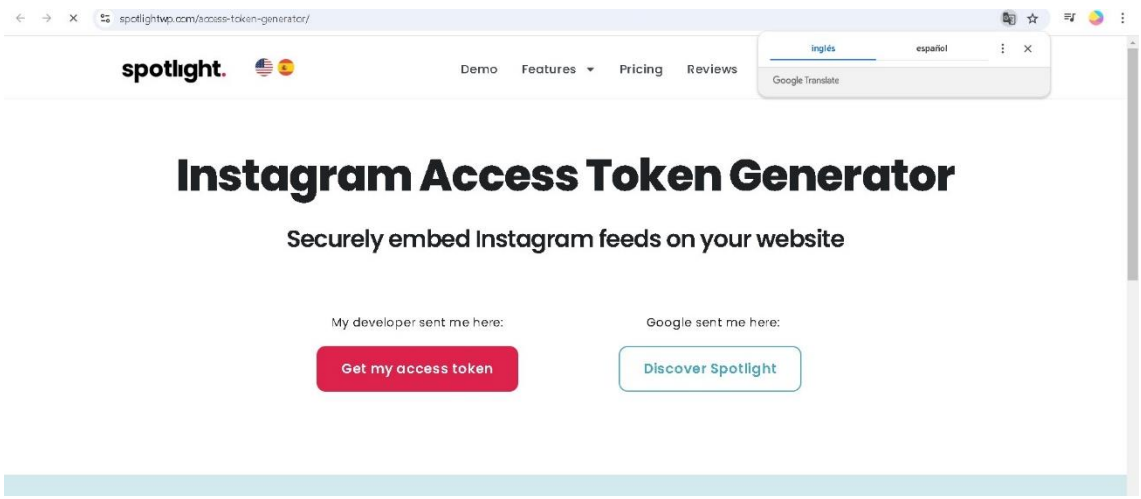


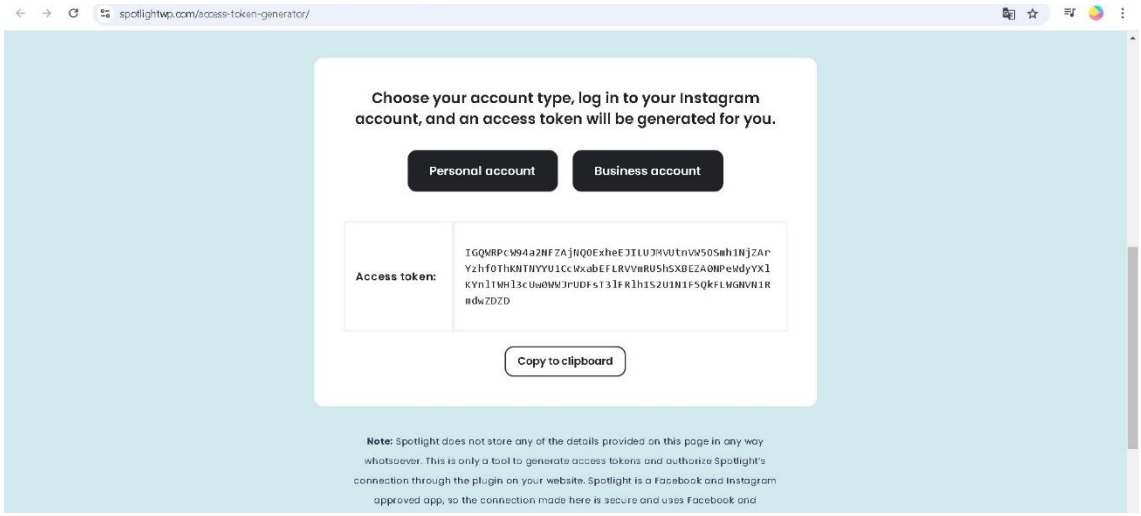
2.2 API de Instagram

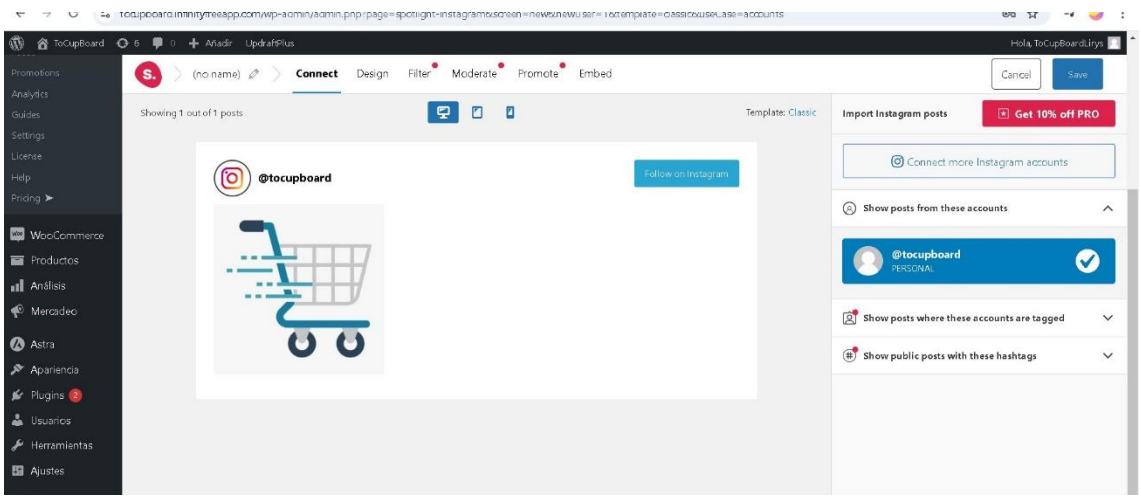
Se configuró una API de Instagram para obtener y mostrar contenido dinámico en el sitio web, específicamente imágenes o publicaciones recientes de la cuenta de Instagram de ToCupboard.

El plugin utilizado genera un access token que permite la conexión segura entre WordPress e Instagram. Este token está protegido para evitar accesos no autorizados.

Ideal cuando se trabaja con clientes y ellos no tengan que dar sus credenciales si no se sienten seguros al hacerlo.







3. Descripción del Proceso de Simulación de la Pasarela de Pagos

3.1 Proceso

Se utilizó WooCommerce para gestionar el carrito de compras y procesar los pagos simulados.
Los usuarios pueden seleccionar productos, añadirlos al carrito, y continuar con el proceso de pago, que está conectado a **PayPal Sandbox**.
Durante la simulación, el usuario es redirigido a la página de PayPal para simular el pago con credenciales de prueba proporcionadas por PayPal.
Al finalizar, WooCommerce recibe la confirmación del pago y actualiza el estado del pedido.

3.2 Seguridad

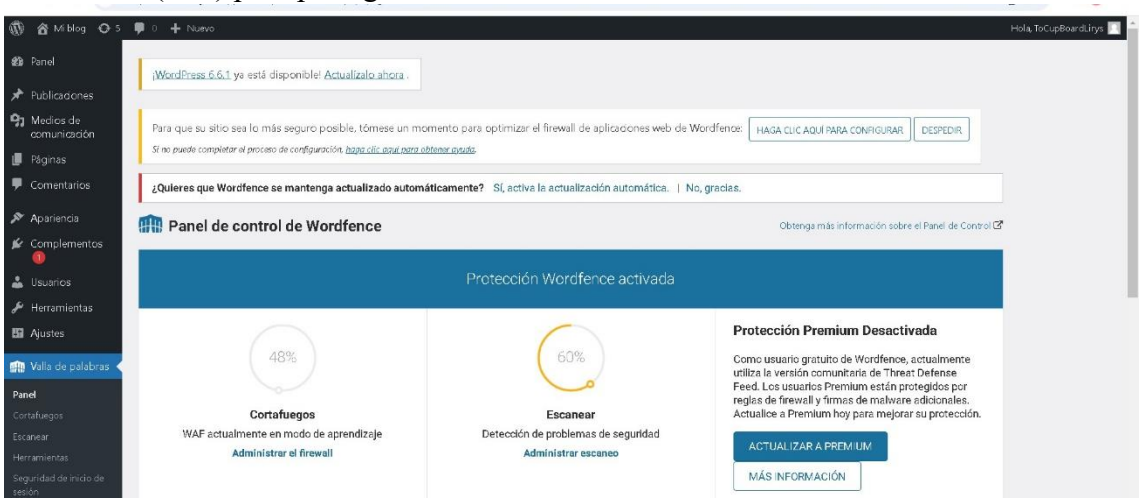
Se implementó la autenticación y autorización a través de tokens generados por PayPal.
Todos los datos sensibles se manejan utilizando el protocolo HTTPS, asegurando que la comunicación sea cifrada y segura.

4. Explicación Detallada de Cómo se Aplicó el Modelo DevSecOps

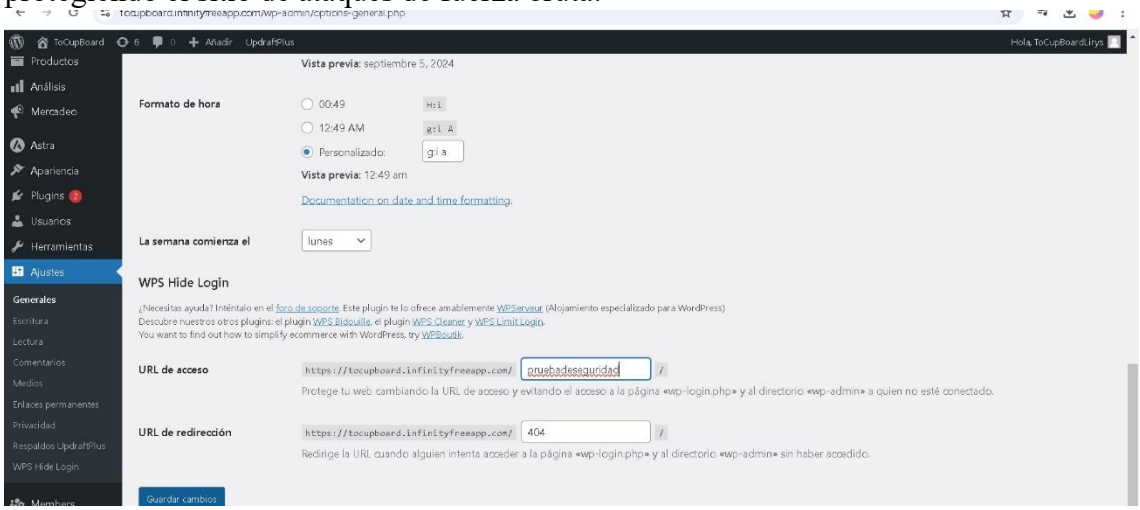
El modelo DevSecOps fue aplicado mediante la implementación de herramientas y prácticas de seguridad en cada fase del desarrollo del sitio.

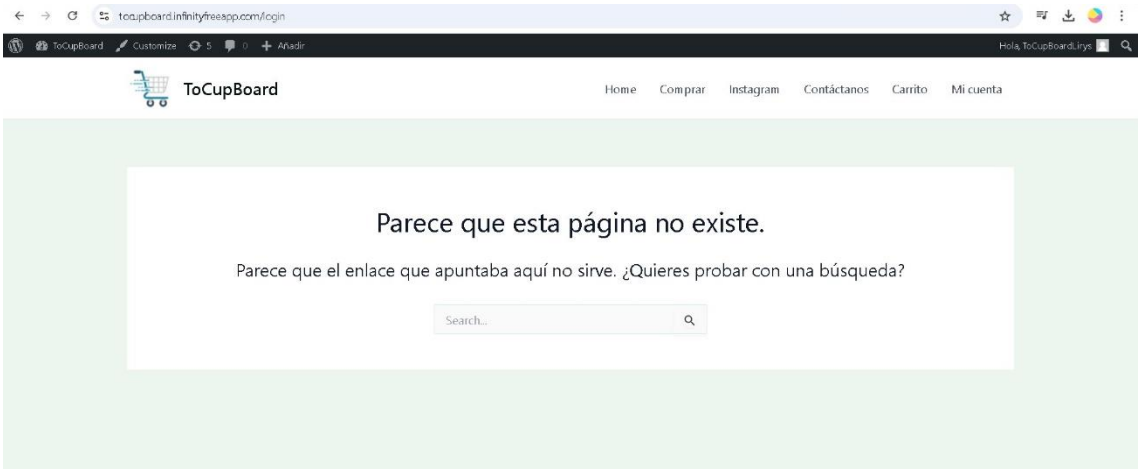
4.1 Prácticas de Seguridad Aplicadas

- **Wordfence:** Se configuró como un firewall y sistema de detección de intrusiones (IDS) para proteger el sitio contra amenazas comunes.

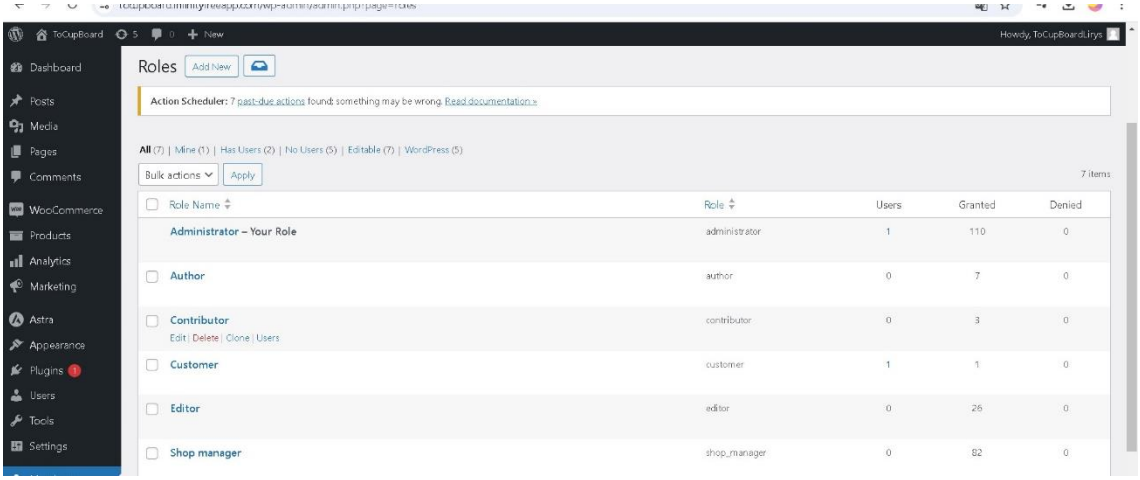


- **WPS Hide Login:** Se utilizó para ocultar la URL de inicio de sesión, protegiendo el sitio de ataques de fuerza bruta.

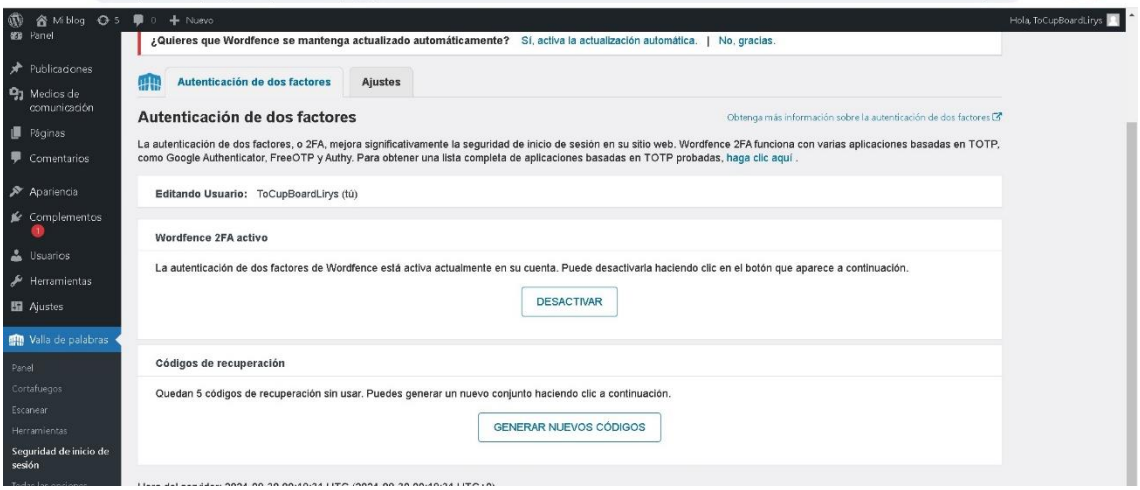




- **Members:** Este plugin fue utilizado para la gestión de roles y permisos, asegurando que solo los usuarios autorizados puedan acceder a las áreas administrativas.



- **Doble Autenticación:** Se habilitó la autenticación de dos factores (2FA) para agregar una capa adicional de seguridad a las cuentas administrativas.



- **Monitoreo de Vulnerabilidades:** Se configuró Wordfence para realizar escaneos regulares de seguridad y monitorear vulnerabilidades, asegurando que el sitio esté protegido de amenazas emergentes.

- **Control de Accesos y Permisos:** A través del plugin Members, se limitaron los accesos a funciones administrativas, asegurando que solo los usuarios autorizados puedan realizar cambios críticos en el sitio.
- **UpdraftPlus**: Es el plugin encargado de realizar copias de seguridad regulares del sitio, garantizando la protección de los datos y la posibilidad de restaurar el sitio en caso de fallos o ataques.