NOMBRE:

JEREMY SAUL ALBAN RUIZ

NAO ID:

3131

Fecha:

01/09/2024

NOMBRE DE LA TRAYECTORIA:

CONSULTOR DE CIBERSEGURIDAD

RETO:

PROTOCOLOS DE SEGURIDAD CON PENTESTING Y CRIPTOGRAFÍA

Tabla de contenido

Instrucciones para acceder y navegar por el sitio web:

Acceso al Sitio Web

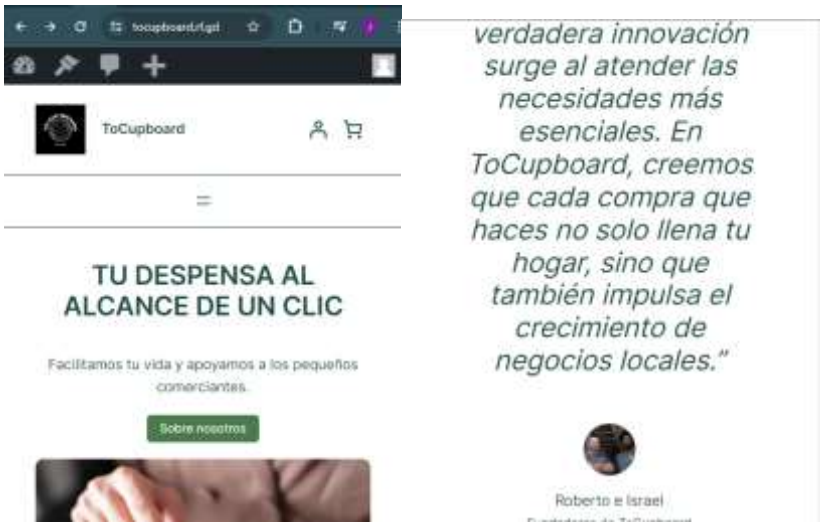
- URL: https://www.tocupboard.rf.gd
- El sitio es compatible con dispositivos móviles y de escritorio, por lo que su diseño es responsivo.

Navegación por el Sitio Web

La página web de ToCupboard está desarrollada en WordPress y cuenta con un diseño profesional y responsive, adaptado a las necesidades de la empresa. A continuación, se describen las secciones y funcionalidades principales:

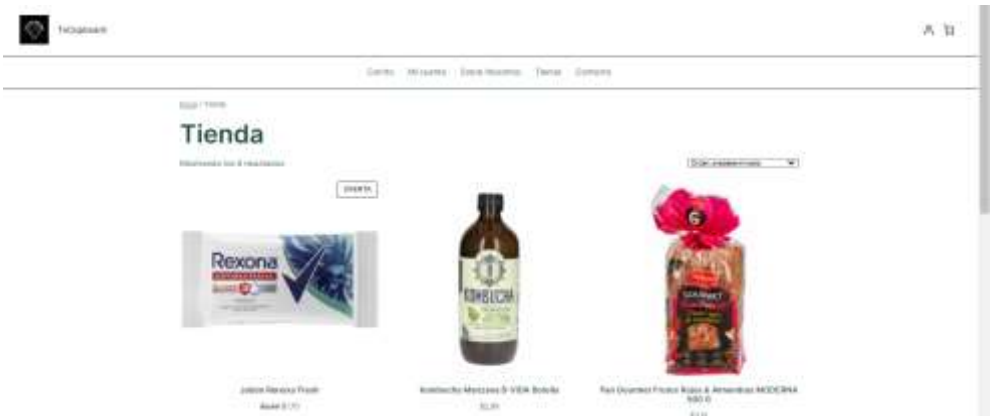
- **Inicio**: Presenta un mensaje de bienvenida de la empresa y una selección de productos destacados.

  - Móvil

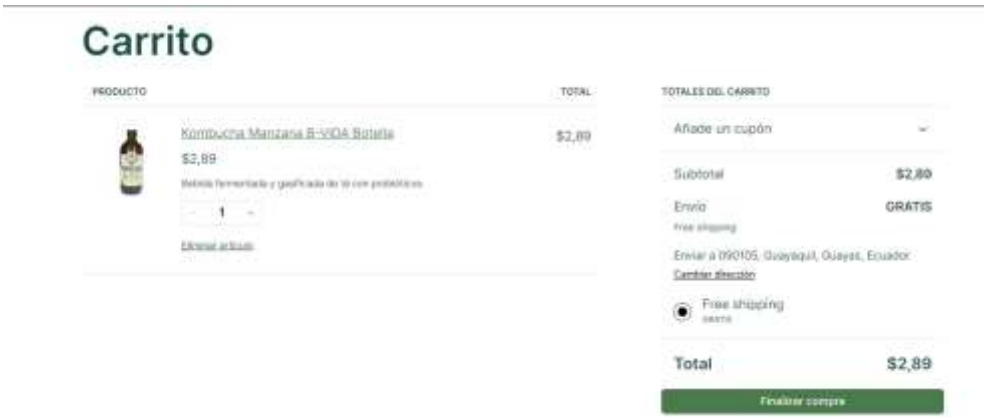


  - Web

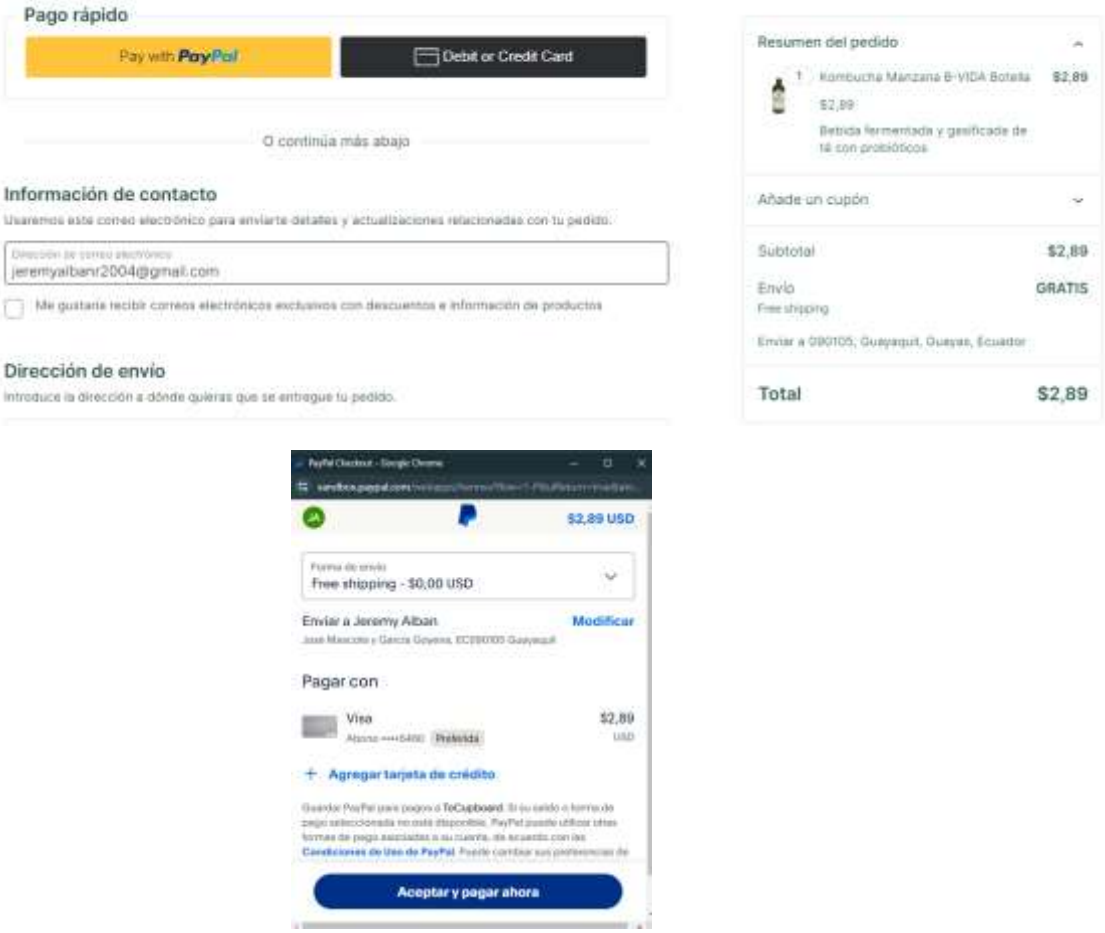
- **Tienda**: Muestra todos los productos disponibles en la tienda, con detalles como precio, descripción y disponibilidad.



- **Carrito**: Aquí los usuarios pueden ver los productos agregados para su compra y realizar modificaciones antes de proceder al pago.



- **Finalizar compra**: Esta página procesa el pago utilizando PayPal, donde los usuarios son redirigidos a una ventana segura para completar la transacción.



- **Nosotros**: Proporciona información sobre la misión y visión de ToCupboard, destacando los valores de la empresa.

- **Contacto**: Un formulario de contacto está disponible para que los usuarios envíen sus preguntas o comentarios, ingresando su nombre, correo y un mensaje.

- **Cuenta**: Los usuarios registrados pueden acceder a esta sección para gestionar sus datos personales, ver pedidos anteriores y realizar configuraciones adicionales.

- **Inicio de sesión**: Debe tocar el ícono de la persona en el lado derecho superior del sitio web. Permite a los usuarios registrarse, iniciar sesión y recuperar su contraseña en caso de ser necesario.

Plugins utilizados:

Todos los plugins implementados están actualizados y aseguran el funcionamiento óptimo y seguro del sitio web. Algunos de ellos incluyen:

- **WooCommerce**: Principal plugin utilizado para gestionar los productos y la tienda online.
- **WooCommerce PayPal Payments**: Permite la integración con PayPal, ofreciendo una pasarela de pago segura para procesar compras.
- **WPForms Lite**: Plugin utilizado para crear formularios de contacto, con opciones para captar datos básicos de los usuarios.
- **Elementor**: Plugin utilizado para diseñar y personalizar las páginas del sitio web con un enfoque visual y fácil de manejar.
- **Sucuri Security** y **Wordfence Security**: Herramientas implementadas para proteger el sitio de amenazas externas y realizar auditorías de seguridad.
- **Really Simple SSL**: Plugin que facilita la configuración de HTTPS en todo el sitio, garantizando que todas las comunicaciones estén cifradas y sean seguras.
- **WP Mail SMTP** y **WP Mail Logging**: Utilizados para gestionar y monitorizar el envío de correos electrónicos desde el sitio, asegurando la correcta entrega de mensajes.

Este conjunto de plugins asegura tanto la funcionalidad del sitio como su seguridad, siguiendo las mejores prácticas para el desarrollo en WordPress.

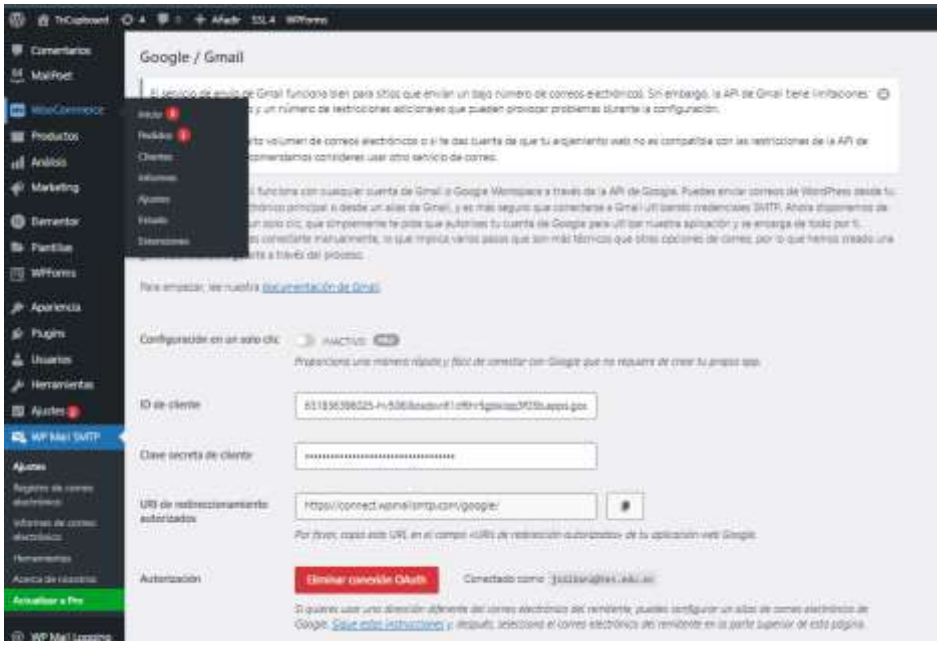
Descripción de las llamadas a la API implementadas

En la página web de ToCupBoard, se han integrado diversas APIs para garantizar funcionalidades críticas, como el manejo de correos electrónicos y la simulación de pagos. A continuación, se detallan las APIs implementadas y las medidas de seguridad adoptadas:

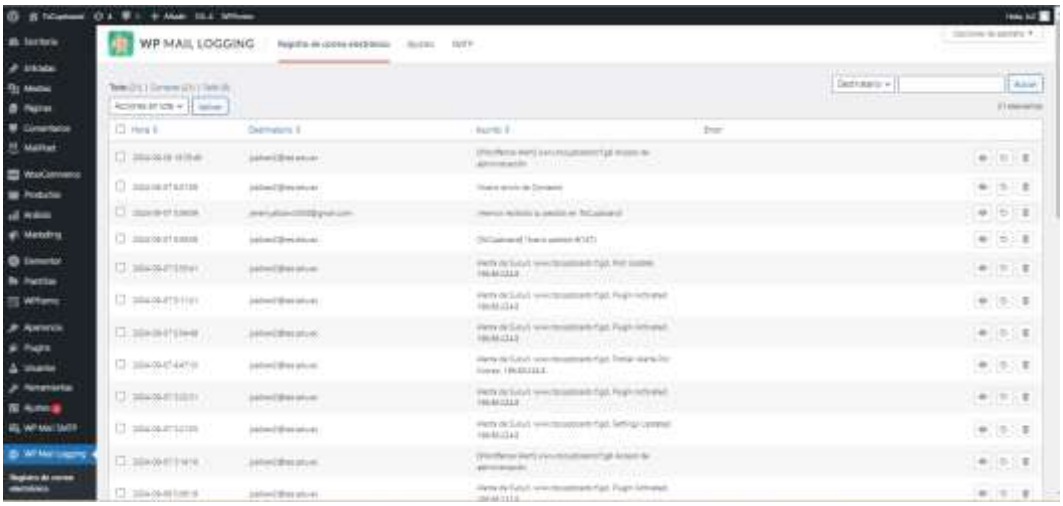
1. Gmail API

- **Función**: La API de Gmail se utiliza para gestionar el envío de correos electrónicos en el sitio, particularmente en la sección de "Contacto". Cada vez que un usuario completa el formulario de contacto, los datos se envían de manera segura mediante la integración con **WP Mail SMTP**, configurado con la **API de Gmail**. Esto asegura que los correos sean entregados de manera confiable, utilizando las credenciales del servidor de Gmail.
    - **Gmail API configuración**:

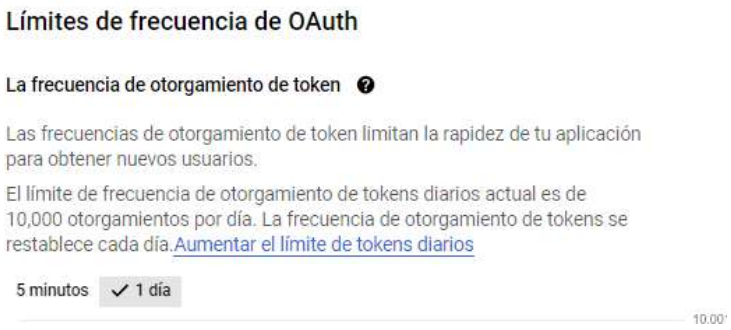
- **WP Mail SMTP (enlazado con las credenciales de GMAIL APIs)**



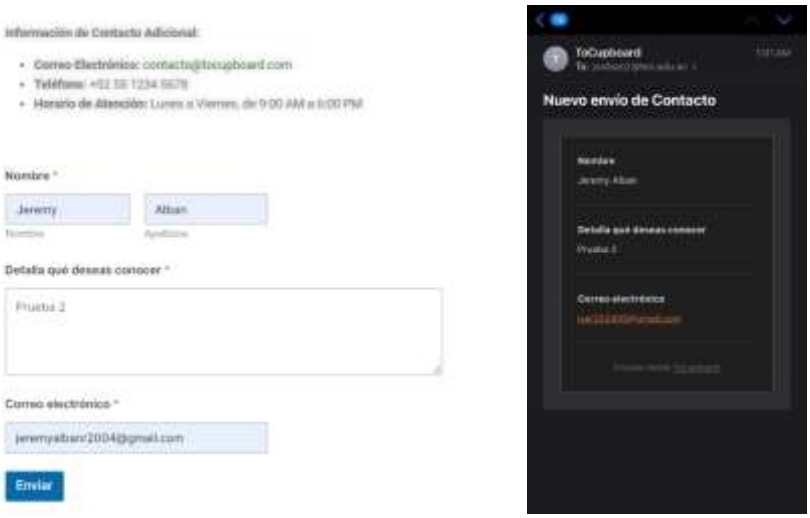
- **Informe de actividades del Correo:**



- **Seguridad**: La API de Gmail utiliza el protocolo **OAuth 2.0** para la autenticación y autorización. Esto asegura que las credenciales del usuario no se compartan directamente con el sitio web, sino que se utiliza un **token de acceso temporal**. Además, los permisos se limitan al envío de correos electrónicos, y los tokens tienen una vida útil limitada, lo que mitiga el riesgo de uso indebido.



- Ejemplo del correo desde la página **CONTACTO:**

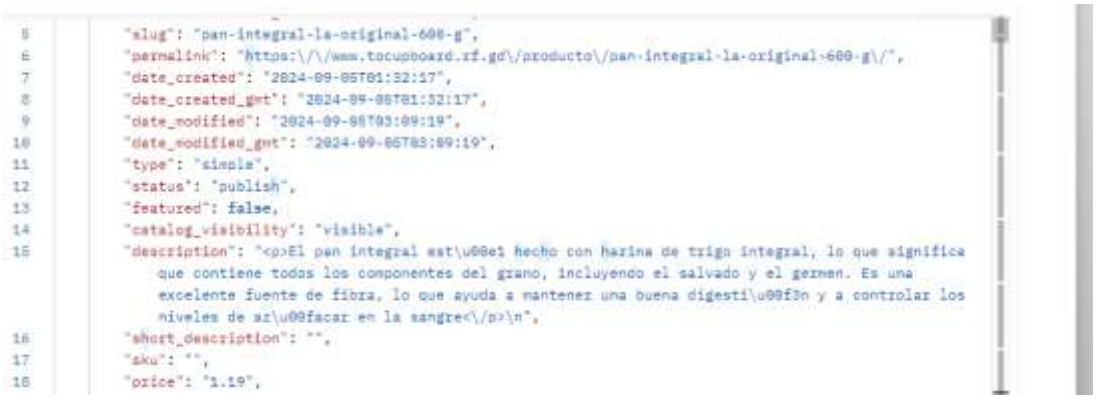


2. WooCommerce API (REST API)

- **Función**: La **REST API de WooCommerce** facilita la integración de datos dinámicos en el sitio web, permitiendo la obtención, creación y actualización de productos, pedidos y clientes en el backend. Esto es esencial para la funcionalidad de la tienda en línea, ya que permite gestionar inventarios y procesar pedidos en tiempo real.

- Extracto del JSON proporcionado por la API:

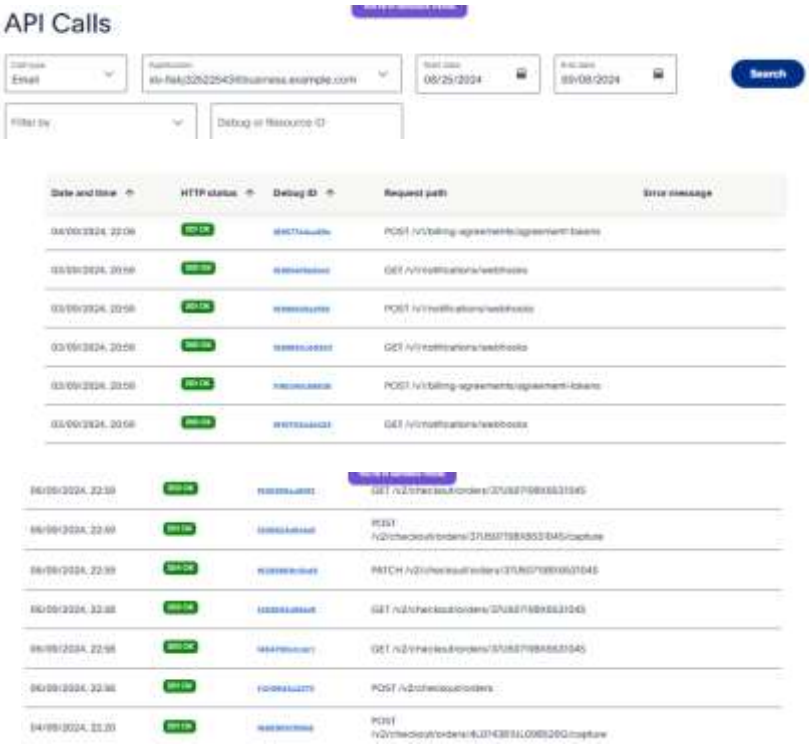
Extracto del JSON estilizado



- **Seguridad**: La integración de la REST API está asegurada mediante autenticación basada en claves de consumidor y secreto de consumidor, que son generadas en el panel de WooCommerce. Estas claves se utilizan para firmar las solicitudes y asegurar que solo usuarios autorizados puedan acceder o modificar los datos. Además, las comunicaciones se realizan a través de HTTPS, lo que encripta los datos durante la transmisión.

3. PayPal API

- **Función**: La **API de PayPal** es utilizada para simular el proceso de pagos en el sitio web. Los usuarios pueden agregar productos al carrito y finalizar la compra mediante una pasarela de pagos simulada en el entorno de pruebas de PayPal (Sandbox). Esto garantiza que el flujo de pago esté correctamente implementado y testeado antes de su puesta en producción.

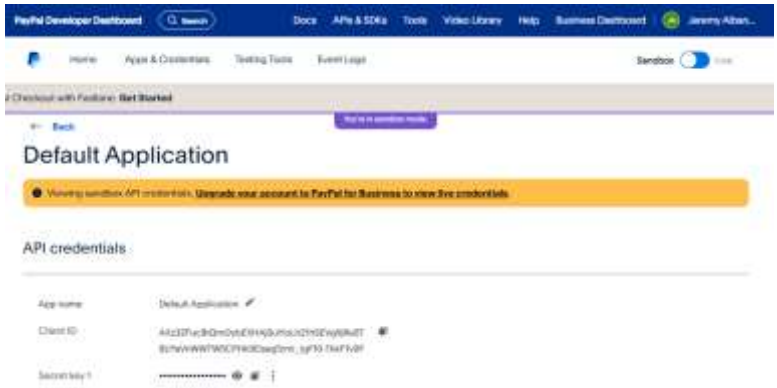


- Evidencia de la consulta de la **API:**
  - **Orden 1:** 1N807859HY4588205

  - **Orden 2:** 4L074381UL098520G

- **Seguridad**: La API de PayPal también implementa **OAuth 2.0** para la autenticación. Cada vez que se realiza una transacción, se genera un **token temporal** que valida y autentica el proceso de pago sin exponer las credenciales del usuario. Además, la tokenización de los datos de pago asegura que la información sensible no se almacene en el sitio web, cumpliendo con las mejores prácticas de seguridad.
    - **Desde Wordpress**

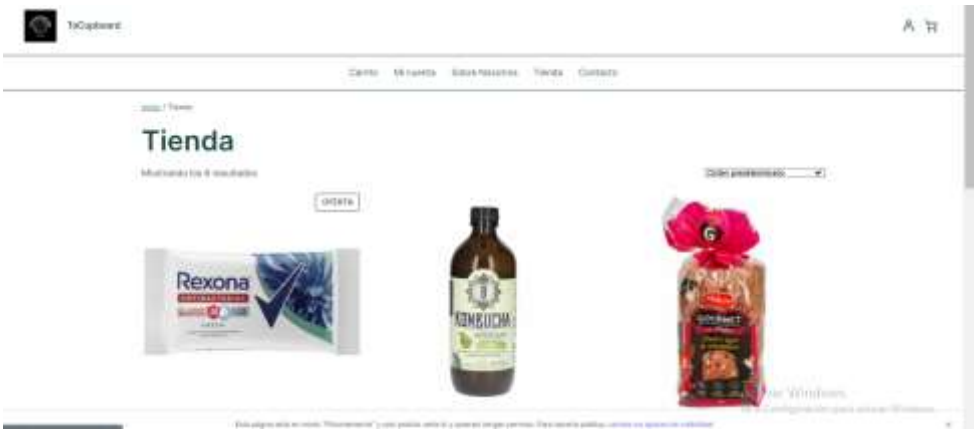
    - **Desde PayPal**



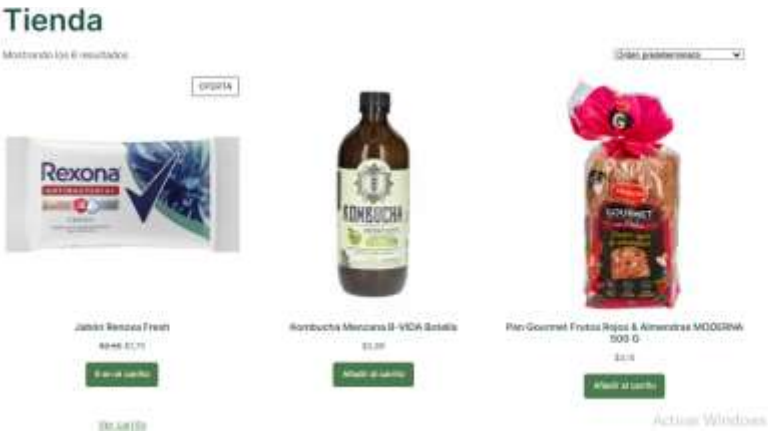
Descripción del Proceso de Simulación de la Pasarela de Pagos

El proceso de simulación de la pasarela de pagos en el sitio de ToCupBoard sigue los siguientes pasos:

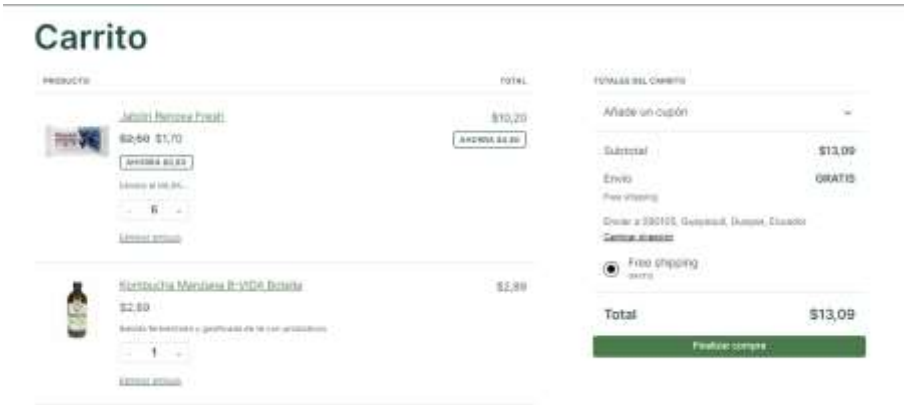
1. **Ir a la tienda de la app**: El usuario navega a la página "Tienda" donde se muestran los productos disponibles con sus detalles.



2. **Seleccionar productos**: El usuario añade los productos deseados al carrito de compras desde la página de la tienda.

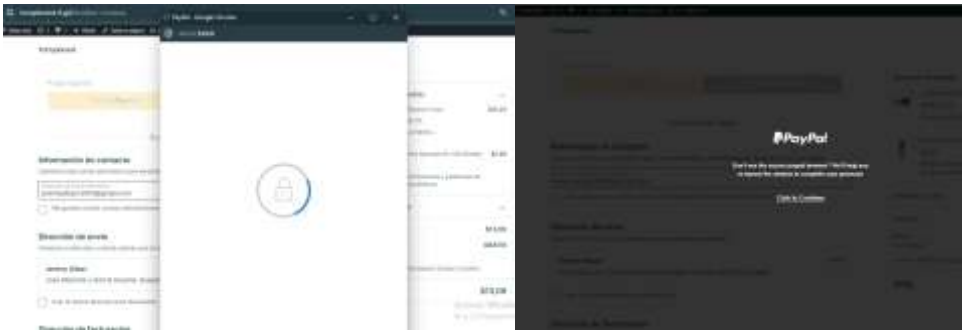


3. **Ver carrito**: El usuario revisa los productos seleccionados en la página "Carrito", donde puede verificar cantidades, precios y detalles de los artículos.



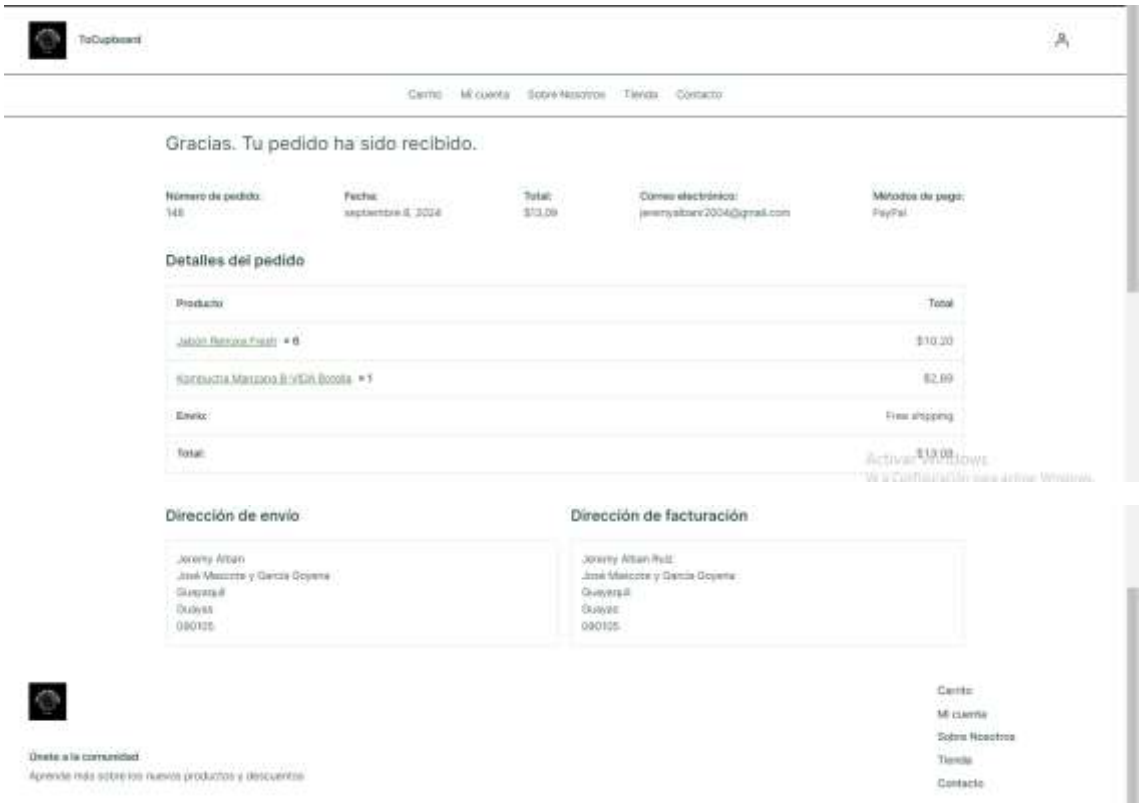
4. **Seleccionar "Finalizar compra"**: Una vez revisado el carrito, el usuario hace clic en el botón "Finalizar compra", donde se muestran los detalles finales de la orden.
5. **Click en el botón de pago PayPal**: En la página de finalización de compra, el usuario selecciona la opción de pagar con PayPal y hace clic en el botón correspondiente.

6. **Apertura de ventana de PayPal**: Se abre una ventana emergente de PayPal para la seguridad y autenticación del usuario, donde este debe ingresar sus credenciales o los datos necesarios para completar la transacción.



7. **Validación por PayPal**: PayPal valida la transacción de manera segura y redirige al usuario de vuelta al sitio web una vez finalizado el proceso de pago.

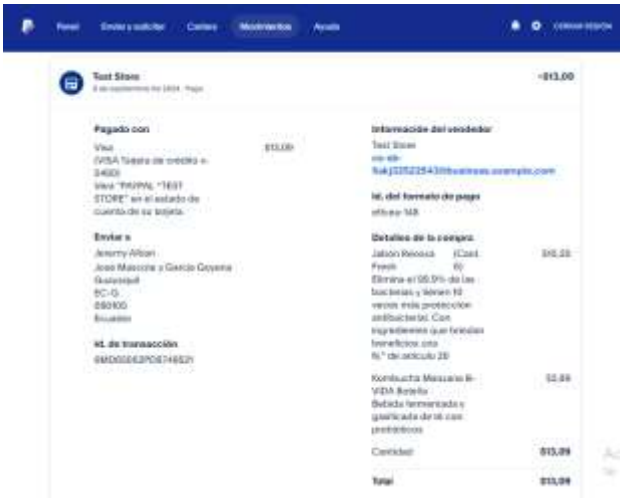
8. **Confirmación de la orden**: La página web muestra un mensaje de confirmación que detalla la orden realizada, con información sobre los productos adquiridos y el monto pagado.



9. **Envío de correo de confirmación**: El sistema automáticamente envía un correo electrónico al cliente, confirmando la orden y proporcionando los detalles de la transacción.

Correo al Administrador / Correo al Cliente / Datos de la Orden

- Dato de la Orden **Paypal:**


Panel
Enviar o solicitar
Carteira
Movimientos
Ayuda
Test Store
-$13.00
Pagado con
Visa
$13.00
Enviar a
Información del vendedor
Test Store
Id. del formato de pago
Detalles de la compra
Id. de transacción

Explicación Detallada De La Implementación Del Modelo Devsecops

DevSecOps en el Desarrollo de ToCupBoard En el desarrollo del sitio web de ToCupBoard, se ha integrado la seguridad de manera continua siguiendo el enfoque DevSecOps. Esto significa que la seguridad se ha considerado en cada fase del desarrollo y operación. Se han utilizado herramientas y plugins de seguridad como Wordfence, Sucuri, y All In One WP Security para proteger el sitio desde el inicio hasta su lanzamiento. Además, se han empleado herramientas externas como SSL Labs, Sucuri SiteCheck y Pentest-Tools para evaluar y reforzar la seguridad.

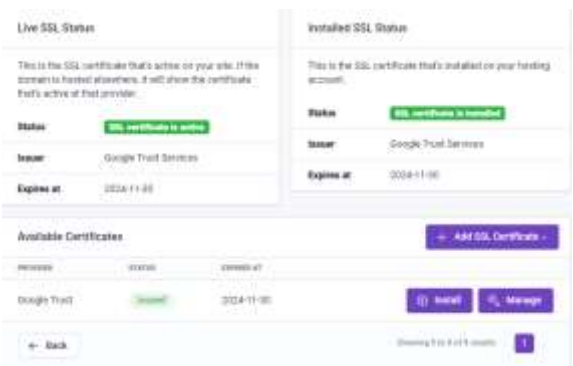
CI/CD: Integración y Entrega Continua El enfoque de CI/CD (Integración Continua y Entrega Continua) ha sido clave en el proyecto, integrando las herramientas de seguridad y automatización directamente en el flujo de desarrollo y despliegue del sitio.

1. **Integración Continua (CI)**: Cada cambio en el sitio se verifica automáticamente con herramientas como Wordfence y All In One WP Security, y se realiza un escaneo con Pentest-Tools para identificar vulnerabilidades antes de que los cambios se integren en el entorno de producción.
2. **Entrega Continua (CD)**: Una vez que las configuraciones pasan las pruebas de seguridad, se despliegan automáticamente. Plugins como Really Simple SSL y WP Encryption aseguran que el sitio esté siempre protegido con certificados SSL actualizados, mientras que Backup Bolt garantiza copias de seguridad automáticas para restaurar el sitio si es necesario.

Herramientas y Plugins Implementados en el CI/CD y DevSecOps

Certificado SSL (HTTPS)

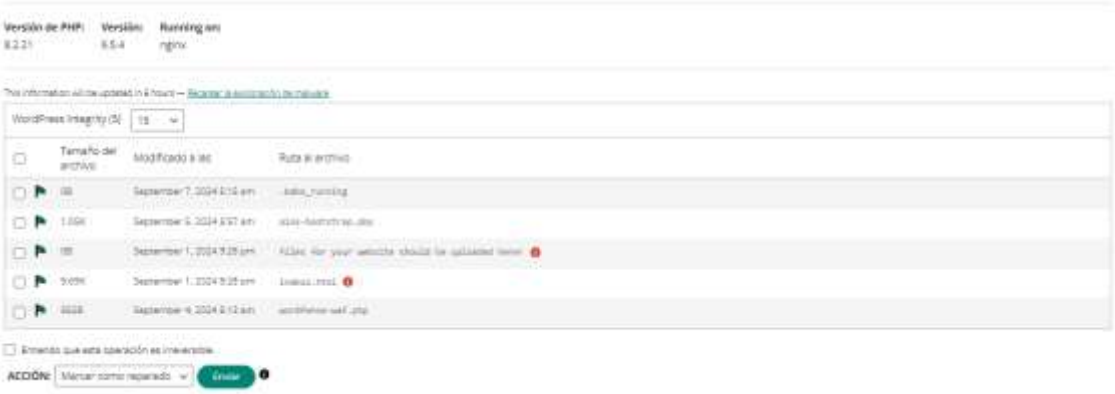
- **Implementación**: Se configuró un certificado SSL para cifrar todas las comunicaciones entre el servidor y los usuarios. Esto garantiza la protección de datos sensibles, como información de pago y detalles de contacto, y refuerza la confianza del usuario al mostrar un candado verde en la barra de direcciones.
- El certificado SSL instalado en el servidor es proporcionado por Google Trust Services y está activo hasta el 30 de noviembre de 2024.

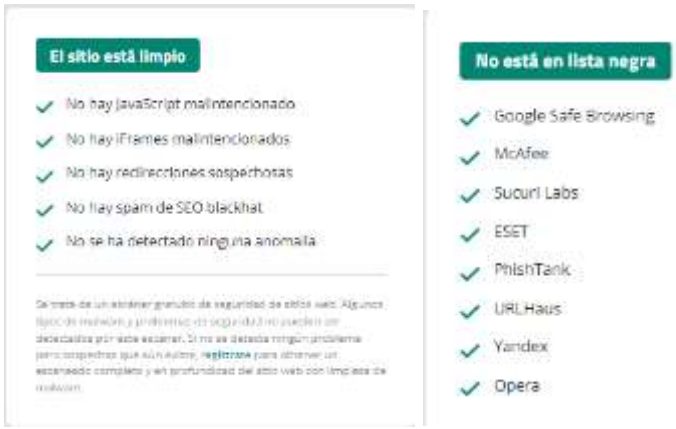


Plugins de Seguridad

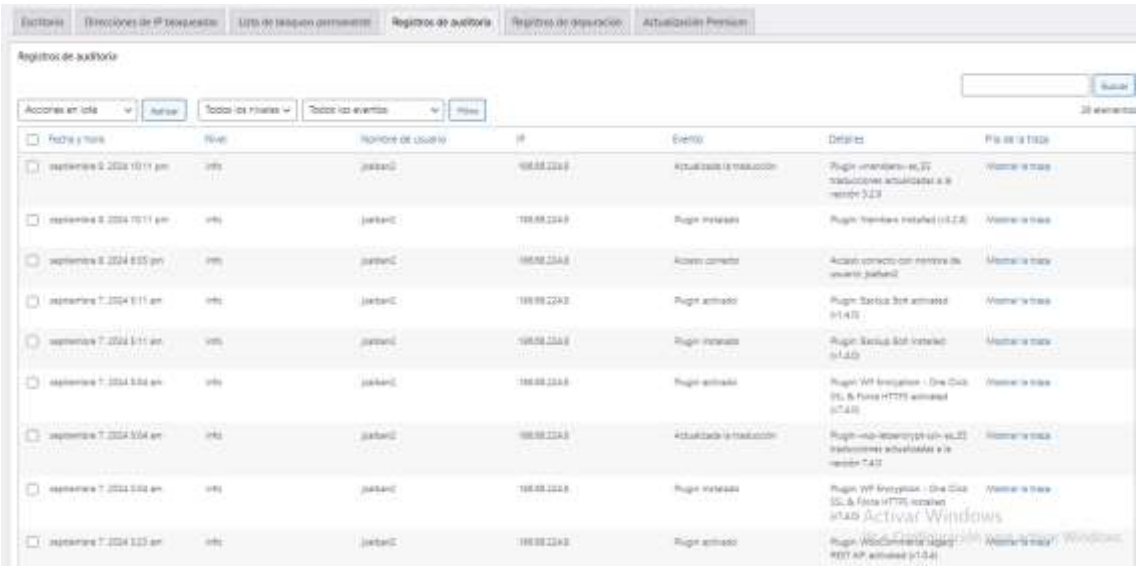
- **Wordfence Security**
    - **Implementación**: Se instaló Wordfence para fortalecer la seguridad del sitio. Actualmente, protege el sitio contra intentos de hackeo, malware y ataques de fuerza bruta, proporcionando monitoreo y alertas en tiempo real.

- **Sucuri Security**
    - **Implementación**: Se añadió Sucuri para una protección integral. Está asegurando el sitio con monitoreo continuo, mitigación de ataques DDoS y protección contra malware.





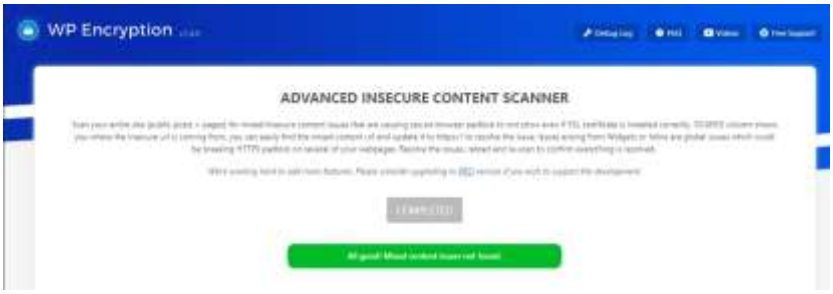
- **All In One WP Security & Firewall**
    - **Implementación**: Se integró este plugin para mejorar la seguridad general del sitio. Refuerza la seguridad del inicio de sesión, aplica un firewall básico y realiza escaneos para detectar vulnerabilidades.



- **Backup Bolt**
    - **Implementación**: Se configuró para realizar copias de seguridad automáticas. Asegura que el sitio tenga copias de seguridad programadas y pueda restaurarse rápidamente en caso de problemas.

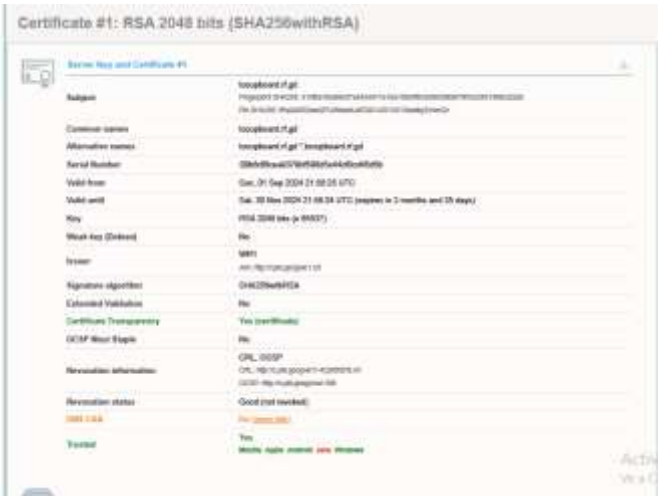
- **Really Simple SSL**
    - **Implementación**: Se habilitó para gestionar la configuración de HTTPS. Redirige automáticamente el tráfico HTTP a HTTPS, asegurando que todo el sitio esté cifrado.

- **WP Encryption**
    - **Implementación**: Se instaló para manejar certificados SSL gratuitos. Automatiza la renovación de certificados SSL, garantizando la seguridad continua del sitio. Además para escanear si existe contenido mixto e inseguro.

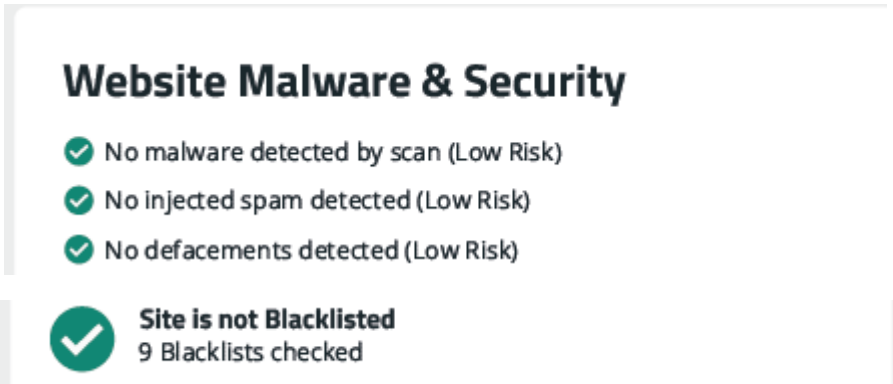


Herramientas Externas

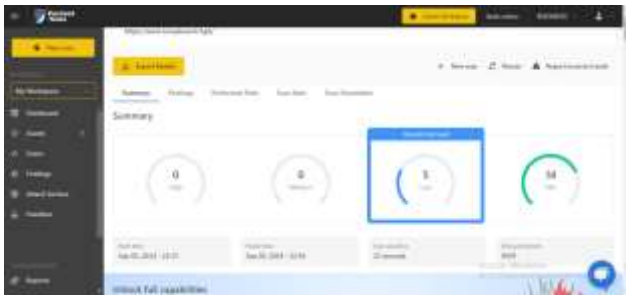
- **SSL Labs**
    - **Implementación**: Se utilizó para evaluar el certificado SSL. Validó la robustez de la implementación de HTTPS, asegurando que el cifrado sea seguro y que el sitio esté correctamente configurado.

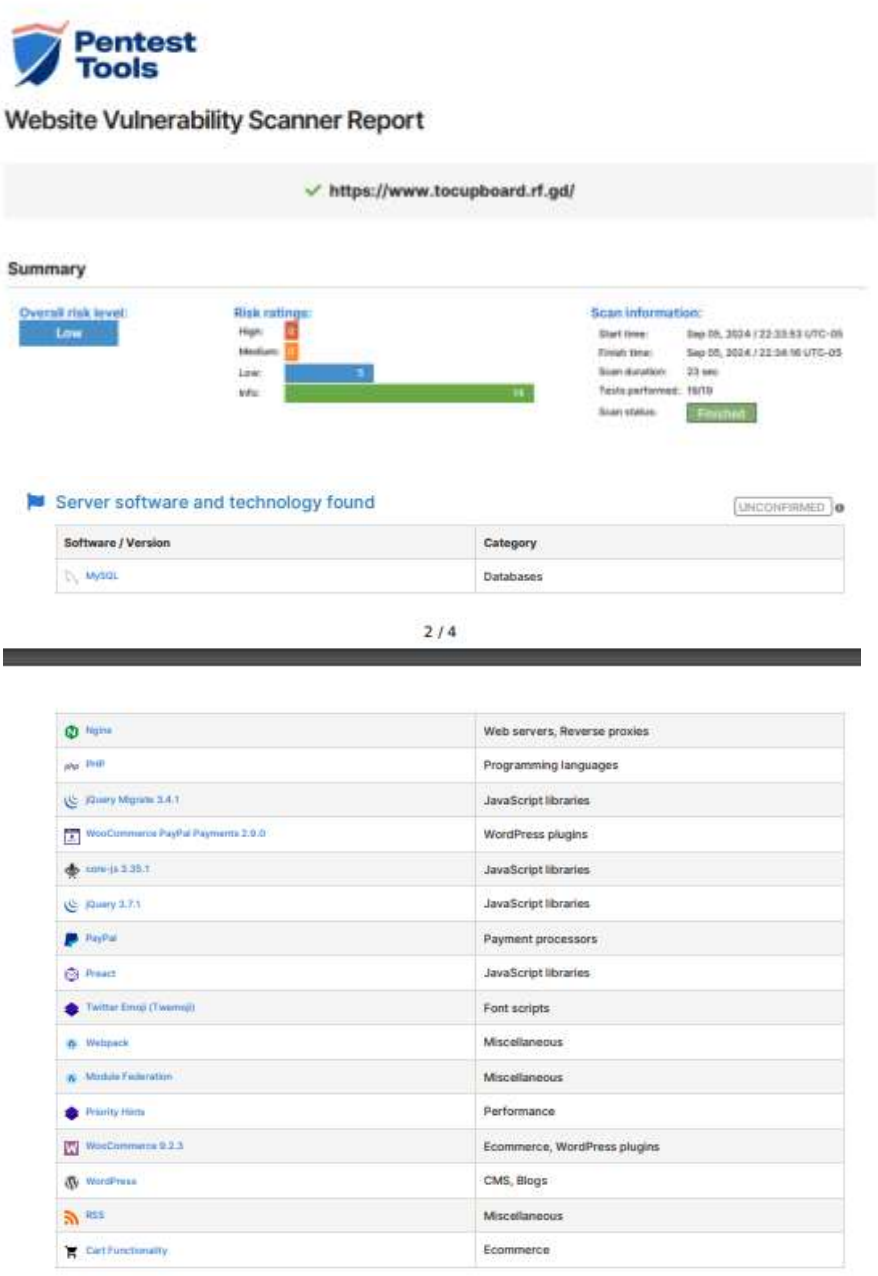


- **Sucuri SiteCheck**
    - **Implementación**: Se empleó para escanear el sitio en busca de vulnerabilidades. Detecta malware y verifica la seguridad del sitio, ayudando a mantenerlo libre de amenazas.



- **Pentest-Tools**
    - **Implementación**: Se aplicó para realizar pruebas de penetración. Identifica y corrige vulnerabilidades críticas, fortaleciendo la seguridad general del sitio web.





Pentest Tools

Website Vulnerability Scanner Report

✓ https://www.tocupboard.rf.gd/

Summary

Overall risk level: Low

Risk ratings: High: 0 Medium: 0 Low: 3 Info: 14

Scan information: Start time: Sep 05, 2024 / 22:33:53 UTC-05 Finish time: Sep 05, 2024 / 22:34:16 UTC-05 Scan duration: 23 sec Tests performed: 19/19 Scan status: Finished

Server software and technology found — UNCONFIRMED

Software / Version	Category
MySQL	Databases

2 / 4

Nginx	Web servers, Reverse proxies
PHP	Programming languages
jQuery Migrate 3.4.1	JavaScript libraries
WooCommerce PayPal Payments 2.9.0	WordPress plugins
core-js 3.35.1	JavaScript libraries
jQuery 3.7.1	JavaScript libraries
PayPal	Payment processors
Preact	JavaScript libraries
Twitter Emoji (Twemoji)	Font scripts
Webpack	Miscellaneous
Module Federation	Miscellaneous
Priority Hints	Performance
WooCommerce 9.2.3	Ecommerce, WordPress plugins
WordPress	CMS, Blogs
RSS	Miscellaneous
Cart Functionality	Ecommerce

Impacto en el Proyecto ToCupBoard

- **Seguridad de Transacciones**: El SSL y los plugins de seguridad protegen los datos de pago y las transacciones del carrito de compras.
- **Protección de Datos Personales**: Los plugins de seguridad y las herramientas externas garantizan la integridad y confidencialidad de la información personal recolectada a través del formulario y otros puntos de entrada.
- **Confianza del Usuario**: La implementación de HTTPS y la gestión de roles con el plugin Members refuerzan la confianza del usuario en el sitio e-commerce.
- **Recuperación ante Incidentes**: Backup Bolt asegura la disponibilidad de datos críticos y la capacidad de recuperación ante fallos o ataques.