



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:	2
Acceso al Sitio Web	2
Navegación por el Sitio Web.....	2
Plugins utilizados:	6
Descripción de las llamadas a la API implementadas	7
1. Gmail API	7
2. WooCommerce API (REST API).....	9
3. PayPal API	10
Descripción del Proceso de Simulación de la Pasarela de Pagos	13
Explicación Detallada De La Implementación Del Modelo Devsecops	17
Herramientas y Plugins Implementados en el CI/CD y DevSecOps	17
Herramientas Externas	21
Impacto en el Proyecto ToCupBoard	23

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

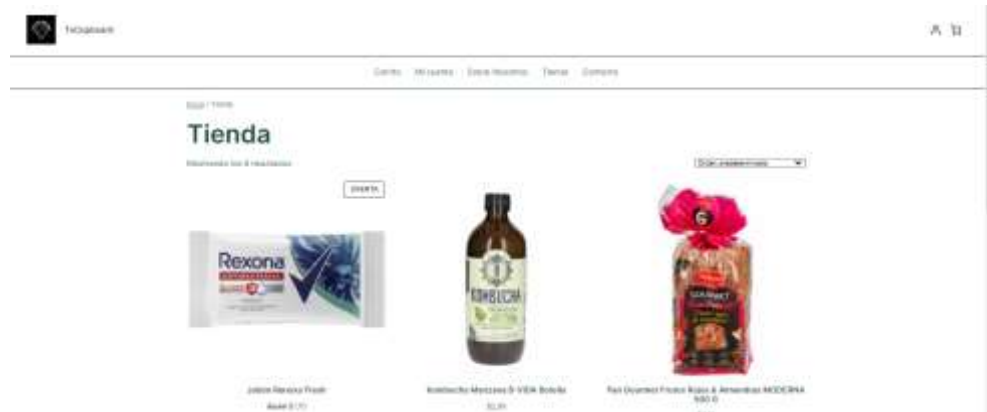


- Web

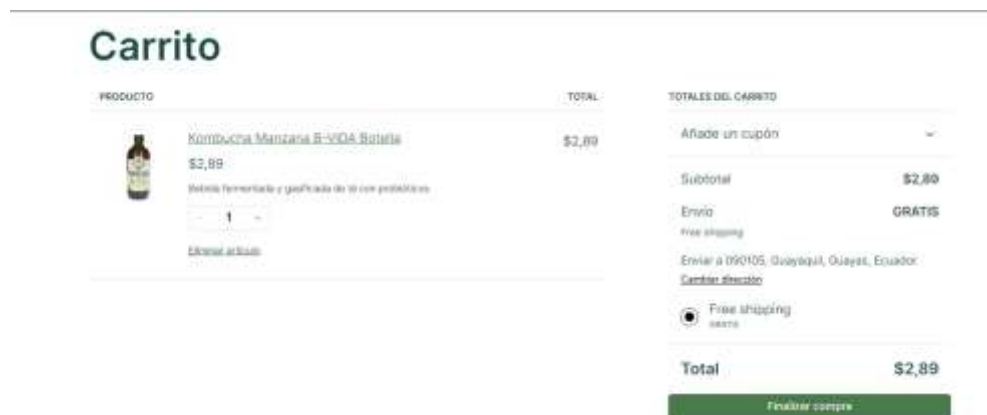




- **Tienda:** Muestra todos los productos disponibles en la tienda, con detalles como precio, descripción y disponibilidad.



- **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.

Pago rápido

Pay with **PayPal**

Debit or Credit Card

O continúa más abajo

Información de contacto

Usaremos este correo electrónico para enviarte detalles y actualizaciones relacionadas con tu pedido.

Dirección de correo electrónico

jeremialbanr2004@gmail.com

☐ Me gustaría recibir correos electrónicos exclusivos con descuentos e información de productos

Dirección de envío

Introduce la dirección a dónde quieras que se entregue tu pedido.

Resumen del pedido



1 Kombucha Manzana B-VIDA Botella

\$2,89

Bebida fermentada y gasificada de té con probióticos

Añade un cupón

Subtotal

\$2,89

Envío

GRATIS

Free shipping

Enviar a 090105, Guayaquil, Guayas, Ecuador

Total

\$2,89



PayPal Checkout - Google Chrome

sanluis.paypal.com/checkout/now?_ga=2.150411111.150411111.150411111.150411111

\$2,89 USD

Forma de envío

Free shipping - \$0,00 USD

Enviar a Jeremiy Alban

Jose Mascote y Genes Goyena, EC090105 Guayaquil

Modificar

Pagar con

Visa

Abono ****4480 Preselec

\$2,89 USD

+ Agregar tarjeta de crédito

Guarde PayPal para pagos a ToCupboard. Si su saldo o forma de pago seleccionada no está disponible, PayPal puede utilizar otras formas de pago asociadas a su cuenta, de acuerdo con las Condiciones de Uso de PayPal. Puede cambiar sus preferencias de

Aceptar y pagar ahora

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

Sobre Nosotros



En **ToCupboard**, creemos en la importancia de apoyar a las pequeñas empresas y facilitar el acceso a productos esenciales para todos. Fundada en 2020, durante los desafíos de la pandemia por Covid-19, ToCupboard nació con la misión de conectar a las personas con los productos de primera necesidad desde la comodidad y seguridad de sus hogares.

Nuestra Misión

Facilitar el acceso a productos esenciales y apoyar el crecimiento de pequeños comerciantes mediante una plataforma segura, confiable y fácil de usar.

Nuestra Visión

Convertirnos en el aliado preferido de los hogares y pequeños negocios, proporcionando soluciones eficientes y seguras para las compras en línea.

Nuestros Valores

- Compromiso con la seguridad.
- Transparencia en nuestras operaciones.
- Innovación constante para mejorar la experiencia del usuario.
- Apoyo al comercio local.

- **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.


Cerrar sesión)' and a description: 'Desde el escritorio de tu cuenta puedes ver tus [pedidos recientes](#), gestionar tus [direcciones de envío y facturación](#) y editar tu [contraseña](#) o los [datos de tu cuenta](#).'"/>

- **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.

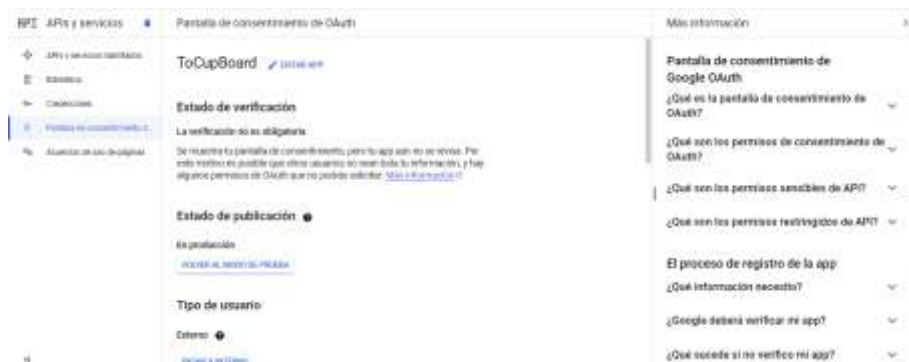
Descripción de las llamadas a la API implementadas

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:**



- Google / Gmail**

El servicio de correo de Gmail funciona bien para sitios que envíen un bajo número de correos electrónicos. Sin embargo, la API de Gmail tiene limitaciones y un número de restricciones adicionales que pueden provocar problemas durante la configuración.

Para evitar problemas de volumen de correo electrónico o si le das cuenta de que tu alojamiento web no es compatible con las restricciones de la API de Gmail, recomendamos considerar usar otro servicio de correo.

Si prefieres continuar con cualquier cuenta de Gmail o Google Workspace a través de la API de Google, puedes enviar correos de WordPress desde tu computadora personal. Al hacer un uso de Gmail, y es más seguro que conectarse a Gmail a través de protocolos SMTP. Ambos dispositivos de correo electrónico son auto-dijo, que simplemente le pide sus credenciales su cuenta de Google para utilizar nuestra aplicación y se envía el todo por sí mismo. Conectarse manualmente, lo que implica varios pasos que son más técnicas que otras opciones de correo, pero que hemos creado una guía a través del proceso:

Para empezar, ve nuestra [Guía paso a paso de Gmail](#).

Configuración en un solo clic ☐ INACTIVO NEW

Pruebe una manera rápida y fácil de conectar con Google que no requiere de crear su propio app.

ID de cliente

Clave secreta de cliente

URL de redireccionamiento autorizados

Por favor, copie esta URL en el campo «URLs de redireccionamiento autorizadas» de su aplicación web Google.

Autorización

Si quieres usar una dirección diferente del correo electrónico del remitente, puedes configurar un alias de correo electrónico de Google. [Sigue estas instrucciones](#) y después, selecciona el correo electrónico del remitente en la parte superior de esta página.

- [illegible]

- **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.

Límites de frecuencia de OAuth

La frecuencia de otorgamiento de token ?

Las frecuencias de otorgamiento de token limitan la rapidez de tu aplicación para obtener nuevos usuarios.

El límite de frecuencia de otorgamiento de tokens diarios actual es de 10,000 otorgamientos por día. La frecuencia de otorgamiento de tokens se restablece cada día. [Aumentar el límite de tokens diarios](#)

5 minutos ☒ 1 día

10.00

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

Información de Contacto Adicional:

- Correo Electrónico:
- Teléfono:
- Horario de Atención: Lunes a Viernes, de 9:00 AM a 6:00 PM

Nombre *

Nombre Apellido

Detalla qué debes conocer *

Correo electrónico *

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

```

5      "slug": "pan-integral-la-original-600-g",
6      "permalink": "https://www.tocupboard.rf.gd/\producto/pan-integral-la-original-600-g/\",
7      "date_created": "2024-09-05T01:32:17",
8      "date_created_gmt": "2024-09-05T01:32:17",
9      "date_modified": "2024-09-05T03:09:19",
10     "date_modified_gmt": "2024-09-05T03:09:19",
11     "type": "simple",
12     "status": "publish",
13     "featured": false,
14     "catalog_visibility": "visible",
15     "description": "<p>El pan integral est\u00e1 hecho con harina de trigo integral, lo que significa  

    que contiene todos los componentes del grano, incluyendo el salvado y el germen. Es una  

    excelente fuente de fibra, lo que ayuda a mantener una buena digesti\u00f3n y a controlar los  

    niveles de az\u00facar en la sangre.</p>\n",
16     "short_description": "",
17     "sku": "",
18     "price": "1.19",

```

- **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.

Clave de la API generada correctamente. Asegúrate de copiar tus nuevas claves ahora ya que la clave secreta se ocultará una vez abandones esta página.

- Las claves API sirven el acceso a información potencialmente sensible. Compartélas solo con organizaciones en las que confíes.
- Límitate a una clave por cliente, así será más fácil revocar el acceso en el futuro a un solo cliente, sin causar problemas a los demás.

Clave del cliente

Copiar

Clave secreta de cliente

Copiar

Revisar

Código QR



Revocar clave

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.

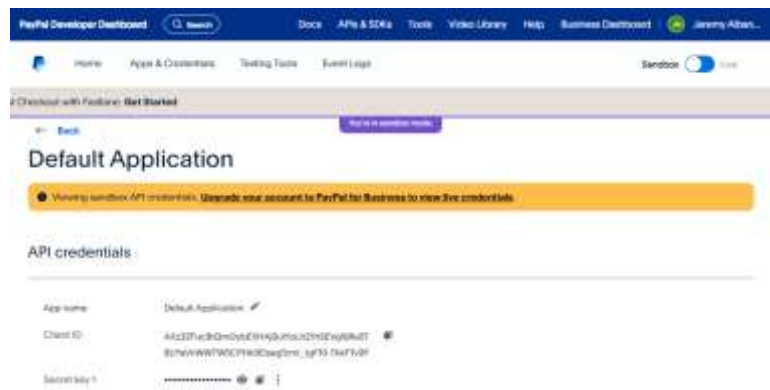


- **Seguridad:** La API de PayPal también implementa **OAuth 2.0** para la autenticación. Cada vez que se realiza una transacción, se genera un **token temporal** que valida y autentica el proceso de pago sin exponer las credenciales del usuario. Además, la tokenización de los datos de pago asegura que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

- **Desde Wordpress**



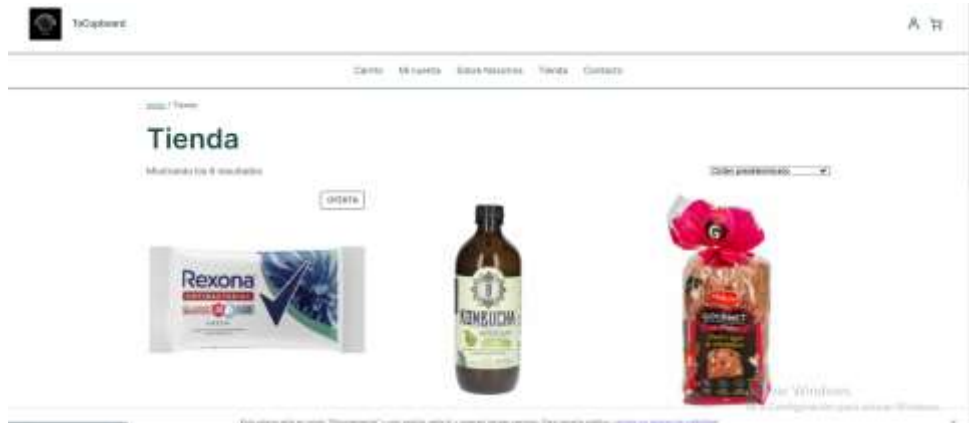
- **Desde PayPal**



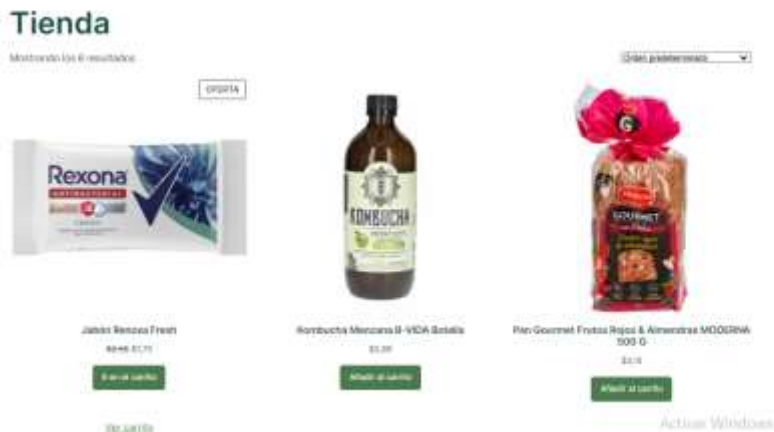
Descripción del Proceso de Simulación de la Pasarela de Pagos

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

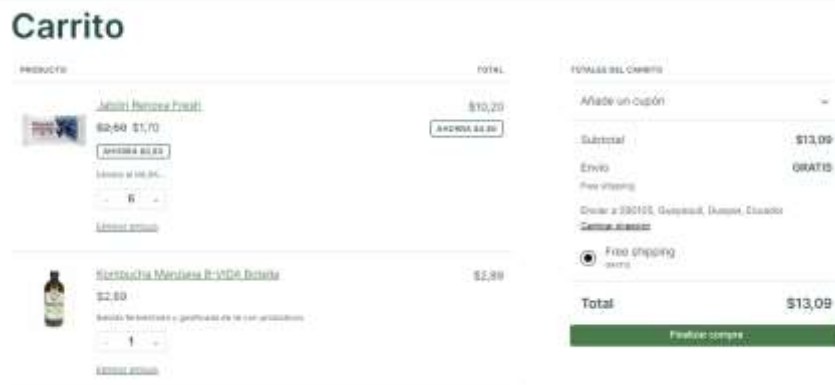
1. **Ir a la tienda de la app:** El usuario navega a la página "Tienda" donde se muestran los productos disponibles con sus detalles.



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

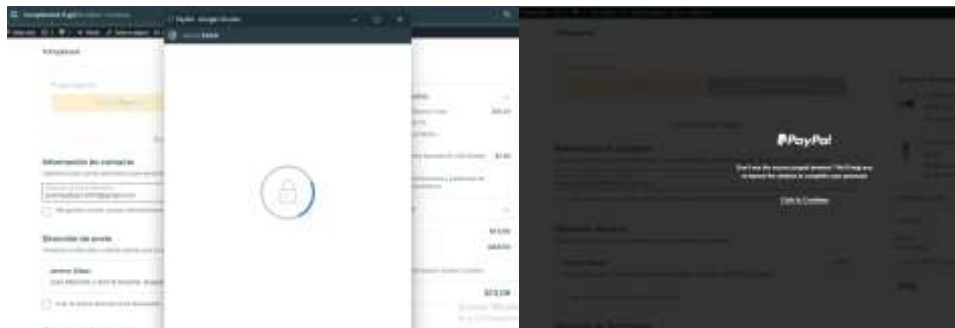


3. **Ver carrito:** El usuario revisa los productos seleccionados en la página "Carrito", donde puede verificar cantidades, precios y detalles de los artículos.



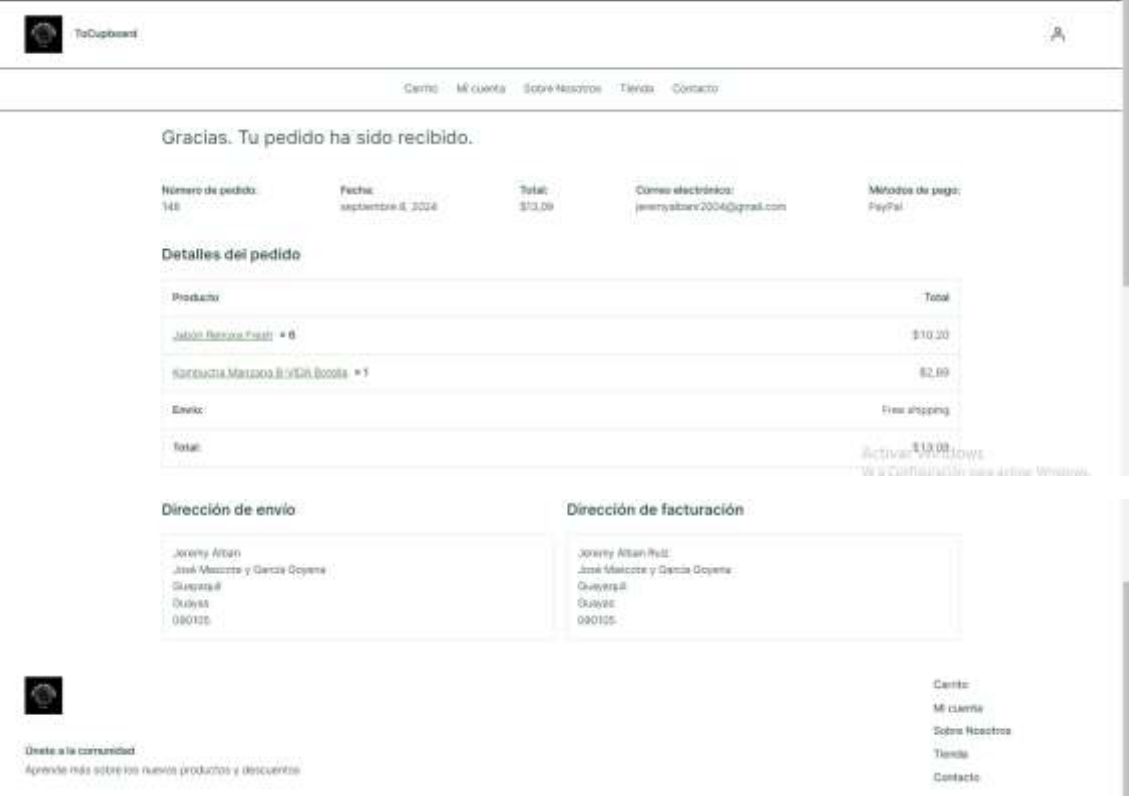
4. **Seleccionar "Finalizar compra":** Una vez revisado el carrito, el usuario hace clic en el botón "Finalizar compra", donde se muestran los detalles finales de la orden.
5. **Click en el botón de pago PayPal:** En la página de finalización de compra, el usuario selecciona la opción de pagar con PayPal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



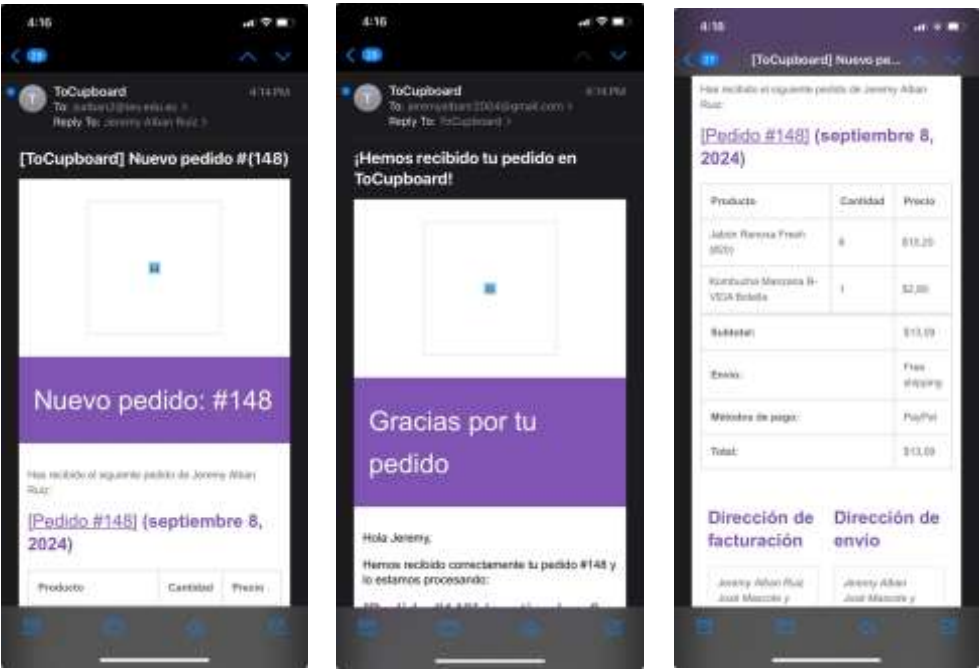
7. **Validación por PayPal:** PayPal valida la transacción de manera segura y redirige al usuario de vuelta al sitio web una vez finalizado el proceso de pago.

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:**

<div><div></div><div>Panel</div></div> <div><div>Enviar y actualizar</div><div>Contar</div><div>Modificaciones</div><div>Ayuda</div></div> <div><div></div><div>0 items</div><div>0 items</div></div>		
<div><div><div></div><div>Test Store</div><div>8 de septiembre de 2024</div><div>Pago</div></div><div>- \$13.00</div></div>		
<div><div><div><div><div>Pagado con</div><div>Visa</div><div>(VISA Tarjeta de crédito n. 3456)</div><div>Visa "MIDPAY -1688 STORE" en el estado de cuenta de la tarjeta</div></div><div><div>\$13.00</div></div></div><div><div><div>Envío a</div><div>Jeremy Allen</div><div>Jose Masada y Gerardo Ojeda</div><div>Guatemala</div><div>SC-0</div><div>550100</div><div>Guatemala</div></div><div><div><div>Id. de transacción</div><div>94D05663D06746829</div></div></div></div><div><div><div>Información del vendedor</div><div>Test Store</div><div>no es</div><div>Subj123225430@business.example.com</div></div><div><div><div>Id. del formato de pago</div><div>ofine-123</div></div></div><div><div><div>Detalles de la compra</div><div>Jalisco Roscos (Cant. 1)</div><div>Elimina el 55.5% de las bacterias y retrasa 10 veces más protección antibacterial. Con repelente que brinda beneficios una 6." de ancho 28</div><div>\$10.25</div></div><div><div><div>Kondustra Masada B-VDA Borela</div><div>Debido fermentado y guarnido de té con probióticos</div><div>\$2.75</div></div><div><div><div>Costo del</div><div>\$13.00</div></div></div><div><div><div>Total</div><div>\$13.00</div></div></div></div></div></div></div></div>		

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.

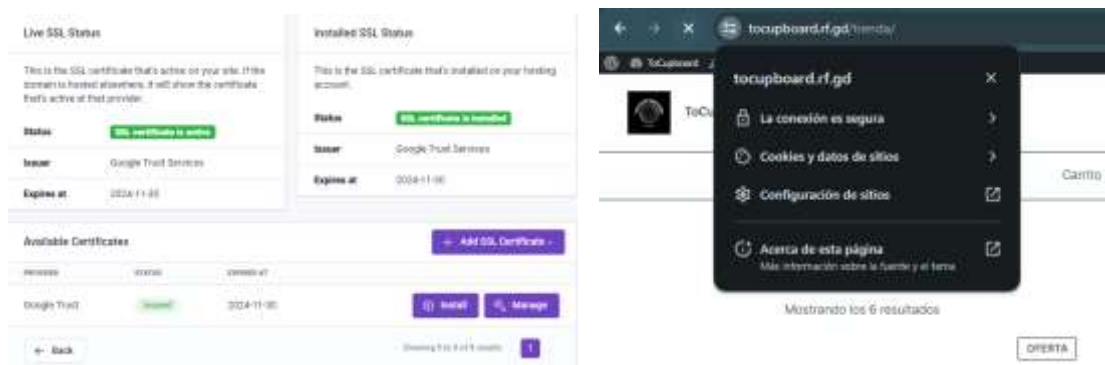
CI/CD: Integración y Entrega Continua El enfoque de CI/CD (Integración Continua y Entrega Continua) ha sido clave en el proyecto, integrando las herramientas de seguridad y automatización directamente en el flujo de desarrollo y despliegue del sitio.

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

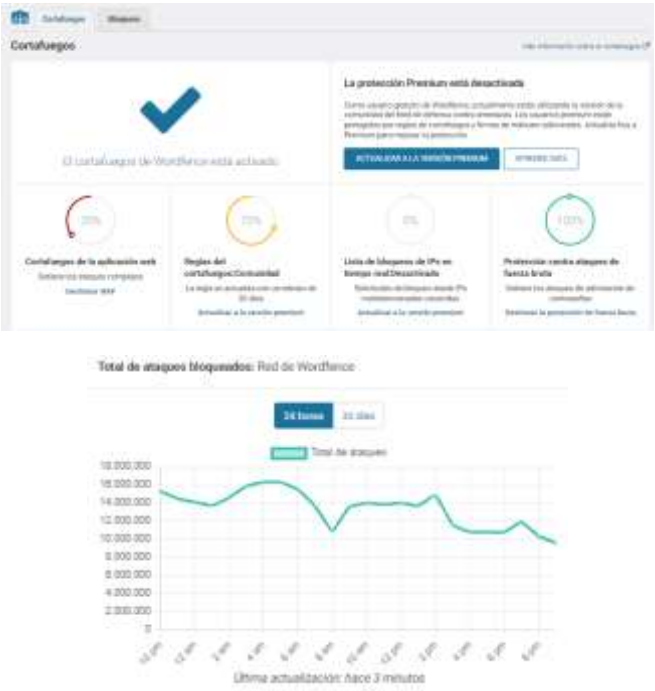
Certificado SSL (HTTPS)

- **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.

Versión de PHP:	Versión:	Running on:
8.2.11	6.5.4	nginx

This information will be updated in 6 hours — [View more details about this update](#)

WordPress Integrity (3)	Tamaño del archivo	Modificado a las	Ruta al archivo
<input type="checkbox"/>	100	September 7, 2024 2:15 am	wp-content/plugins/woocommerce
<input type="checkbox"/>	1.00K	September 5, 2024 5:57 am	wp-content/plugins/woocommerce
<input type="checkbox"/>	100	September 1, 2024 7:29 am	wp-content/plugins/woocommerce
<input type="checkbox"/>	5.00K	September 1, 2024 5:25 am	wp-content/plugins/woocommerce
<input type="checkbox"/>	100K	September 16, 2024 2:12 am	wp-content/plugins/woocommerce

☐ Enviar una notificación de integridad

Acción:



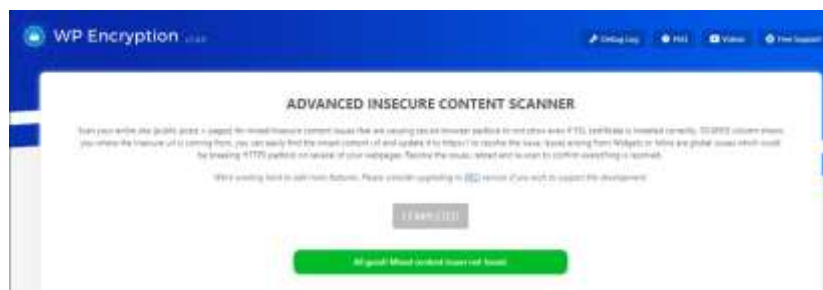
- **Really Simple SSL**

- **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**

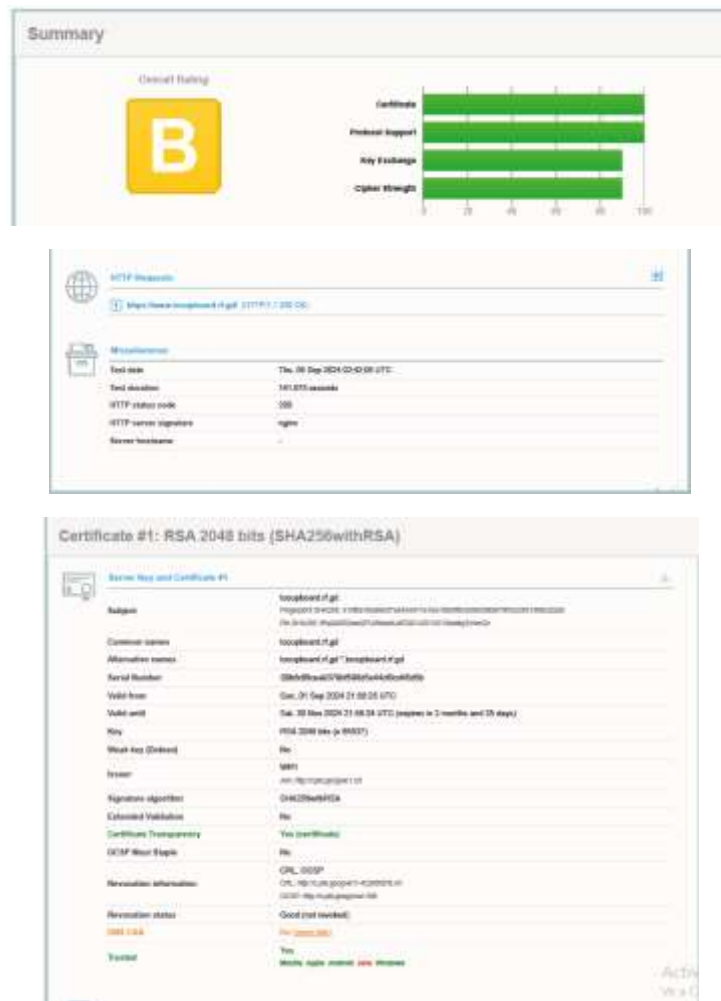
- **Implementación:** Se instaló para manejar certificados SSL gratuitos. Automatiza la renovación de certificados SSL, garantizando la seguridad continua del sitio. Además para escanear si existe contenido mixto e inseguro.



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.

Website Malware & Security

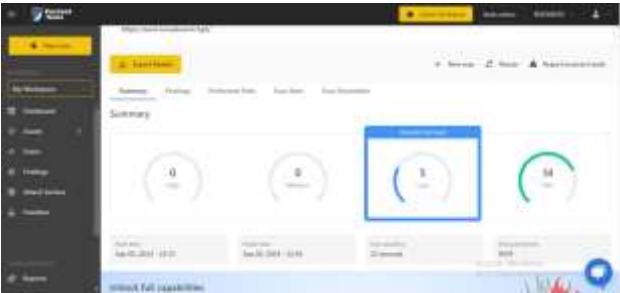
- ✓ No malware detected by scan (Low Risk)
- ✓ No injected spam detected (Low Risk)
- ✓ No defacements detected (Low Risk)

✓

Site is not Blacklisted
9 Blacklists checked

- **Pentest-Tools**

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



Website Vulnerability Scanner Report

✓ <https://www.tocupboard.rf.gd/>

Summary



Server software and technology found

UNCONFIRMED 0

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
Proact	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.