



Protocolos de seguridad con pentesting y criptografía

Nombre: Angel Orlando Zambrano Uriña

Nao ID: 3117

Fecha: 30/08/2024

Nombre de la trayectoria: Consultor de Cyberseguridad

Título del reto: Protocolos de seguridad con pentesting y criptografía

Sprint 2

Desarrolla

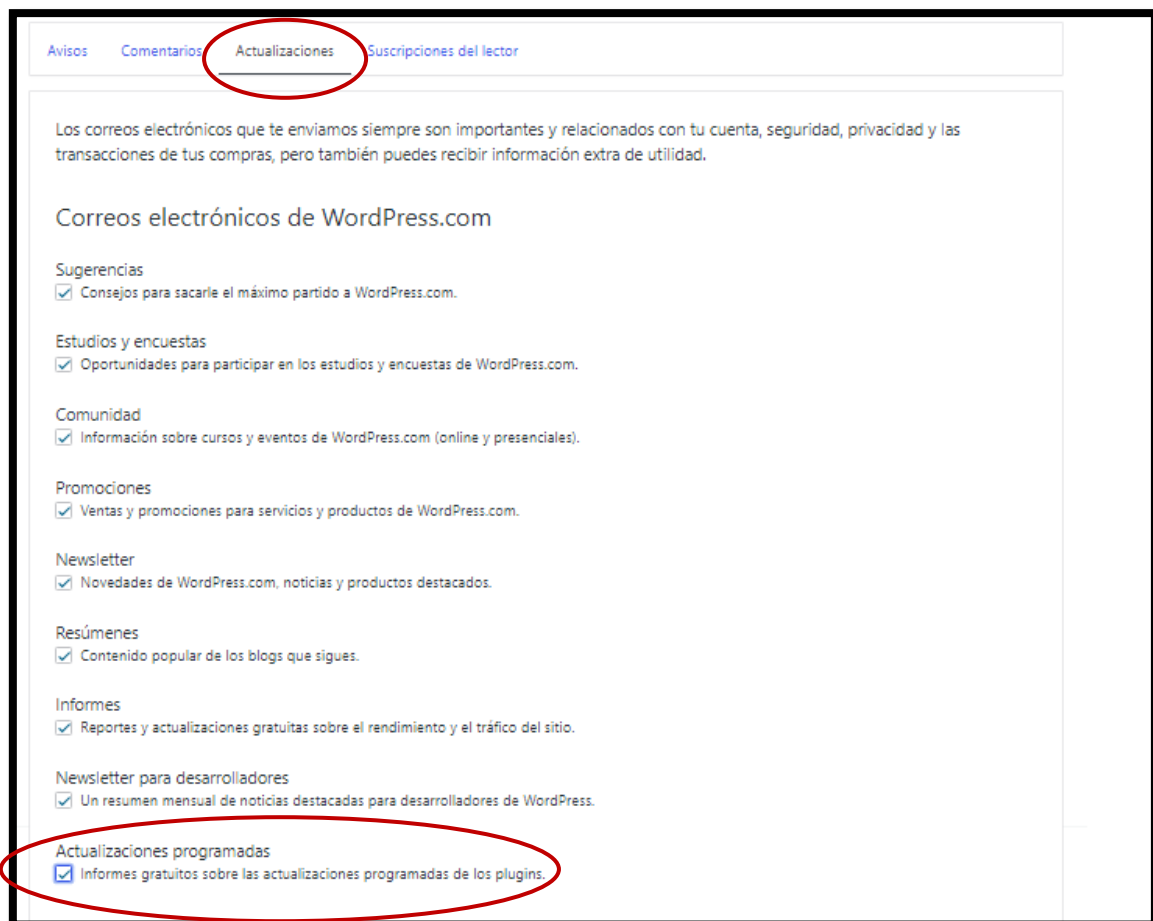
Sigue estas instrucciones para desarrollar el segundo avance de tu proyecto.

1 . Desarrolla una página web con WordPress, que incluye llamadas a una API y una simulación de una [pasarela de pagos](#) , aplicando el modelo DevSecOps.

- Características de la página web:
- **Página web en WordPress :**
- Tema y Diseño: Utiliza un tema apropiado para la empresa ToCupboard, con un diseño profesional y responsive.
- Contenido Básico: Incluye páginas como Inicio, Sobre Nosotros, Productos/Servicios, Contacto.



- Seguridad en el Desarrollo: Asegúrese de que el sitio web cumpla con las mejores prácticas de seguridad desde el diseño, incluyendo:
- Actualización de WordPress y sus complementos.



Avisos Comentarios **Actualizaciones** Suscripciones del lector

Los correos electrónicos que te enviamos siempre son importantes y relacionados con tu cuenta, seguridad, privacidad y las transacciones de tus compras, pero también puedes recibir información extra de utilidad.

Correos electrónicos de WordPress.com

Sugerencias
☒ Consejos para sacarle el máximo partido a WordPress.com.

Estudios y encuestas
☒ Oportunidades para participar en los estudios y encuestas de WordPress.com.

Comunidad
☒ Información sobre cursos y eventos de WordPress.com (online y presenciales).

Promociones
☒ Ventas y promociones para servicios y productos de WordPress.com.

Newsletter
☒ Novedades de WordPress.com, noticias y productos destacados.

Resúmenes
☒ Contenido popular de los blogs que sigues.

Informes
☒ Reportes y actualizaciones gratuitas sobre el rendimiento y el tráfico del sitio.

Newsletter para desarrolladores
☒ Un resumen mensual de noticias destacadas para desarrolladores de WordPress.

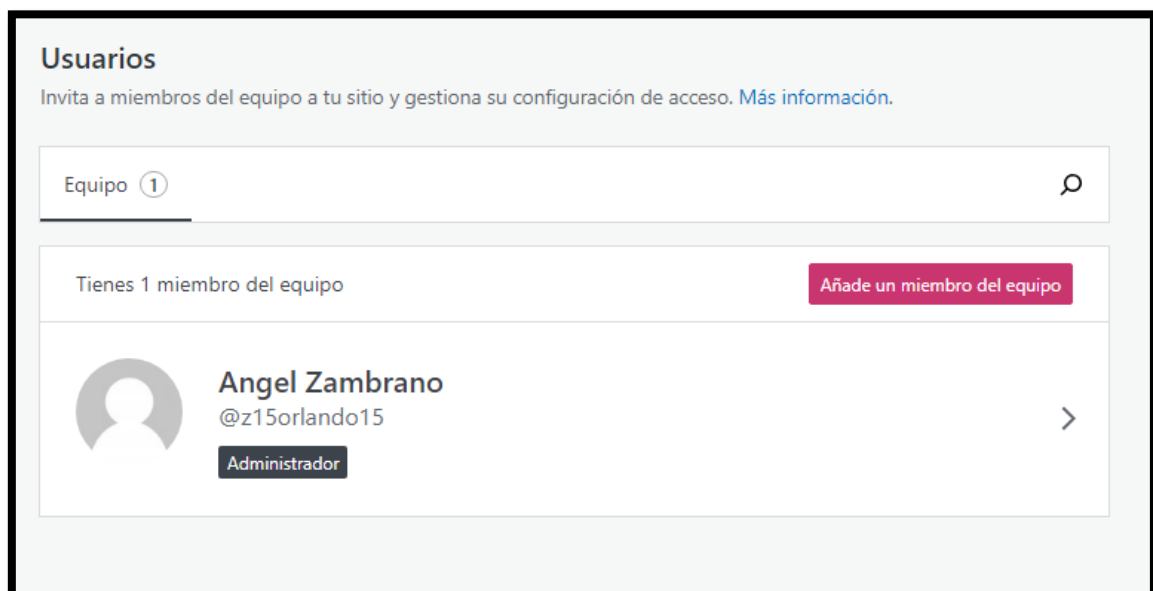
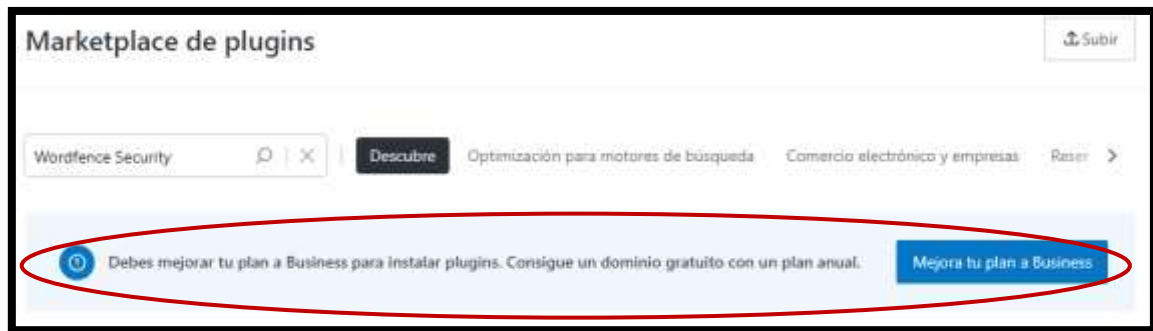
Actualizaciones programadas
☒ Informes gratuitos sobre las actualizaciones programadas de los plugins.

Está actualizada.

- Uso de complementos de seguridad.

Wordfence Security. – Plugin de seguridad que incluyen cortafuegos, escaneo de malware, y bloqueo de IP.

iThemes Security. – Ofrece protección contra ataques de fuerza bruta y auditoría de seguridad.



Solo yo como administrador tengo los permisos para editar mi página Web.

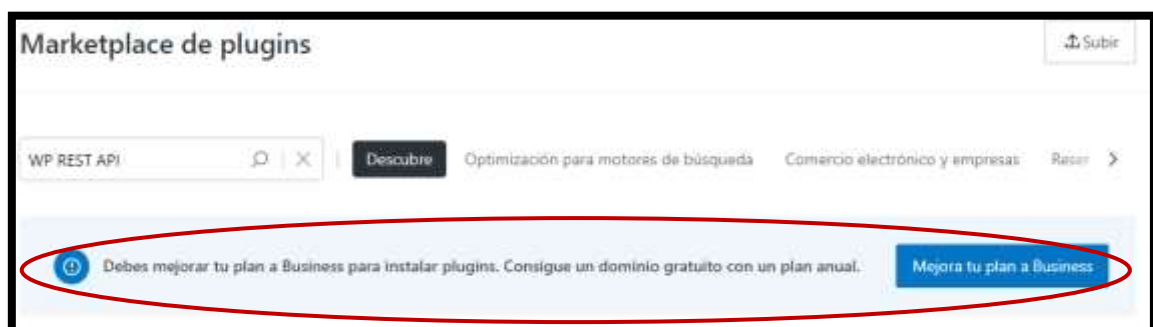
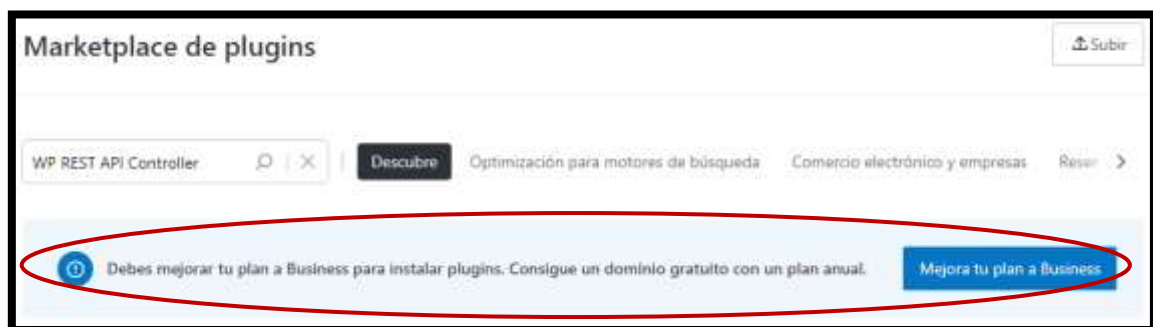
- Configuración de HTTPS.



- **Llamadas a una API :**
- Integración de API: Implementa llamadas a una API externa o propia, asegurando la correcta integración con el sitio web.
- Ejemplos de Llamadas: Incluye al menos dos ejemplos de llamadas API (por ejemplo, obtención de datos de productos, envío de formularios).
- Seguridad en las Llamadas: Asegúrese de que las llamadas a la API sean seguras, utilizando métodos de autenticación y autorización adecuados.

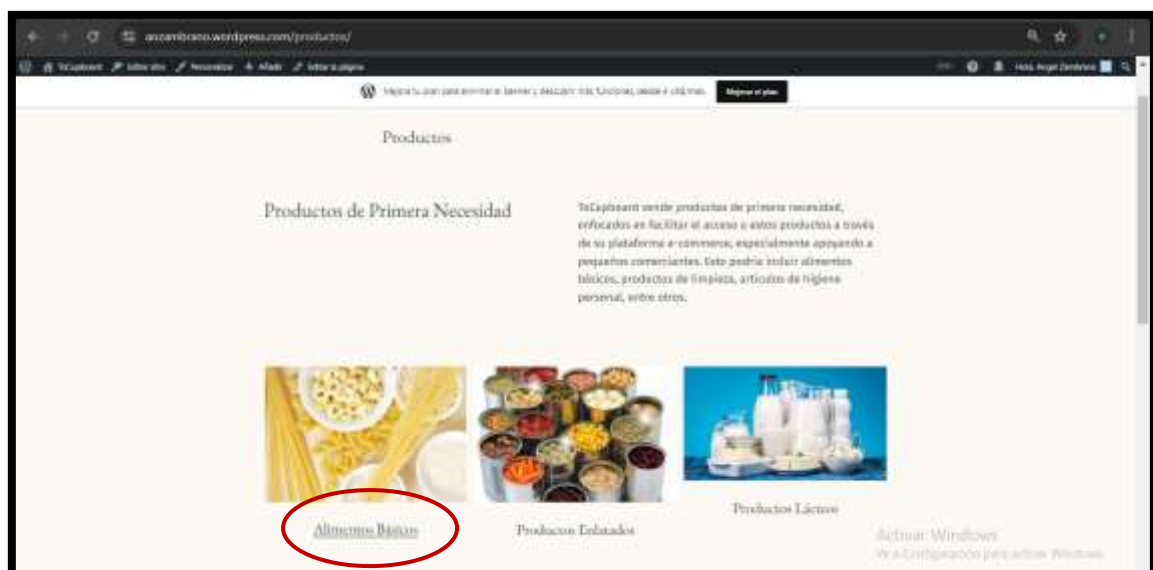
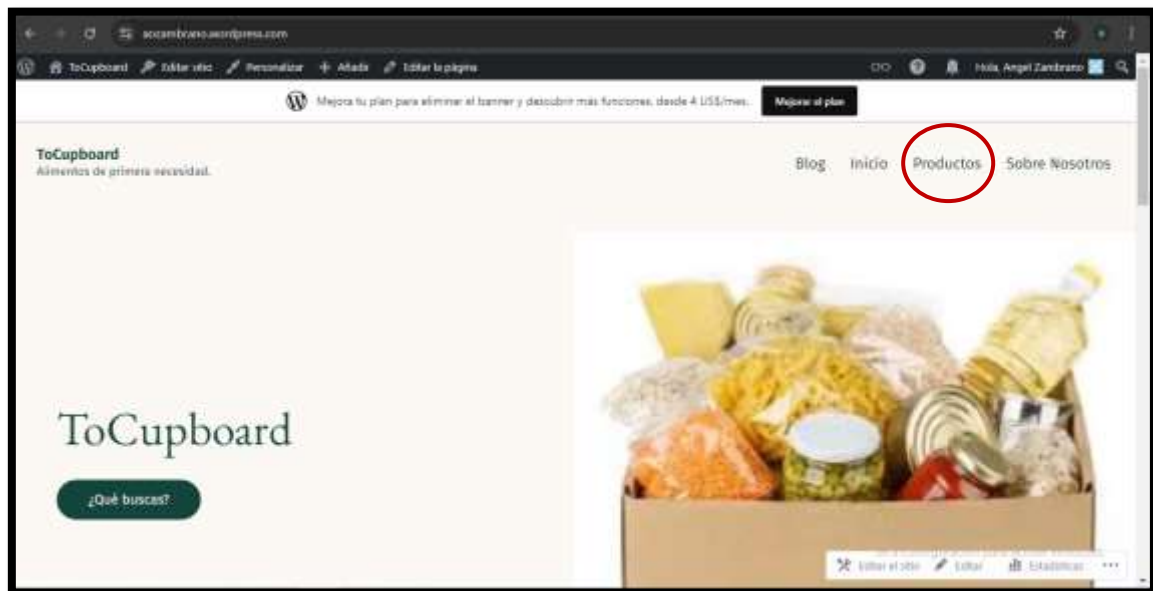
WP REST API Controller. – Se utiliza para configurar la API REST de WordPress a través de una interfaz gráfica sin necesidad de escribir código.

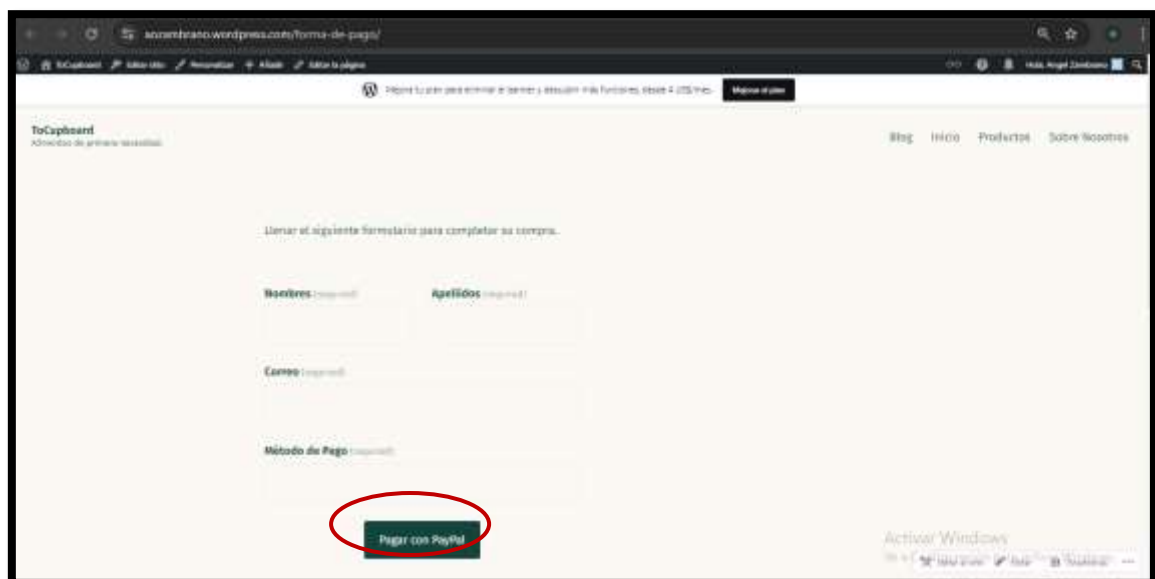
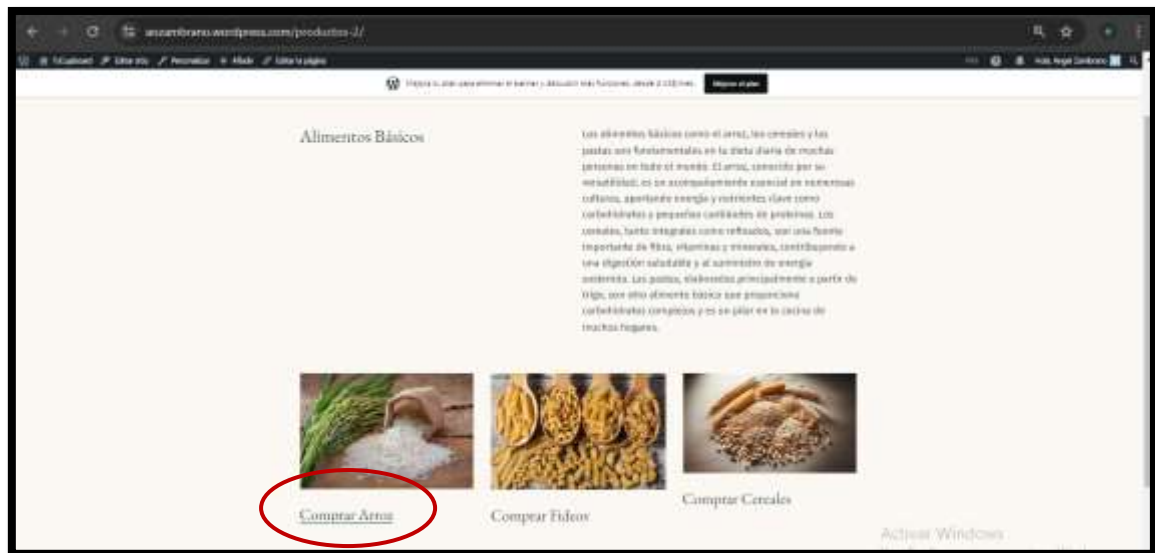
WP API (REST API de WordPress): Se utiliza para crear endpoints personalizados, integrar con APIs externas, o acceder y manipular datos de WordPress mediante solicitudes HTTP.



- **Simulación de una Pasarela de Pagos :**

- Proceso de Pago: Implementa una simulación del proceso de pago, desde la selección del producto hasta la confirmación del pago.
- Seguridad en el Pago: Asegura que la simulación siga las mejores prácticas de seguridad en pagos, como:
 - Uso de tokens de pago.
 - Validación de datos del cliente.
- Simulación de entornos seguros (por ejemplo, utilizando PayPal Sandbox o Stripe Test Mode).








¿Tiene una cuenta PayPal? **Iniciar sesión**

0


Pagar con tarjeta de débito o crédito

No compartiremos su información financiera con el vendedor.

País
Ecuador

Nº de la tarjeta



Iniciar sesión



- **Aplicación del Modelo DevSecOps :**
- Integración del Modelo: Describa cómo se ha aplicado el modelo DevSecOps en la implementación de la página web.

La implementación del modelo DevSecOps se aplicó de manera integral en la página web de WordPress, garantizando la seguridad.

Planificación y Diseño

Se seleccionaron temas y plugins que cumplen con las mejores prácticas de seguridad.

Desarrollo

Las llamadas a la API y las simulaciones de la pasarela de pagos fueron implementadas con autenticación segura y validación de datos, protegiendo contra ataques comunes como la inyección de código o el acceso no autorizado.

Despliegue

- Se aseguraron las mejores prácticas para el despliegue seguro, como la configuración de HTTPS mediante un certificado SSL para cifrar la comunicación entre el servidor y los usuarios.
- Se implementaron controles de acceso estrictos en el panel de administración y se actualizaron constantemente WordPress y sus complementos para minimizar riesgos.

Operación y Monitoreo

Después del despliegue, se configuró un monitoreo continuo de eventos de seguridad, utilizando plugins específicos de seguridad que proporcionan alertas en tiempo real sobre posibles amenazas.

- Prácticas de Seguridad: Documenta las prácticas de seguridad implementadas, como:
- Integración continua y despliegue continuo (CI/CD).
- Pruebas automatizadas de seguridad.
- Monitoreo continuo de vulnerabilidades

Seguridad y análisis de código

Las funciones de seguridad y análisis ayudan a mantener su repositorio seguro y actualizado. Al habilitar estas funciones, nos otorga permiso para realizar análisis de solo lectura en su repositorio.

Descripción general de seguridad

Política de seguridad • **Habilitada**

Vea cómo informar de forma segura las vulnerabilidades de seguridad de este repositorio

[Ver política de seguridad](#)

Avisos de seguridad • **Habilitado**

Ver o divulgar avisos de seguridad para este repositorio

[Ver avisos de seguridad](#)

Informes de vulnerabilidad privados • **Habilitado**

Permitir a los usuarios informar de forma privada sobre posibles vulnerabilidades de seguridad

[Ver vulnerabilidades reportadas](#)

Alertas de Dependabot • **Habilitado**

Recibe una notificación cuando una de tus dependencias tenga una vulnerabilidad

[Ver alertas de Dependabot](#)

Alertas de escaneo de código • **Habilitado**

Detecta automáticamente vulnerabilidades comunes y errores de codificación

[Ver alertas](#)

Alertas de escaneo secreto • **Habilitado**

Recibir una notificación cuando se envíe un secreto a este repositorio

[Ver secretos detectados](#)

Seguridad y análisis de código

Las funciones de seguridad y análisis ayudan a mantener su repositorio seguro y actualizado. Al habilitar estas funciones, nos otorga permiso para realizar análisis de solo lectura en su repositorio.

Informes de vulnerabilidad privados

Permita que su comunidad informe de forma privada sobre posibles vulnerabilidades de seguridad a los encargados del mantenimiento y a los propietarios de repositorios. [Obtenga más información sobre los informes privados de vulnerabilidades](#)

[Desactivar](#)

Gráfico de dependencia

Comprenda sus dependencias.
El gráfico de dependencia siempre está habilitado para los repositorios públicos.

Activado

Envío automático de dependencias

Detecta e informa automáticamente las dependencias en tiempo de compilación para ecosistemas seleccionados.

Activado

Dependabot

Mantenga sus dependencias seguras y actualizadas. [Obtenga más información sobre Dependabot](#)

Alertas de Dependabot

Recibe alertas sobre vulnerabilidades que afecten a sus dependencias y genere manualmente solicitudes de incorporación de cambios de Dependabot para resolverlas. [Configure notificaciones de alerta](#)

[Desactivar](#)

Reglas del Dependabot

Use sus propias reglas personalizadas y administre ajustes preestablecidos de alerta.

1 regla habilitada



Actualizaciones de seguridad de Dependabot

Si habilita esta opción, Dependabot intentará abrir solicitudes de extracción automáticamente para resolver cada alerta de Dependabot abierta con un parche disponible. Si desea opciones de configuración más específicas, desactive esta opción y use [las reglas de Dependabot](#).

[Desactivar](#)

Actualizaciones de seguridad agrupadas

Agrupar todas las actualizaciones disponibles que resuelven una alerta de Dependabot en una solicitud de incorporación de cambios (por administrador de paquetes y directorio de manifiestos de requisito). Esta opción puede ser anulada por las reglas de grupo especificadas en dependabot.yml. [Obtenga más información aquí](#)

[Desactivar](#)

Actualizaciones de la versión de Dependabot

Permite que Dependabot abra solicitudes de incorporación de cambios automáticamente para mantener sus dependencias actualizadas cuando haya nuevas versiones disponibles. [Obtenga más información sobre cómo configurar un archivo dependabot.yml](#)

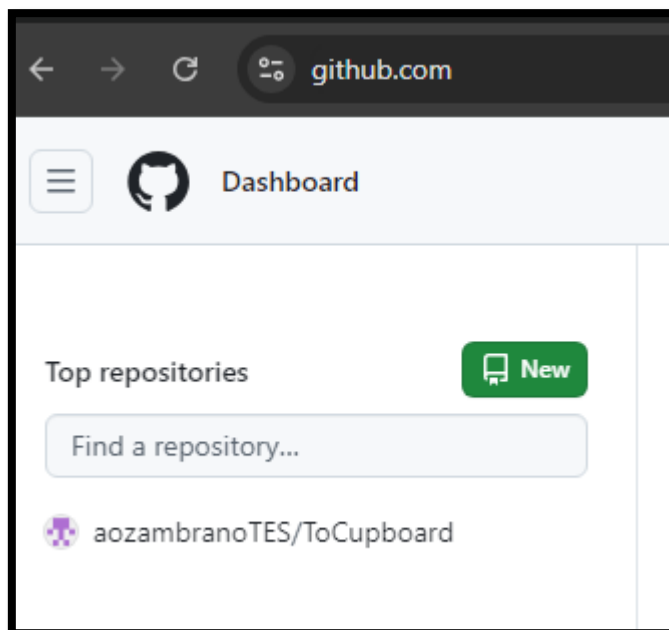
Permitir

Dependabot de los ejecutores de acciones

Ejecuta actualizaciones de seguridad y versiones de Dependabot en los ejecutores de Acciones.

[Desactivar](#)

- **Crea un repositorio en GitHub** y nómbralo acorde al proyecto. Asegúrate de incluir:
- Un archivo README.md que describe brevemente el contenido y propósito del repositorio.



Inicialice este repositorio con:

- ☒ **Agregar un archivo README**

Aquí puedes escribir una descripción detallada de tu proyecto. [Obtén más información sobre los archivos README.](#)



- Integra todos los archivos, códigos y documentación correspondientes a los entregables de este Sprint, organizando el contenido de manera estructurada.

 aozambranoTES Añadir archivos mediante carga		3767d80 · ahora	🕒 7 confirmaciones
 Angel Zambrabo_Desarrolla - Sprint 2.pdf	Añadir archivos mediante carga	ahora	
 Angel Zambrabo_Planifica - Sprint 2.pdf	Añadir archivos mediante carga	ahora	
 README.md	Actualizar README.md	hace 8 minutos	
 SEGURIDAD.md	Actualizar SECURITY.md	hace 26 minutos	

- Configure los permisos de acceso necesarios para que el equipo de Digital NAO pueda acceder fácilmente.

¿Quién tiene acceso?



Repositorio público

Este repositorio es público y visible para cualquier persona.

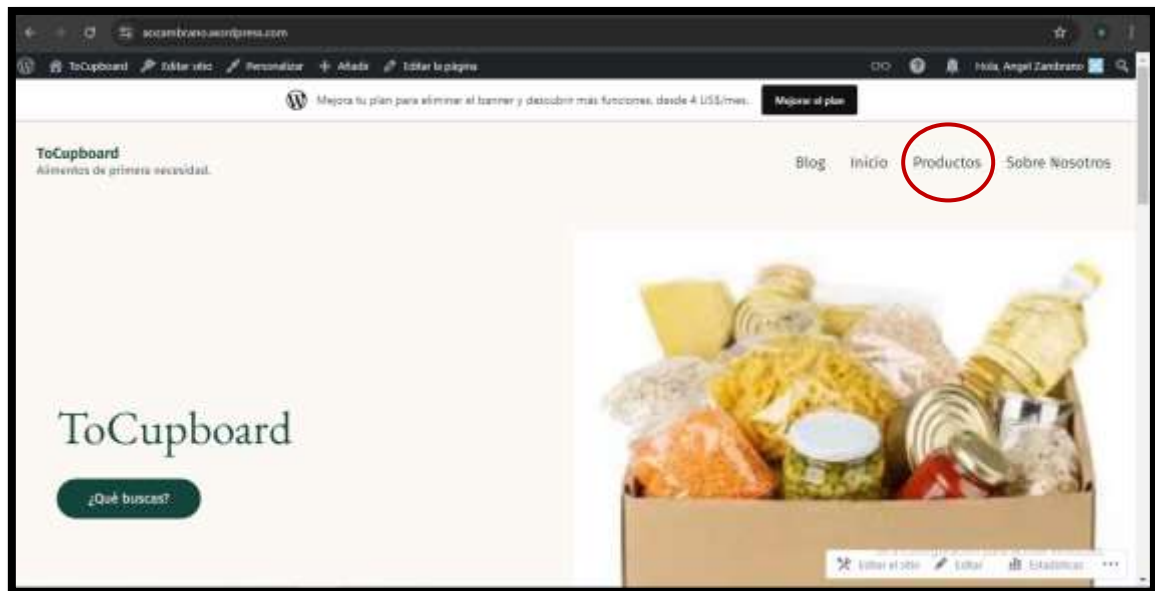
Administrar

2 . Realiza un Reporte Técnico que incluya:

- Instrucciones para acceder y navegar por el sitio web.

A continuación, se proporcionará las instrucciones para acceder y navegar por el sitio web de ToCupboard:

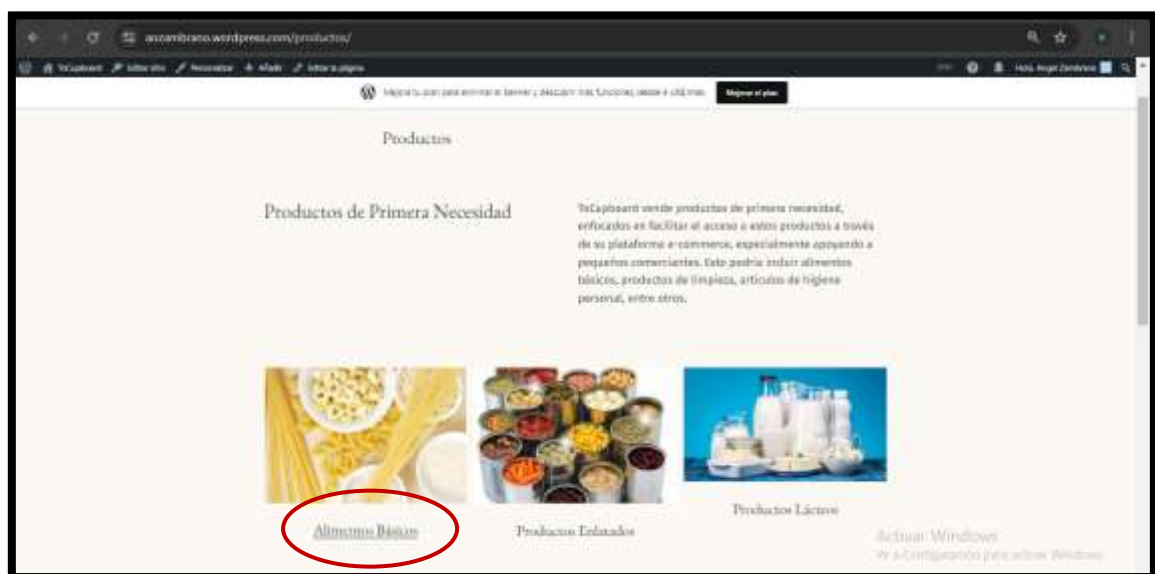
1. Ingresa a tu navegador de preferencia.
2. Ingrese la siguiente URL en la barra de direcciones:
<https://aozambrano.wordpress.com/>
3. En la página de Inicio podrá acceder a “Productos”, “Sobre Nosotros” y en los diferentes tipos de productos podrá dar clic en la palabra “Entrar”.
4. Al dar clic en “Productos”, se les abrirá otra página donde podrá elegir qué tipo de producto necesita.
5. Como es una página de prueba solo podrá entrar en “Alimentos Básicos”.
6. Al dar clic en “Alimentos Básicos”, se les abrirá otra página donde podrá elegir qué tipo de producto necesita.
7. Como es una página de prueba solo podrá entrar en “Comprar Arroz”.
8. Al dar clic en “Comprar Arroz”, se les abrirá otra página donde tendrá que llenar un formulario.

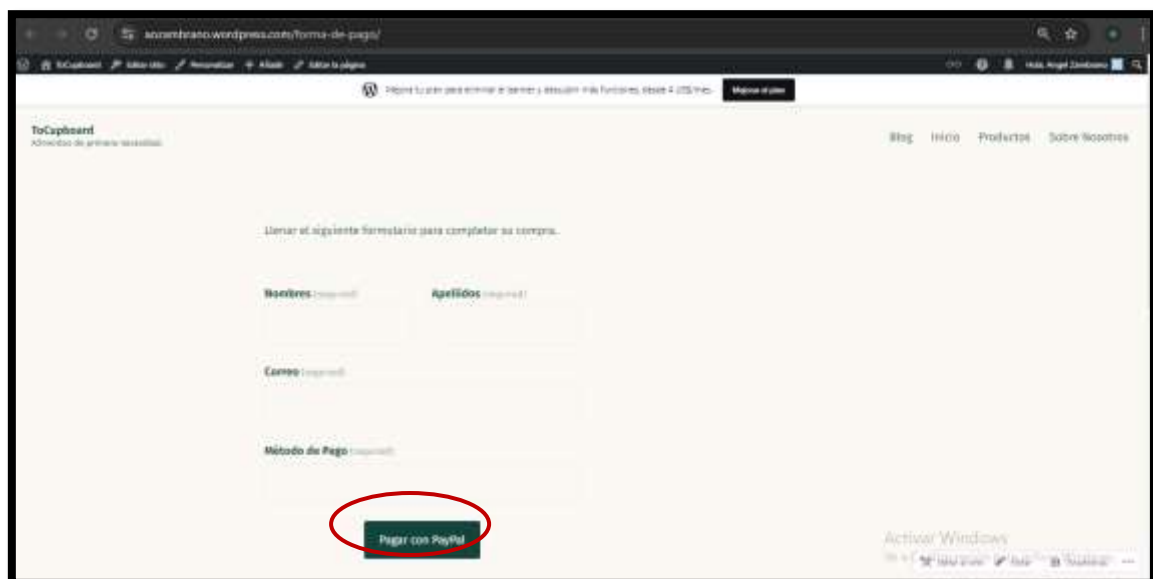
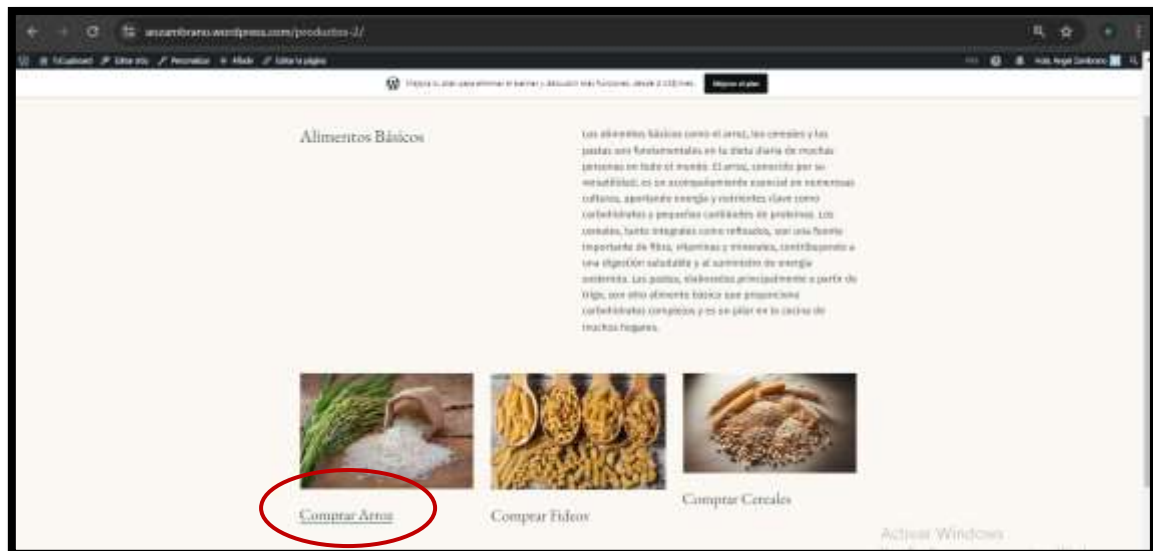


PRODUCTOS ENLATADOS

¡No esperes más! Explora nuestra selección de productos enlatados y experimenta la combinación perfecta de sabor, frescura y practicidad. Contacta a nuestro equipo de ventas para realizar tu pedido hoy mismo.

[ENTRAR](#)



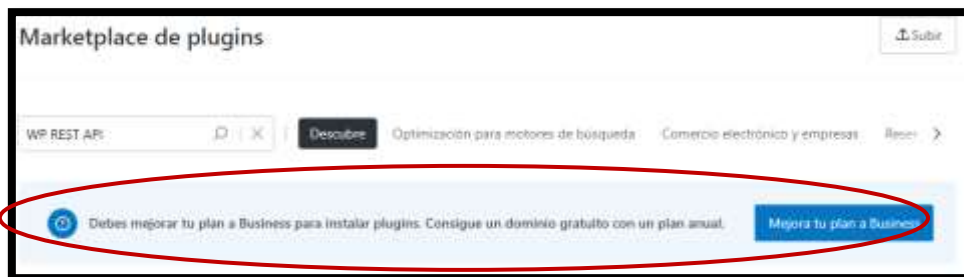
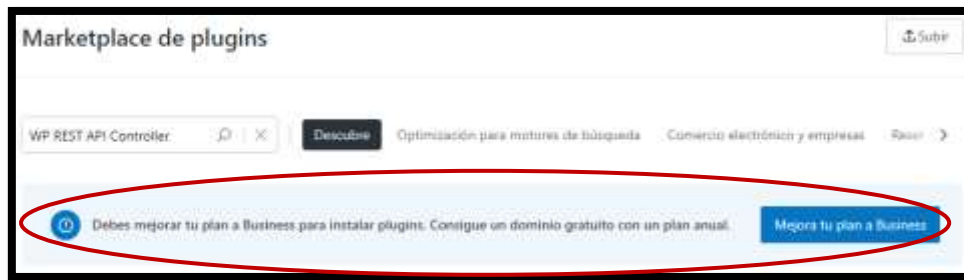


- Descripción de las llamadas a la API implementadas.

Se le quiso aplicar estas dos API “WP REST API Controller” y “WP API (REST API de WordPress)”, pero para poder instalarla se necesitaba mejorar el plan a Business, ya que, mi plan es el gratuito.

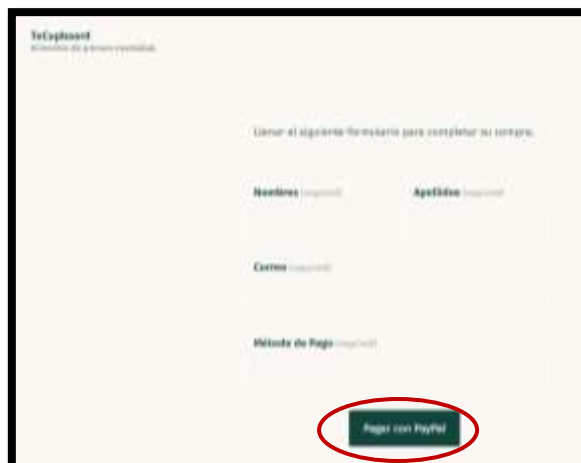
WP REST API Controller. – Se utiliza para configurar la API REST de WordPress a través de una interfaz gráfica sin necesidad de escribir código.

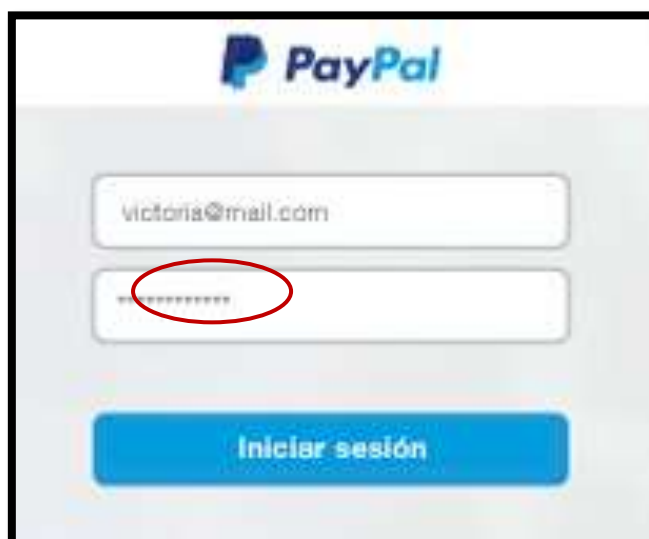
WP API (REST API de WordPress): Se utiliza para crear endpoints personalizados, integrar con APIs externas, o acceder y manipular datos de WordPress mediante solicitudes HTTP.



- Descripción del proceso de simulación de la pasarela de pagos.

Se realizó una simulación de pago con algunas imágenes ficticias, el pago se hizo a través de PayPal. Después de llenar el formulario se les abrirá otra pestaña donde tendrán que iniciar sesión en PayPal y podrá confirmar su compra. A continuación, se adjunta imágenes:







- Explicación detallada de cómo se aplicó el modelo DevSecOps.

La implementación del modelo DevSecOps se aplicó de manera integral en la página web de WordPress, garantizando la seguridad.

Planificación y Diseño

Se seleccionaron temas y plugins que cumplen con las mejores prácticas de seguridad.

Desarrollo

Las llamadas a la API y las simulaciones de la pasarela de pagos fueron implementadas con autenticación segura y validación de datos, protegiendo contra ataques comunes como la inyección de código o el acceso no autorizado.

Despliegue

- Se aseguraron las mejores prácticas para el despliegue seguro, como la configuración de HTTPS mediante un certificado SSL para cifrar la comunicación entre el servidor y los usuarios.
- Se implementaron controles de acceso estrictos en el panel de administración y se actualizaron constantemente WordPress y sus complementos para minimizar riesgos.

Operación y Monitoreo

Después del despliegue, se configuró un monitoreo continuo de eventos de seguridad, utilizando plugins específicos de seguridad que proporcionan alertas en tiempo real sobre posibles amenazas.

Nota: Agrego los links de la página web de WordPress y el Repositorio.

<https://aozambrano.wordpress.com/>

<https://github.com/aozambranoTES/ToCupboard>

- Capturas de pantalla relevantes y cualquier otra documentación de soporte.



