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

Contenido

DevSecOps: Integración de Seguridad a lo Largo del Ciclo de Vida En el marco del desarrollo del sitio web de ToCupBoard, la implementación de prácticas y herramientas de seguridad en WordPress se alinea con el enfoque **DevSecOps**, que integra la seguridad en cada etapa del desarrollo y la operación del software. Desde la fase de desarrollo hasta la producción, la seguridad se ha aplicado de manera proactiva, utilizando herramientas y plugins como **Wordfence**, **Sucuri** y **All In One WP Security**, además de herramientas externas como **SSL Labs**, **Sucuri Security** y **Pentest-Tools**.

El objetivo del modelo DevSecOps es detectar y mitigar vulnerabilidades antes de que puedan convertirse en problemas críticos, garantizando que la seguridad no sea un paso adicional, sino una parte continua del proceso de desarrollo.

CI/CD: Integración Continua y Entrega Continua Los principios de **CI/CD** también se reflejan en la implementación del reto, permitiendo que las herramientas de seguridad, las automatizaciones de copias de seguridad y la gestión de certificados SSL sean integradas directamente en el flujo de desarrollo y despliegue.

1. **Integración Continua (CI):** Cada cambio en la configuración del sitio se integra de manera continua. En este punto, herramientas como **Wordfence**, **All In One WP Security** y los escaneos externos mediante **Pentest-Tools** pueden realizar verificaciones automáticas del entorno. De esta manera, se garantiza que cualquier vulnerabilidad potencial sea identificada de inmediato y los cambios no se desplieguen hasta que sean seguros.
2. **Entrega Continua (CD):** Una vez que la configuración ha pasado las verificaciones de seguridad, se despliega automáticamente a producción. Las herramientas como **Really Simple SSL** y **WP Encryption** aseguran que el sitio esté siempre protegido con certificados SSL actualizados, mientras que **Backup Bolt** garantiza que existan copias de seguridad automatizadas en caso de que sea necesario revertir cambios o restaurar el sistema. Esto asegura que el sitio mantenga su integridad y seguridad en todo momento.

Configuración HTTPS

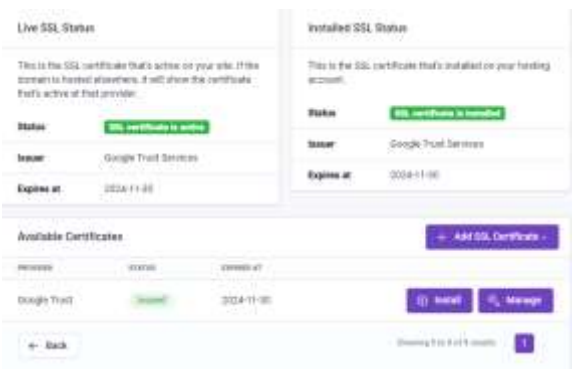
El sitio web está configurado con **HTTPS**, lo que asegura que las comunicaciones entre el servidor y el cliente estén **cifradas** y protegidas contra interceptaciones. El **certificado SSL**, emitido por **Google Trust Services**, está activo hasta el **30 de noviembre de 2024**.

Funcionalidad del Certificado SSL:

- **Cifrado de Tráfico**: Protege datos sensibles (contraseñas, pagos) de ser interceptados.
- **Autenticación del Sitio**: Verifica que el sitio es legítimo, evitando ataques como phishing.
- **Confianza del Usuario**: El candado en la barra de direcciones mejora la seguridad percibida.

Beneficios de HTTPS:

- **Protección contra Ataques**: Evita escucha y manipulación de datos.
- **Mejora SEO**: Google favorece sitios con HTTPS, mejorando su visibilidad.
- **Compatibilidad**: Navegadores modernos requieren HTTPS para algunas funciones, como geolocalización.



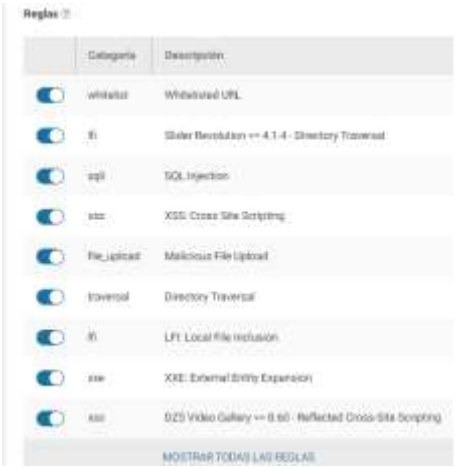
Plugins de Seguridad Wordpress

Wordfence Security

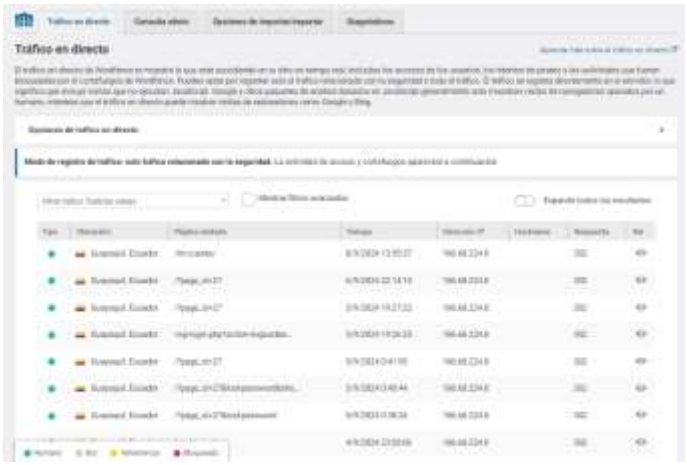
Se implementó **Wordfence Security** para proteger el sitio contra amenazas como hackeos, malware y ataques de fuerza bruta. Entre sus funcionalidades más importantes se destacan:

- **Firewall**: Bloquea accesos maliciosos, ataques DDoS, y aplica reglas de protección como contra **SQL Injection** y **XSS**.
- **Protección de Fuerza Bruta**: Bloquea intentos de inicio de sesión repetidos y detecta IPs sospechosas.
- **Monitoreo en Tiempo Real**: Permite visualizar el tráfico en directo, mostrando actividad de usuarios, intentos de ataque y accesos bloqueados.
- **Escáner de Malware**: Detecta y elimina código malicioso y vulnerabilidades en archivos, temas y plugins.
- **Alertas por Correo**: Informa sobre eventos sospechosos, intentos fallidos de acceso y solicitudes de cambio de contraseña.
- **Configuración de 2FA**: Refuerza la seguridad del inicio de sesión para usuarios clave.

- Reglas implementadas

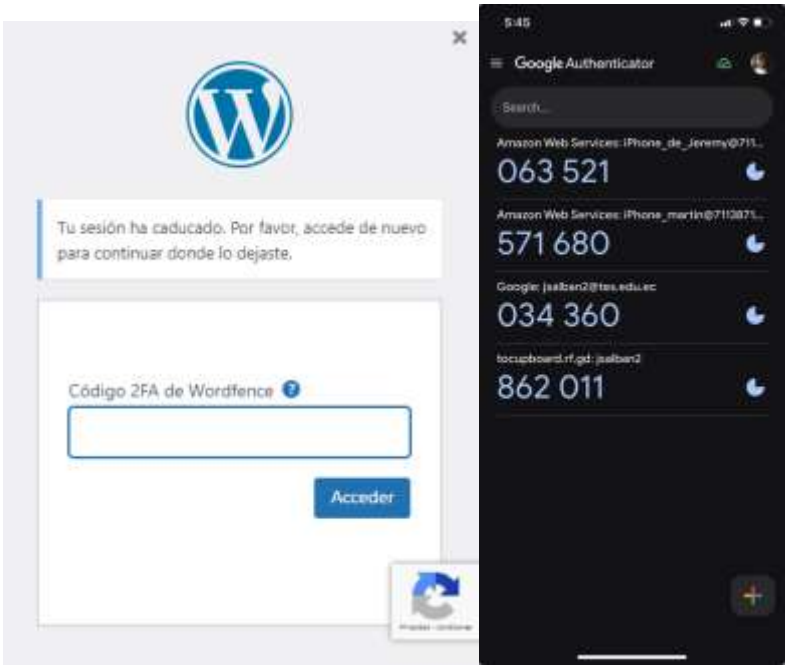


- Monitoreo de las actividades relacionadas a la seguridad.



- Alerta (vía mail) acerca de una actividades inusual

- 2FA Activo:



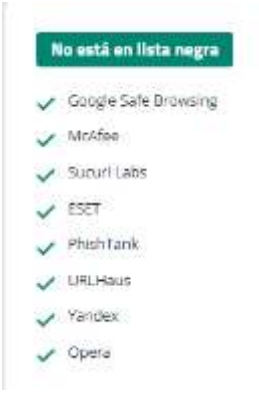
Sucuri Security

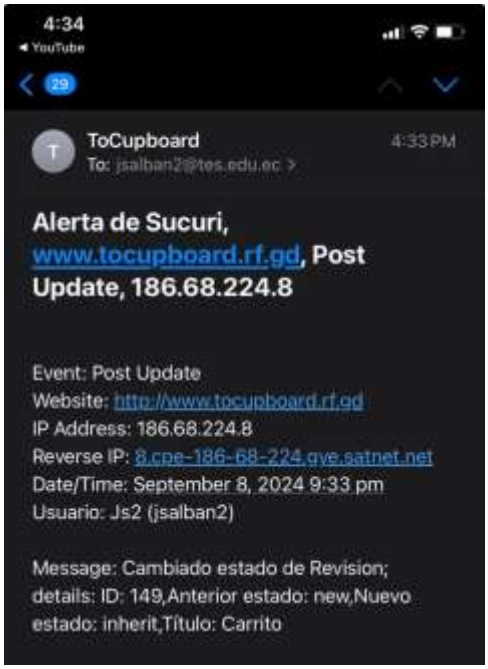
Se implementó **Sucuri** para proteger el sitio de **ToCupBoard**, proporcionando monitoreo de seguridad en tiempo real y mitigación de ataques DDoS y malware. Además, cualquier actividad notifica mediante correo. Entre sus funciones principales están:

- **Firewall de Aplicación Web (WAF)**: Bloqueó intentos de ataques DDoS y posibles explotaciones de vulnerabilidades.

- **Escaneo de Malware y Auditoría de Seguridad**: Ejecutó análisis regulares de malware y verificaciones de integridad de archivos, asegurando que no se detectaron códigos maliciosos.
- **Monitoreo de Listas Negras**: Confirmó que el sitio no ha sido incluido en listas negras de motores de búsqueda ni ha mostrado actividad desde IPs maliciosas.
- **Detección de Anomalías**: Verificó que no existían redirecciones sospechosas, spam o frames malintencionados.

Los resultados de los escaneos han sido positivos en general, confirmando que el sitio está seguro y libre de amenazas o anomalías.

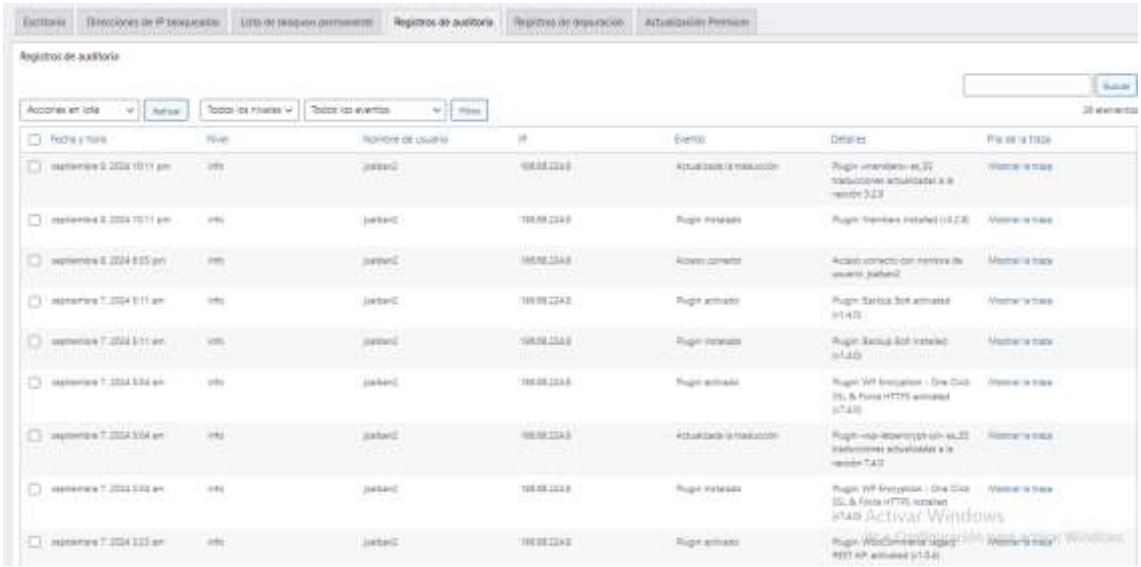


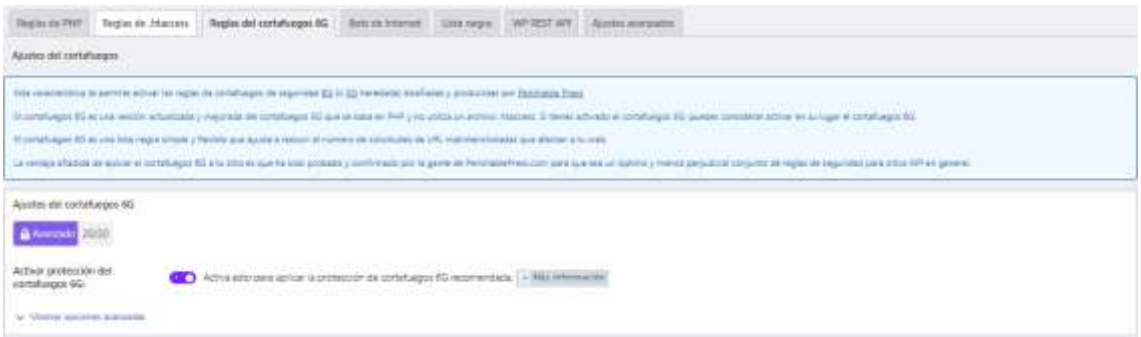


All In One WP Security & Firewall

Se implementó **All In One WP Security & Firewall** en **ToCupBoard** para fortalecer la seguridad general del sitio.

- **Endurecimiento del Sitio**: Se activaron reglas básicas de firewall.
- **Escaneo de Vulnerabilidades**: Se ejecutaron escaneos regulares para identificar riesgos de configuración inseguros y mantener el sitio protegido.
- **Registros de Auditoría**: Se monitorizan actividades y cambios para asegurar un control constante sobre el sistema.





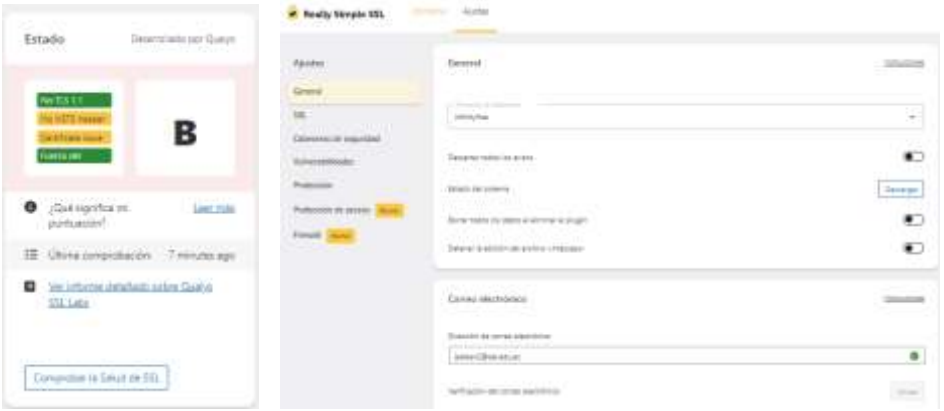
Backup Bolt

Se implementó **Backup Bolt** en **ToCupBoard** para asegurar la recuperación de datos en caso de fallos o ataques.

- **Copia de Seguridad Automática**: Se configuraron copias de seguridad programadas para proteger la base de datos y los archivos del sitio.
- **Restauración Rápida**: La funcionalidad permite devolver el sitio a un estado seguro en caso de pérdida de datos o problemas de seguridad.

Really Simple SSL

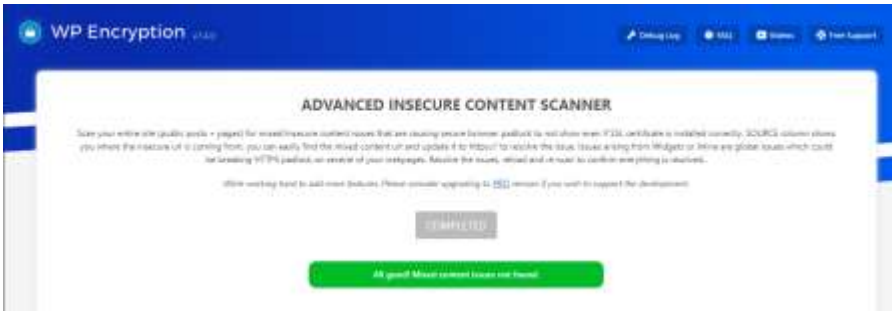
Instalé el plugin **Really Simple SSL** para asegurar que todo el tráfico de mi sitio web se redirija automáticamente de HTTP a HTTPS. Aunque ya tenía un certificado SSL activo en mi hosting, el plugin me facilitó la gestión al configurar todo sin necesidad de realizar ajustes manuales. Además, utilicé el plugin para revisar y mejorar la seguridad de la conexión, aunque mi sitio ya estaba protegido con HTTPS, ayudándome a verificar que el certificado estuviera correctamente implementado.

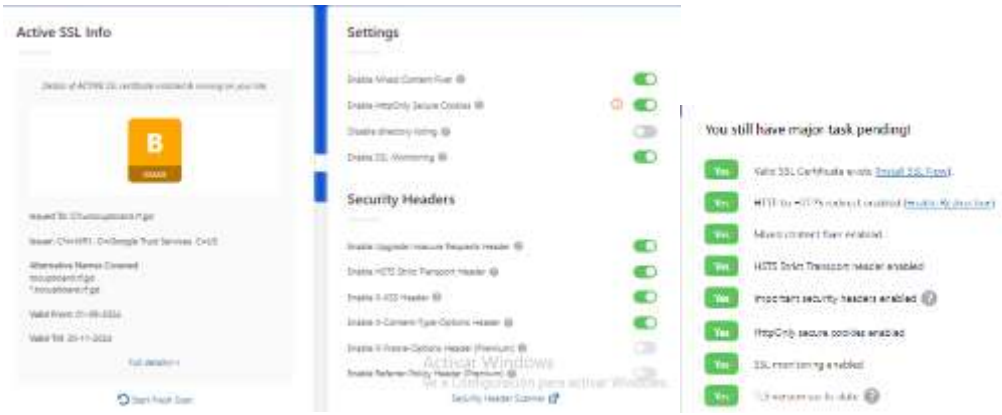


WP Encryption

Con el plugin **WP Encryption**, realicé las siguientes configuraciones en mi sitio web de WordPress:

1. **Encabezados de seguridad**: Activé la opción para que encabezados importantes como HSTS y X-Frame-Options sean fortalecidos para la protección del sitio.
2. **Solución de contenido mixto**: Habilité una herramienta que resuelve automáticamente los problemas de contenido mixto, asegurando que todos los elementos del sitio se sirvan a través de HTTPS.
3. **Monitoreo de SSL**: Activé la supervisión automática del certificado SSL para garantizar que esté siempre actualizado y funcionando correctamente.





Herramientas externas

SSL LABS

Se utilizó la herramienta **SSL Labs** para realizar una evaluación exhaustiva del certificado SSL/TLS del sitio we. Esta plataforma de análisis es ampliamente reconocida por ofrecer una revisión completa de la configuración de seguridad SSL/TLS de los sitios web.

Puntos Destacados:

- **Validez y Origen del Certificado:** El certificado SSL fue emitido por **Google Trust** y es válido desde el 1 de septiembre de 2024 hasta el 30 de noviembre de 2024, lo que garantiza una conexión segura para los usuarios durante este periodo.
- **Implementación de Protocolos Seguros:** La evaluación confirmó que el sitio utiliza versiones seguras de **TLS**, evitando el uso de versiones obsoletas como SSLv3 o TLS 1.0, lo cual es fundamental para la protección de los datos intercambiados.
- **Cipher Suites:** Se validó el uso de **algoritmos de cifrado robustos**, lo cual fortalece aún más la seguridad del sitio frente a posibles ataques.

Este análisis permitió identificar cualquier posible debilidad en la implementación del SSL, asegurando que las comunicaciones entre el sitio y los usuarios estén protegidas por cifrado adecuado y que se sigan las mejores prácticas de seguridad recomendadas para mantener la integridad de las conexiones.

Sucuri SiteCheck

Se utilizó la herramienta **Sucuri SiteCheck** para realizar un escaneo exhaustivo de seguridad del sitio web. Esta herramienta se especializa en la detección de infecciones de malware, vulnerabilidades conocidas y posibles bloqueos en listas negras de seguridad.

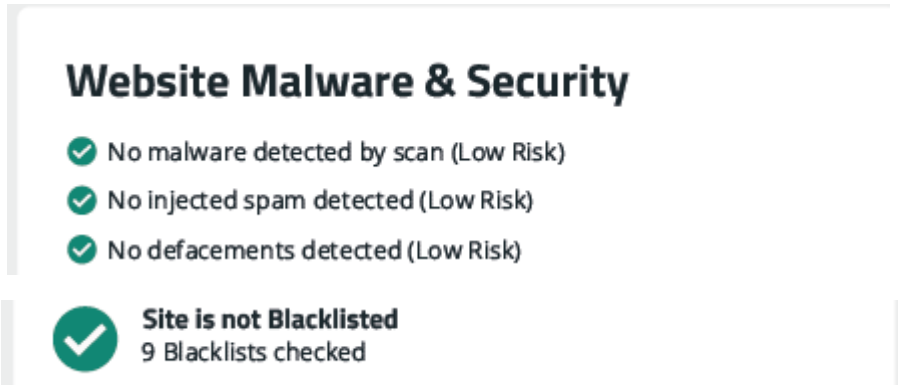
Puntos Destacados:

- **Escaneo de Malware:** El análisis no detectó la presencia de malware ni scripts maliciosos en el código fuente del sitio, confirmando que el sitio está libre de infecciones.
- **Verificación de Listas Negras:** El dominio fue evaluado en **9 listas negras de seguridad**, incluyendo **Google Safe Browsing**, **McAfee**, **Sucuri Labs**, **ESET**, **PhishTank**, **Yandex** y **Opera**, obteniendo resultados positivos en todas. El sitio no está bloqueado en ninguna de estas plataformas, lo que asegura la buena reputación del dominio.

Detalle del estado de listas negras:

  - **Google Safe Browsing:** Dominio limpio.
  - **McAfee:** Dominio limpio.
  - **Sucuri Labs:** Dominio limpio.
  - **ESET:** Dominio limpio.
  - **PhishTank:** Dominio limpio.
  - **Yandex:** Dominio limpio.
  - **Opera:** Dominio limpio.

Este análisis proporcionó un informe detallado del estado de seguridad del sitio web, destacando la ausencia de malware y la inexistencia de bloqueos en las listas negras más relevantes.



Pentest-Tools

Se realizó un análisis de seguridad del sitio utilizando la plataforma **Pentest-Tools**, la cual permite realizar pruebas de penetración automatizadas, simulando ataques reales para evaluar la solidez de la seguridad de la aplicación web. El análisis fue concluyente y presentó un **nivel de riesgo global bajo**, con **0 vulnerabilidades de riesgo alto o medio** detectadas.

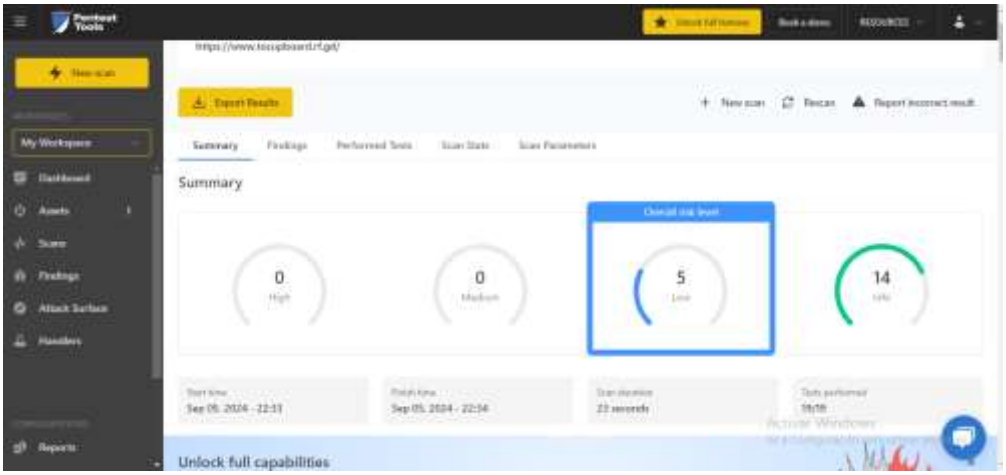
Puntos Destacados:

- **Nivel de Riesgo Global:** El análisis reportó un **nivel de riesgo bajo**. No se detectaron vulnerabilidades críticas (alto o medio), lo que demuestra la robustez de la configuración de seguridad actual del sitio.
- **Ausencia de Vulnerabilidades Críticas:** Las pruebas no encontraron vulnerabilidades significativas en los siguientes aspectos:
    - **Software del lado del servidor:** No se detectaron fallos en el software del servidor.
    - **Políticas de acceso del cliente:** No se encontraron problemas con las políticas de acceso para los usuarios.
    - **Archivos de configuración clave:** No se identificaron problemas relacionados con los archivos robots.txt o la ausencia de un archivo security.txt.
    - **Certificados de Seguridad:** El sitio no presentó el uso de certificados no confiables, lo que garantiza que las comunicaciones están bien protegidas.
- **Verificación de Métodos HTTP:** El análisis confirmó que los métodos HTTP de depuración y las opciones no seguras no están habilitadas, lo que refuerza la seguridad del sitio contra ataques comunes que explotan estas configuraciones.
- **Encabezados de Seguridad:** Aunque se detectaron algunas cabeceras de seguridad ausentes en la configuración (como **X-Content-Type-Options** y **Strict-Transport-Security**), estas no representan vulnerabilidades críticas y se pueden mejorar en futuras actualizaciones.

Resultados del Análisis:

- **Nivel de Riesgo:** Bajo
- **Vulnerabilidades Detectadas:**
    - **Alto:** 0
    - **Medio:** 0
    - **Bajo:** 5
    - **Información:** 14
- **Duración del Escaneo:** 23 segundos
- **Número de Pruebas Ejecutadas:** 19/19 (100% de cobertura)

El análisis confirmó que el sitio web es accesible, está bien configurado y no presenta vulnerabilidades críticas. Los aspectos evaluados, como la ausencia de configuraciones inseguras en el servidor, la correcta gestión de los certificados y la implementación de políticas adecuadas de acceso para los usuarios, garantizan un entorno seguro.



Pentest Tools

Website Vulnerability Scanner Report

✓ https://www.tocupboard.rf.gd/

Summary

Overall risk level:

Low

Risk ratings:

High:	0
Medium:	0
Low:	5
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

Modificaciones en el .htaccess

Redireccionamiento de HTTP a HTTPS

```
# BEGIN Redireccionar todo el tráfico HTTP a HTTPS
<IfModule mod_rewrite.c>
RewriteEngine On
RewriteCond %{HTTPS} !=on [NC]
RewriteCond %{HTTP:X-Forwarded-Proto} !https
RewriteCond %{REQUEST_URI} !^/\.well-known/acme-challenge/
RewriteRule ^(.*)$ https://%{HTTP_HOST}%{REQUEST_URI} [R=301,L]
</IfModule>
# END Redireccionar todo el tráfico HTTP a HTTPS
```

Se ha implementado una regla que redirige automáticamente todo el tráfico de HTTP a HTTPS, lo que garantiza que todas las conexiones con el sitio sean seguras. Al activar el motor de reescritura, se comprueba si la conexión no está utilizando HTTPS, y en caso contrario, se redirige a la versión segura del sitio mediante un redireccionamiento permanente (código 301). Esto asegura que todas las solicitudes sean procesadas a través de HTTPS, mejorando la protección de los datos en tránsito.

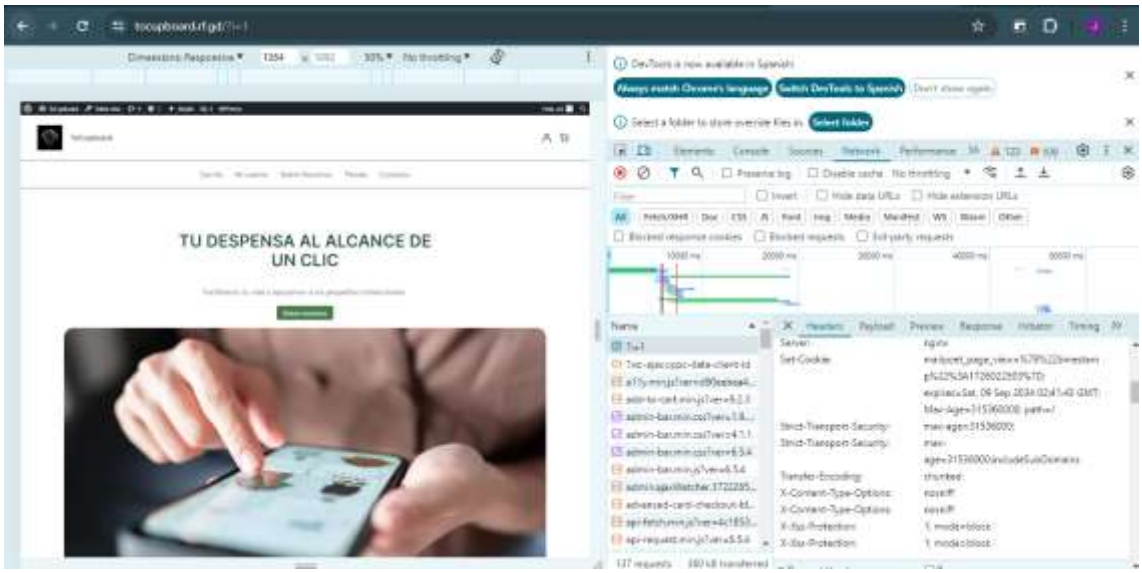
Configuración de cabeceras HTTP de seguridad

Además, se han añadido varias cabeceras HTTP de seguridad para mitigar riesgos comunes de ataques. Las cabeceras configuradas son:

- **X-Frame-Options**: Previene ataques de clickjacking al limitar la capacidad de incrustar el sitio en iframes externos.
- **X-XSS-Protection**: Activa la protección contra ataques de inyección de scripts (XSS) en navegadores compatibles.
- **Content-Security-Policy**: Establece una política que restringe la carga de recursos únicamente desde el propio dominio del sitio.
- **Strict-Transport-Security (HSTS)**: Obliga a utilizar HTTPS en todas las conexiones futuras, evitando accesos no seguros por HTTP.
- **X-Content-Type-Options**: Impide que el navegador intente adivinar los tipos de contenido, protegiendo contra ciertos ataques de inyección.
- **Referrer-Policy**: Controla la cantidad de información de referencia que se comparte con sitios externos, mejorando la privacidad del usuario.

Estas configuraciones contribuyen a reforzar la seguridad del sitio, protegiéndolo de vulnerabilidades como clickjacking, ataques XSS y el envío de datos no cifrados.

- Se reflejan cabeceras en el navegador



Implementación del Modelo DevSecOps

El enfoque de **DevSecOps** permitió integrar la seguridad de manera continua durante el desarrollo y mantenimiento del sitio web. Esto incluye la implementación de las siguientes prácticas:

1. **Seguridad desde el diseño**: Desde la selección de plugins hasta la configuración del servidor, se consideraron las mejores prácticas de seguridad.
2. **Integración continua**: Con la ayuda de plugins como Wordfence y Sucuri, las amenazas potenciales son monitoreadas y mitigadas en tiempo real sin interrumpir el desarrollo.
3. **Automatización de procesos**: Los plugins como Backup Bolt y WP Encryption automatizan la creación de copias de seguridad y la renovación de certificados SSL, garantizando que el sitio esté siempre actualizado y protegido sin necesidad de intervención manual constante.
4. **Revisión constante**: Las herramientas de auditoría y escaneo proporcionadas por los plugins de seguridad ayudan a detectar vulnerabilidades a medida que el sitio evoluciona, garantizando una protección continua.