EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://asojuntasgirardot.dev/	Checks	9 pruebas
Dominio	asojuntasgirardot.dev	Hallazgos	52 totales
Fecha	23 de septiembre de 2026 a las 01:17	Problemas	18 detectados

C

65/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado al dominio asojuntasgirardot.dev arroja una puntuación de 65/100, lo que corresponde a una calificación de grado C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 4 resultaron exitosos, 4 generaron advertencias y 1 fue clasificado como fallo crítico. Se han detectado deficiencias importantes en la configuración de cabeceras de seguridad y una exposición de infraestructura que compromete la confidencialidad de la plataforma. Debido a la presencia de puertos de bases de datos abiertos y cookies desprotegidas, se concluye que el sitio es vulnerable y requiere intervención inmediata.

Resumen de Riesgos

1	7	8	2	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 74 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	No se detecto un CMS conocido
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	50	AVISO	XSRF-TOKEN: falta HttpOnly; XSRF-TOKEN: falta Se...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	2 puerto(s) potencialmente riesgoso(s): 22 (SSH)...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 74 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  74 dias restantes (expira: 2026-12-05T18:05:39.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-09-06T18:05:40.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: nginx/1.31.4 — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.4.25 — Revela framework/lenguaje
- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- MEDIO **X-Content-Type-Options**
  Falta — Evita MIME-type sniffing
- MEDIO **Referrer-Policy**
  Falta — Controla la informacion de referer enviada
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://asojuntasgirardot.dev/
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

No se detecto un CMS conocido

- INFO **WordPress**
  No detectado
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  No detectado
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- INFO **Tecnologias detectadas**
  PHP/8.4.25

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente

- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente
- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 50/100

Estado: AVISO

XSRF-TOKEN: falta HttpOnly; XSRF-TOKEN: falta Secure; laravel-session: falta Secure

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- ALTO **Cookie: XSRF-TOKEN — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: XSRF-TOKEN — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: XSRF-TOKEN — SameSite**
  SameSite=lax
- INFO **Cookie: laravel-session — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: laravel-session — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: laravel-session — SameSite**
  SameSite=lax

Contenido Mixto — 100/100

Estado: OK

No se detecto contenido mixto

- INFO **Contenido mixto**
  Todos los recursos se cargan por HTTPS

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (24 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 60/100

Estado: AVISO

2 puerto(s) potencialmente riesgoso(s): 22 (SSH), 5432 (PostgreSQL)

- INFO **Puerto 21 (FTP)**
  Cerrado — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — Acceso remoto seguro
- INFO **Puerto 23 (Telnet)**
  Cerrado — Acceso remoto sin cifrar
- INFO **Puerto 25 (SMTP)**
  Cerrado — Envio de correo
- INFO **Puerto 80 (HTTP)**
  Abierto (esperado) — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Abierto (esperado) — Servidor web seguro
- INFO **Puerto 3306 (MySQL)**
  Cerrado — Base de datos MySQL expuesta

- INFO **Puerto 3389 (RDP)**
  Cerrado — Escritorio remoto Windows
- CRITICO **Puerto 5432 (PostgreSQL)**
  ABIERTO — Base de datos PostgreSQL expuesta
- INFO **Puerto 6379 (Redis)**
  Cerrado — Cache Redis sin autenticacion por defecto
- INFO **Puerto 8080 (HTTP-Alt)**
  Cerrado — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
  Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[CRITICAL] Puerto 5432 (PostgreSQL): El puerto de la base de datos está abierto y accesible desde internet, lo que permite intentos de conexión externa y ataques de fuerza bruta.
[HIGH] Ausencia de Content-Security-Policy: No se detectó esta cabecera, lo que facilita la ejecución de ataques Cross-Site Scripting (XSS) e inyección de contenido.
[HIGH] Ausencia de X-Frame-Options: La falta de esta directiva permite que el sitio sea cargado en marcos externos, haciendo a los usuarios vulnerables a ataques de clickjacking.
[HIGH] Ausencia de Strict-Transport-Security: No se implementa HSTS, por lo que el navegador no fuerza la conexión cifrada, permitiendo ataques de degradación de protocolo.
[HIGH] Cookie XSRF-TOKEN sin HttpOnly: Esta cookie carece del flag de seguridad, permitiendo que sea accesible mediante scripts maliciosos en el navegador.
[HIGH] Cookies XSRF-TOKEN y laravel-session sin flag Secure: Las cookies de sesión se envían a través de conexiones no cifradas, lo que permite su interceptación en redes inseguras.
[MEDIUM] Ausencia de X-Content-Type-Options: El servidor no previene el sniffing de tipos MIME, lo que podría permitir la ejecución de archivos maliciosos disfrazados de contenido legítimo.
[MEDIUM] Rutas de administración expuestas: Se detectó acceso público a /administrator/ y /user/login, aumentando el riesgo de ataques dirigidos contra el panel de gestión.
[MEDIUM] Archivos informativos accesibles: Los archivos /readme.html y /README.txt están expuestos, pudiendo revelar versiones de software y detalles de la arquitectura interna.
[MEDIUM] Puerto 22 (SSH) ABIERTO: El servicio de acceso remoto está expuesto, representando un vector de entrada potencial si no cuenta con políticas de acceso restrictivas.
[MEDIUM] Ausencia de Referrer-Policy y Permissions-Policy: No existe control sobre la información de navegación enviada a terceros ni sobre el uso de APIs del dispositivo.
[LOW] Cabecera Server expuesta: Se revela el uso de nginx/1.31.4, facilitando a los atacantes la identificación de vulnerabilidades específicas para esa versión de servidor.
[LOW] Cabecera X-Powered-By expuesta: El servidor confirma el uso de PHP/8.4.25, lo que entrega información técnica innecesaria sobre el entorno de ejecución.