EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.dragonjar.org	Checks	9 pruebas
Dominio	www.dragonjar.org	Hallazgos	48 totales
Fecha	17 de julio de 2026 a las 21:41	Problemas	14 detectados

C

69/100

puntos de seguridad

RESUMEN EJECUTIVO

Tras realizar el análisis de seguridad en el sitio web, se ha obtenido una puntuación de 69/100 con una nota C, lo que sitúa a la plataforma en un nivel de riesgo moderado. Se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 2 generaron advertencias y 2 fallaron debido a configuraciones críticas ausentes. El sitio presenta una excelente gestión de certificados SSL, pero carece de cabeceras de seguridad fundamentales y expone versiones de software desactualizadas. En su estado actual, se concluye que el sitio es vulnerable a ataques de suplantación, secuestro de clics y explotación de vulnerabilidades conocidas.

Resumen de Riesgos

0	4	6	4	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 83 dias
Cabeceras de Seguridad	25	FALLO	Solo 1/6 presentes. Faltan: X-Frame-Options, Str...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 6.3 expuesta, WordPress 2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 83 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  83 dias restantes (expira: 2026-10-09T02:03:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-07-11T01:04:02.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 25/100

Estado: FALLO

Solo 1/6 presentes. Faltan: X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: cloudflare — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.2.30 — Revela framework/lenguaje
- INFO **Content-Security-Policy**
  Presente: upgrade-insecure-requests
- 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://www.dragonjar.org/
- 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

CMS detectado: WordPress, PrestaShop

- INFO **WordPress**
  Detectado via HTML body
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  Detectado via HTML body
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: Site Kit by Google 1.183.0
- INFO **Tecnologias detectadas**
  Next.js, PHP/8.2.30

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.3 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 6.3 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS

- INFO **Archivo /README.txt**
  No accesible (correcto)
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente

Seguridad de Cookies — 100/100

Estado: OK

No se encontraron cookies

- INFO **Cookies detectadas**
  El sitio no establece cookies en la respuesta inicial

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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (121 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://www.dragonjar.org/sitemap_index.xml
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- INFO **Puerto 21 (FTP)**
  Cerrado — Transferencia de archivos sin cifrar
- INFO **Puerto 22 (SSH)**
  Cerrado — 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
- INFO **Puerto 5432 (PostgreSQL)**
  Cerrado — Base de datos PostgreSQL expuesta
- INFO **Puerto 6379 (Redis)**
  Cerrado — Cache Redis sin autenticacion por defecto
- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — Servidor web alternativo / proxy

INFO **Puerto 27017 (MongoDB)**

Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[HIGH] Falta de Strict-Transport-Security: No se fuerza el uso de HTTPS mediante HSTS, permitiendo ataques de interceptación de tráfico tipo Man-in-the-Middle.
[HIGH] Falta de X-Frame-Options: La ausencia de esta cabecera permite que el sitio sea cargado en iframes, facilitando ataques de clickjacking para engañar usuarios.
[HIGH] Version de WordPress 6.3 expuesta: Revelar la versión exacta permite a los atacantes identificar y explotar vulnerabilidades públicas específicas (CVEs).
[MEDIUM] Falta de X-Content-Type-Options: El sitio es vulnerable al sniffing de tipos MIME, lo que podría permitir la ejecución de archivos maliciosos como scripts.
[MEDIUM] Falta de Referrer-Policy y Permissions-Policy: No se controla la información enviada en los enlaces salientes ni se restringen las capacidades del navegador del usuario.
[MEDIUM] Acceso público a /readme.html y /wp-login.php: La exposición de estos archivos y rutas facilita el reconocimiento y los ataques de fuerza bruta contra el panel administrativo.
[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La visibilidad de puertos alternativos aumenta la superficie de ataque y sugiere servicios internos mal configurados.
[LOW] Cabeceras de servidor expuestas (Server y X-Powered-By): Se revela el uso de Cloudflare y PHP/8.2.30, proporcionando datos valiosos para la fase de reconocimiento de un ataque.
[LOW] Meta generator expuesto: El plugin Site Kit by Google revela información sobre la estructura interna y herramientas utilizadas en el CMS.
[LOW] Ruta sensible en robots.txt: La referencia directa al directorio admin facilita la identificación de áreas restringidas para atacantes automatizados.