EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://fedosa.org/	Checks	9 pruebas
Dominio	fedosa.org	Hallazgos	51 totales
Fecha	3 de agosto de 2026 a las 19:39	Problemas	8 detectados

B

88/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado a la plataforma arroja una puntuación de 88/100 con una nota final de B. Se ejecutaron un total de 9 checks pasivos, de los cuales 7 resultaron satisfactorios, 1 generó una advertencia y 1 se identificó como fallo crítico. La infraestructura presenta una base sólida en cuanto a cifrado y cabeceras de seguridad, pero exhibe fugas de información técnica sensibles. Se concluye que el sitio es generalmente seguro para el usuario final, aunque vulnerable ante ataques dirigidos debido a la exposición de versiones de software.

Resumen de Riesgos

0	1	4	3	43
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 53 dias
Cabeceras de Seguridad	100	OK	Todas las cabeceras de seguridad presentes
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
Deteccion CMS	100	OK	CMS detectado: WordPress
Version CMS Expuesta	20	FALLO	WordPress 7.0.2 expuesta, WordPress 2 expuesta
Seguridad de Cookies	100	OK	1 cookies, todas con flags correctos
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 53 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  53 dias restantes (expira: 2026-09-25T19:01:35.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-27T18:04:04.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 100/100

Estado: OK

Todas las cabeceras de seguridad presentes

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

- INFO **Content-Security-Policy**
  Presente: default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn....
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN, SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; includeSubDomains
- INFO **X-Content-Type-Options**
  Presente: nosniff, nosniff
- INFO **Referrer-Policy**
  Presente: strict-origin-when-cross-origin, no-referrer-when-downgrade
- INFO **Permissions-Policy**
  Presente: camera=(), microphone=(), geolocation=()

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://fedosa.org/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000; includeSubDomains
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 dias)
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

CMS detectado: WordPress

- INFO **WordPress**
  Detectado via HTML body
- 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
- BAJO **Meta generator**
  Expone: WordPress 7.0.2

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 7.0.2 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 7.0.2 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- 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

Seguridad de Cookies — 100/100

Estado: OK

1 cookies, todas con flags correctos

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: PHPSESSID — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: PHPSESSID — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: PHPSESSID — SameSite**
  SameSite=strict

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 (1947 bytes)
- INFO **Reglas robots.txt**
  10 Disallow, 2 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://fedosa.org/wp-sitemap.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] WordPress version: La versión 7.0.2 del CMS se encuentra expuesta públicamente, lo que facilita a atacantes la búsqueda de vulnerabilidades específicas (CVEs).
[MEDIUM] Archivo /readme.html: Este archivo es accesible de forma pública y puede revelar detalles internos y versiones precisas del gestor de contenidos.
[MEDIUM] Archivo /README.txt: Documentación técnica expuesta que asiste en el reconocimiento del sistema por parte de terceros no autorizados.
[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La disponibilidad de un puerto alternativo incrementa la superficie de ataque al exponer posibles servicios de administración o proxies.
[MEDIUM] Configuración de robots.txt: El archivo bloquea la indexación total del sitio y revela rutas sensibles como el directorio de administración.
[LOW] Server header expuesto: La cabecera revela el uso de Cloudflare, proporcionando pistas sobre la tecnología de protección y red del servidor.
[LOW] Meta generator: La etiqueta en el código fuente confirma el uso de WordPress 7.0.2, reforzando la exposición de la versión.