EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.cfisiomad.org	Checks	9 pruebas
Dominio	www.cfisiomad.org	Hallazgos	46 totales
Fecha	22 de junio de 2026 a las 20:22	Problemas	16 detectados

D

56/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio cfisiomad.org arroja una puntuación de 56/100, lo que equivale a una calificación de grado D. Durante la evaluación se ejecutaron 9 checks pasivos, resultando en 4 verificaciones exitosas, 2 advertencias por configuraciones mejorables y 3 fallos críticos en la infraestructura. Se han identificado riesgos severos relacionados con la exposición de bases de datos y la falta total de cabeceras de protección. Debido a la apertura de puertos sensibles y la visibilidad de versiones de software, el sitio se concluye como vulnerable ante ataques dirigidos. Es imperativo aplicar medidas correctivas inmediatas para elevar los estándares de seguridad de la plataforma.

Resumen de Riesgos

1	6	7	2	30
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 35 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	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 7.3.8 expuesta, WordPress 2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	60	AVISO	2 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	20	FALLO	3 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 35 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  35 dias restantes (expira: 2026-07-28T02:40:49.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-29T02:40:50.000Z
- 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 — Revela tecnologia del servidor

- 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://www.cfisiomad.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: WordPress 6.9.4
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 7.3.8 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 7.3.8 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)

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 — 60/100

Estado: AVISO

2 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://cfisiomad.com/#/auth/login
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://prevencionescolares.es

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (249 bytes)
- INFO **Reglas robots.txt**
  2 Disallow, 0 Allow
- INFO **Sitemap en robots.txt**
  https://cfisiomad.org/sitemap_index.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 20/100

Estado: FALLO

3 puertos riesgosos abiertos

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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
- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — 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

[CRITICAL] Puerto 3306 (MySQL) abierto: La base de datos se encuentra expuesta a internet, lo que permite ataques de fuerza bruta o explotación directa de la información almacenada.
[HIGH] Cabeceras de seguridad ausentes: El sitio no implementa CSP, X-Frame-Options ni HSTS, facilitando ataques de inyección de scripts, clickjacking y secuestro de sesiones.
[HIGH] Puerto 21 (FTP) abierto: Servicio de transferencia de archivos activo que transmite datos sin cifrar, permitiendo la interceptación de credenciales de acceso.
[HIGH] Exposición de versión de WordPress: La visibilidad de la versión 7.3.8 y 2 permite a atacantes identificar y explotar CVEs específicos ya documentados.
[HIGH] HSTS no configurado: El servidor no obliga al navegador a utilizar siempre conexiones seguras, dejando la puerta abierta a ataques de degradación de protocolo (SSL Stripping).
[MEDIUM] Contenido mixto detectado: Existen recursos cargados mediante HTTP en una página HTTPS, lo que compromete la integridad de la conexión cifrada.
[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La presencia de un servidor web secundario aumenta la superficie de ataque y suele ocultar servicios menos protegidos.
[MEDIUM] Archivo /readme.html accesible: Este archivo revela información técnica sobre la instalación del CMS que debería ser privada.
[LOW] Cabecera de servidor expuesta: El servidor revela el uso de nginx, proporcionando datos útiles para el reconocimiento inicial de un atacante.
[LOW] Meta generator expuesto: El código fuente muestra la versión exacta de WordPress, facilitando el perfilado de vulnerabilidades.