EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://cfisiomad.madrid	Checks	9 pruebas
Dominio	cfisiomad.madrid	Hallazgos	39 totales
Fecha	23 de junio de 2026 a las 09:11	Problemas	14 detectados

D

57/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado sobre el sitio web ha arrojado una puntuación de 57/100, lo que resulta en una calificación de grado D. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales únicamente 3 resultaron satisfactorios, mientras que se identificaron 2 advertencias y 2 fallos críticos. El hallazgo de puertos de infraestructura expuestos y la ausencia total de cabeceras de protección básicas sitúan al sitio en una posición de vulnerabilidad. Se concluye que el sitio no es seguro y requiere intervenciones inmediatas para proteger la integridad de los datos y la disponibilidad del servicio.

Resumen de Riesgos

1	5	6	2	25
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
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	60	AVISO	2 recurso(s) HTTP en pagina HTTPS
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://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

- 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 6.9.4
- INFO **Tecnologias detectadas**
  Next.js

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

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): La base de datos se encuentra abierta a internet, permitiendo intentos de conexión externa y ataques de fuerza bruta.
[HIGH] Content-Security-Policy (CSP): La ausencia de esta cabecera facilita la ejecución de ataques XSS y la inyección de contenido malicioso.
[HIGH] X-Frame-Options: La falta de esta protección hace al sitio vulnerable a ataques de clickjacking, donde un atacante puede secuestrar clics del usuario.
[HIGH] Strict-Transport-Security (HSTS): No se obliga al navegador a usar HTTPS, permitiendo ataques de degradación de SSL y la interceptación de tráfico.
[HIGH] Puerto 21 (FTP): Servicio de transferencia de archivos sin cifrar expuesto, lo que facilita la captura de credenciales en tránsito.
[MEDIUM] X-Content-Type-Options: El sitio no previene el sniffing de tipos MIME, lo que podría permitir la ejecución de archivos maliciosos disfrazados.
[MEDIUM] Contenido Mixto: Se detectaron recursos cargados mediante HTTP inseguro dentro de la página protegida, comprometiendo la seguridad de la sesión.
[MEDIUM] Referrer-Policy: No se define qué información de navegación se comparte con otros sitios, afectando a la privacidad de los usuarios.
[MEDIUM] Permissions-Policy: Falta de restricciones sobre APIs sensibles del navegador como la geolocalización o la cámara.
[MEDIUM] Puerto 8080 (HTTP-Alt): Un puerto de servidor web alternativo está abierto, aumentando la superficie de ataque disponible para agentes externos.
[LOW] Meta generator: El sitio expone públicamente que utiliza WordPress 6.9.4, facilitando la identificación de exploits para esta versión específica.
[LOW] Server header expuesto: La cabecera revela el uso de Nginx, proporcionando información valiosa a los atacantes sobre la tecnología del servidor.