

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://ironx-mern-fitness-app.vercel.app/
Dominio ironx-mern-fitness-app.vercel.app
Fecha 28 de mayo de 2026 a las 20:53

Checks 9 pruebas
Hallazgos 49 totales
Problemas 7 detectados

A

100/100

puntos de seguridad

RESUMEN EJECUTIVO

Tras completar la auditoría técnica, el sitio web presenta una puntuación de 100/100 y una calificación de nota A. Se han ejecutado un total de 9 checks pasivos con resultados plenamente satisfactorios, no registrándose fallos ni advertencias críticas en la infraestructura analizada. Cabe destacar que el pentest activo no fue ejecutado en esta instancia, por lo que los resultados se limitan a la configuración de seguridad perimetral. En conclusión, el sitio se considera seguro y cumple con los estándares óptimos de implementación de cabeceras y cifrado.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 59 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	No se detecto un CMS conocido
Version CMS Expuesta	100	OK	No se detecto version de CMS 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	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 59 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
59 dias restantes (expira: 2026-07-27T02:04:42.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-04-28T02:04:43.000Z
- 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: Vercel — Revela tecnologia del servidor

- INFO **Content-Security-Policy**
Presente: default-src 'self'; script-src 'self' https://js.stripe.com; style-src 'self' 'u...
- INFO **X-Frame-Options**
Presente: DENY
- INFO **Strict-Transport-Security**
Presente: max-age=63072000; includeSubDomains; preload
- INFO **X-Content-Type-Options**
Presente: nosniff
- INFO **Referrer-Policy**
Presente: strict-origin-when-cross-origin
- INFO **Permissions-Policy**
Presente: camera=(), microphone=(), geolocation=(), payment=(self "https://js.stripe.com")

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
HTTP 308 redirige a https://ironx-mern-fitness-app.vercel.app/
- INFO **HSTS (Strict-Transport-Security)**
HSTS activo: max-age=63072000; includeSubDomains; preload
- BAJO **HSTS includeSubDomains**
HSTS cubre subdominios
- INFO **HSTS max-age**
max-age=63072000 (730 dias)
- 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

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 /wp-login.php**
Panel de login accesible publicamente

- 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 — 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 (180 bytes)
- INFO** Reglas robots.txt
4 Disallow, 1 Allow
- BAJO** Ruta sensible en robots.txt
Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO** Sitemap en robots.txt
<https://ironx-mern-fitness-app.vercel.app/sitemap.xml>
- INFO** security.txt
Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 100/100

Estado: OK

2 puerto(s) abierto(s), todos esperados

- 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

● 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

[LOW] Server header expuesto: El encabezado Server revela el uso de Vercel, lo cual facilita el reconocimiento de la tecnología subyacente a posibles atacantes.

[MEDIUM] Archivos informativos accesibles: Las rutas /readme.html y /README.txt están disponibles públicamente, pudiendo filtrar información sobre versiones o configuraciones internas.

[MEDIUM] Puntos de acceso administrativos expuestos: Se detectó que las rutas /wp-login.php, /administrator/ y /user/login son accesibles, aumentando la superficie de ataque para intentos de intrusión por fuerza bruta.

[LOW] Exposición de rutas en robots.txt: El archivo incluye una referencia directa a la ruta admin, lo cual permite a actores maliciosos identificar directorios sensibles de forma simplificada.