

EscanearVulnerabilidades

Informe de Seguridad Web

URL https://fapic.es
Dominio fapic.es
Fecha 1 de octubre de 2026 a las 15:52

Checks 9 pruebas
Hallazgos 15 totales
Problemas 3 detectados

C

73/100

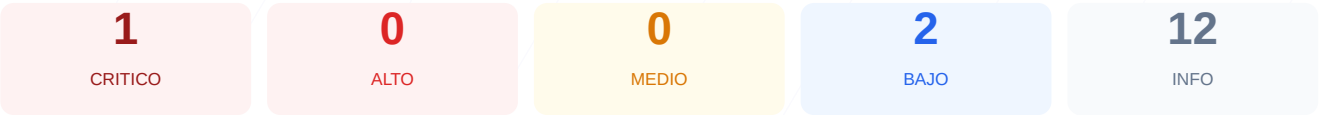
puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad del dominio fapic.es ha resultado en una puntuación de 73/100, obteniendo una nota de C. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 1 resultó correcto y 1 fue identificado como fallo directo, mientras que el resto presentaron errores de conexión que impidieron su validación. Debido a la imposibilidad de verificar el cifrado SSL y las cabeceras de seguridad esenciales, el sitio se considera actualmente vulnerable. Es imperativo solucionar los problemas de conectividad y configuración base para garantizar una navegación segura.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	0	ERROR	No se pudo verificar SSL/TLS
Cabeceras de Seguridad	0	ERROR	No se pudieron verificar las cabeceras
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion HTTPS
Deteccion CMS	0	ERROR	No se pudo analizar el CMS
Version CMS Expuesta	0	ERROR	No se pudo verificar la version del CMS
Seguridad de Cookies	0	ERROR	No se pudieron verificar las cookies
Contenido Mixto	0	ERROR	No se pudo verificar contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 0/100

Estado: ERROR

No se pudo verificar SSL/TLS

- CRITICO Conexion SSL
No se pudo establecer conexion SSL/TLS

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO robots.txt
Error al acceder
- BAJO sitemap.xml
Error al acceder

Puertos Abiertos — 100/100

Estado: OK

No se detectaron puertos abiertos

●	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 — Envío de correo
●	INFO	Puerto 80 (HTTP) Cerrado — Servidor web
●	INFO	Puerto 443 (HTTPS) Cerrado — 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 autenticación 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

[CRITICAL] Conexión SSL/TLS: No se pudo establecer una conexión cifrada, lo que expone los datos de los usuarios a interceptaciones.

[HIGH] Cabeceras de Seguridad: No se detectaron cabeceras de protección, dejando el sitio expuesto a ataques de tipo Cross-Site Scripting y Clickjacking.

[LOW] Ausencia de robots.txt: El archivo de directivas para rastreadores no está accesible, afectando el control de indexación.

[LOW] Ausencia de sitemap.xml: No se encontró el mapa del sitio, lo que dificulta la visibilidad y organización técnica en motores de búsqueda.

[MEDIUM] Error de Redirección HTTPS: El sitio no fuerza de manera efectiva el tráfico seguro, permitiendo conexiones potencialmente inseguras.