

EscanearVulnerabilidades

Informe de Seguridad Web

URL https://afiliación.gesoft.es
Dominio xn--afiliacin-d7a.gesoft.es
Fecha 7 de abril de 2026 a las 03:32

Checks 9 pruebas
Hallazgos 15 totales
Problemas 3 detectados

C

73/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad del sitio web ha arrojado una puntuación de 73/100, lo que equivale a una calificación de nota C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 1 resultó satisfactorio y 1 fue calificado como fallo, mientras que el resto presentó errores de conexión. La imposibilidad de verificar el cifrado y las cabeceras de seguridad impide garantizar la protección de la información transmitida. Por lo tanto, se concluye que el sitio es actualmente vulnerable y presenta riesgos significativos de infraestructura.

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: No se pudo establecer una conexión SSL/TLS, lo que impide el cifrado de datos entre el usuario y el servidor.

[LOW] Archivo robots.txt: Error al acceder al archivo, lo que dificulta el control sobre qué partes del sitio deben ser indexadas por buscadores.

[LOW] Archivo sitemap.xml: No se pudo localizar el mapa del sitio, afectando la estructura de navegación y visibilidad del portal.

[INFO] Cabeceras de seguridad: No se pudieron verificar, lo que sugiere una posible falta de protecciones contra ataques de inyección o clickjacking.