

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://bienestarsocial.dipgra.es/	Checks	9 pruebas
Dominio	bienestarsocial.dipgra.es	Hallazgos	15 totales
Fecha	8 de septiembre de 2026 a las 09:28	Problemas	3 detectados

C

73/100

puntos de seguridad



RESUMEN EJECUTIVO

El analisis de seguridad realizado al sitio bienestarsocial.dipgra.es ha resultado en una puntuacion de 73/100, lo que equivale a una nota C. Se ejecutaron un total de 9 checks pasivos, obteniendo 1 resultado satisfactorio, 0 advertencias y 1 fallo directo, ademas de multiples errores de conexion en parametros criticos. La imposibilidad de verificar el estado del cifrado SSL y las cabeceras de seguridad sugiere una configuracion de red restrictiva o defectuosa. Debido a estas deficiencias tecnicas en elementos base, el sitio se considera vulnerable ante posibles ataques de interceptacion de datos.

Resumen de Riesgos

1 CRITICO	0 ALTO	0 MEDIO	2 BAJO	12 INFO
--------------	-----------	------------	-----------	------------

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] Conexion SSL/TLS: No se pudo establecer una conexion segura, lo que indica que el intercambio de informacion entre el ciudadano y el servidor podria no estar cifrado.

[HIGH] Cabeceras de Seguridad: Ausencia de verificacion de cabeceras HTTP esenciales, lo que facilita ataques de tipo Cross-Site Scripting (XSS) y Clickjacking.

[HIGH] Redireccion HTTPS: El sistema no garantiza el trafico exclusivo por canales seguros, permitiendo potencialmente el acceso a traves de protocolos vulnerables.

[MEDIUM] Seguridad de Cookies: No se pudo confirmar la presencia de atributos de seguridad en las cookies, aumentando el riesgo de robo de sesiones.

[LOW] Archivo robots.txt: No se detecto el archivo de directrices para buscadores, lo que impide una gestion controlada de la indexacion del sitio.

[LOW] Archivo sitemap.xml: La falta de un mapa del sitio dificulta la correcta exploracion de la estructura web por parte de herramientas legiti-mas.