

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://cert-bienestarsocial.dipgra.es/login	Checks	9 pruebas
Dominio	cert-bienestarsocial.dipgra.es	Hallazgos	15 totales
Fecha	8 de septiembre de 2026 a las 08:06	Problemas	3 detectados

C

73/100

puntos de seguridad



RESUMEN EJECUTIVO

La auditoría de seguridad realizada sobre el portal web ha dado como resultado una puntuación de 73/100, obteniendo una calificación de C. El análisis constó de 9 checks pasivos, de los cuales uno resultó exitoso, se registró un fallo técnico y el resto presentaron errores de conexión que impidieron su verificación completa. Debido a la imposibilidad de confirmar la existencia de un cifrado SSL válido y cabeceras de seguridad esenciales, el sitio presenta un nivel de riesgo considerable. Se concluye que el sitio es actualmente vulnerable, especialmente en lo que respecta a la privacidad de los datos transmitidos en el formulario de acceso.

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 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

[CRITICO] Conexion SSL: El escáner no pudo establecer una conexión TLS/SSL cifrada, lo que sugiere que la comunicación entre el usuario y el servidor podría ser interceptada por terceros.

[BAJO] Archivo robots.txt: No fue posible acceder al archivo de configuración de rastreo, lo que afecta la gestión de indexación del sitio.

[BAJO] Archivo sitemap.xml: El mapa del sitio no está disponible o es inaccesible, dificultando la visibilidad de la estructura del portal para herramientas de mantenimiento y seguridad.

[ADVERTENCIA] Cabeceras de Seguridad: No se pudo verificar la presencia de directivas de protección contra ataques XSS o Clickjacking debido a errores en la respuesta del servidor.