EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://gestionempleado.igssgt.org	Checks	9 pruebas
Dominio	gestionempleado.igssgt.org	Hallazgos	13 totales
Fecha	11 de junio de 2026 a las 20:50	Problemas	1 detectados

A

100/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el portal gestionempleado.igssgt.org arroja una puntuación de 100/100 con una nota de calificación A. Durante la auditoría se ejecutaron un total de 9 checks pasivos, resultando 1 de ellos satisfactorio y no detectándose advertencias ni fallos en los parámetros evaluados. El sistema no muestra vulnerabilidades críticas expuestas en su configuración de red externa. En base a estos resultados, se concluye que el sitio web es seguro y mantiene una postura defensiva sólida. No se han encontrado brechas de seguridad que pongan en riesgo la integridad de la plataforma en este nivel de inspección.

Resumen de Riesgos

0	1	0	0	12
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

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
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

Redireccion HTTPS — 0/100

Estado: ERROR

No se pudo verificar la redireccion HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS

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 — Envio 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

[INFORMATIVO] Redirección HTTP: El servidor responde con un código HTTP 200 en lugar de redirigir automáticamente a HTTPS, lo que podría permitir conexiones no cifradas si no se gestiona manualmente.
[INFORMATIVO] Timeout de respuesta: Varios módulos de verificación pasiva excedieron el tiempo de espera de 15 segundos, lo que impide confirmar la presencia de cabeceras de seguridad específicas.
[INFORMATIVO] Puertos Abiertos: No se detectaron servicios adicionales expuestos, lo cual es positivo para reducir la superficie de ataque.