EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://hospigen.gob.gt	Checks	9 pruebas
Dominio	hospigen.gob.gt	Hallazgos	19 totales
Fecha	30 de marzo de 2026 a las 15:51	Problemas	3 detectados

F

37/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web https://hospigen.gob.gt ha resultado en una puntuación de 37/100, obteniendo una nota de F. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales solo 1 resultó exitoso, detectándose 2 fallos críticos relacionados con el cifrado y la estructura de indexación, además de múltiples errores de acceso a configuraciones de seguridad. La ausencia de un certificado SSL válido y la imposibilidad de verificar cabeceras de protección indican una infraestructura altamente expuesta. Se concluye que el sitio es actualmente vulnerable y no cumple con los estándares mínimos de seguridad para la protección de datos.

Resumen de Riesgos

1	0	0	2	16
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	0	FALLO	Certificado SSL no valido
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: FALLO

Certificado SSL no valido

- CRITICO **Certificado valido**
  El certificado SSL NO es valido
- INFO **Dias hasta expiracion**
  87 dias restantes (expira: 2026-06-25T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-07-18T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Redireccion HTTPS — 0/100

Estado: ERROR

No se pudo verificar la redireccion HTTPS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 302 redirige a https://hospigen.gob.gt/

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 — 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

[CRITICA] Certificado SSL no válido: El certificado SSL del sitio ha fallado la validación, lo que impide establecer una conexión cifrada y permite la interceptación de datos entre el usuario y el servidor.
[BAJA] Ausencia de robots.txt: No se pudo acceder al archivo robots.txt, lo que impide controlar el acceso de rastreadores y puede exponer directorios sensibles de forma involuntaria.
[BAJA] Ausencia de sitemap.xml: El archivo de mapa del sitio no está disponible o es inaccesible, dificultando la auditoría de la estructura técnica y la indexación del portal.
[ERROR] Cabeceras de seguridad no verificadas: No se pudieron validar cabeceras críticas como HSTS, X-Frame-Options o CSP, lo que sugiere una configuración de servidor que no protege contra ataques de clickjacking o inyección.
[ERROR] Seguridad de cookies no verificada: Al no detectarse la configuración de cookies, no se puede garantizar que los atributos Secure o HttpOnly estén activos para proteger las sesiones de los usuarios.