EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://cmsirrhh.igssgt.org/	Checks	9 pruebas
Dominio	cmsirrhh.igssgt.org	Hallazgos	29 totales
Fecha	11 de mayo de 2026 a las 15:44	Problemas	9 detectados

C

60/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio https://cmsirrhh.igssgt.org/ arroja una puntuación de 60/100 con una calificación de grado C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 3 resultaron satisfactorios y 2 presentaron fallos críticos relacionados con la configuración del servidor. A pesar de contar con un certificado SSL válido, la ausencia total de cabeceras de seguridad esenciales compromete la integridad de la plataforma. Se concluye que el sitio es actualmente vulnerable ante ataques comunes de interceptación e inyección de código.

Resumen de Riesgos

0	3	3	3	20
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 186 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion HTTPS
Deteccion CMS	0	ERROR	No se pudo analizar el CMS
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
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 — 100/100

Estado: OK

Certificado valido, expira en 186 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  186 dias restantes (expira: 2026-11-13T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-11-17T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: Kestrel — Revela tecnologia del servidor

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- MEDIO **X-Content-Type-Options**
  Falta — Evita MIME-type sniffing
- MEDIO **Referrer-Policy**
  Falta — Controla la informacion de referer enviada
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- INFO **Archivo /readme.html**
  No accesible (correcto)
- INFO **Archivo /README.txt**
  No accesible (correcto)
- INFO **Version CMS**
  No se detecta ninguna version expuesta

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  No encontrado (HTTP 404)
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

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

[HIGH] Content-Security-Policy: Falta — Al no estar implementada, el sitio queda expuesto a ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[HIGH] X-Frame-Options: Falta — La ausencia de esta cabecera permite que el sitio sea cargado en marcos (iframes), facilitando ataques de clickjacking.
[HIGH] Strict-Transport-Security: Falta — No se obliga al navegador a usar conexiones HTTPS mediante HSTS, permitiendo posibles ataques de degradación de SSL.
[MEDIUM] X-Content-Type-Options: Falta — Permite que el navegador realice MIME-sniffing, lo que puede derivar en la ejecución de archivos con contenido malicioso disfrazado.
[MEDIUM] Referrer-Policy: Falta — No se controla cuánta información de referencia se envía a otros dominios, lo que podría filtrar URLs internas sensibles.
[MEDIUM] Permissions-Policy: Falta — No se restringe el acceso a funciones del navegador como la cámara, el micrófono o la geolocalización desde el sitio.
[LOW] Server header expuesto: Server: Kestrel — El servidor revela explícitamente que utiliza tecnología Kestrel, facilitando a los atacantes la búsqueda de vulnerabilidades específicas para esa versión.
[LOW] robots.txt: No encontrado — El servidor responde con un error HTTP 404, lo que impide dar instrucciones claras a los motores de búsqueda sobre qué áreas no indexar.
[LOW] sitemap.xml: No encontrado — La falta de este archivo dificulta la auditoría de la estructura completa del sitio y su correcta indexación.