

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://hospitalsch.sisvent.duckdns.org/	Checks	9 pruebas
Dominio	hospitalsch.sisvent.duckdns.org	Hallazgos	47 totales
Fecha	6 de abril de 2026 a las 15:29	Problemas	8 detectados

B

77/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada sobre el dominio https://hospitalsch.sisvent.duckdns.org/ ha resultado en una puntuación de 77/100, lo que equivale a una nota B. Se ejecutaron un total de 9 checks pasivos, de los cuales 5 fueron exitosos, 2 generaron advertencias y 2 resultaron en fallos críticos. Aunque la infraestructura base presenta una configuración de cifrado sólida, existen deficiencias importantes en la gestión de sesiones y políticas de seguridad del navegador. El sitio se considera parcialmente vulnerable, requiriendo intervenciones técnicas inmediatas para alcanzar un nivel de seguridad óptimo.

Resumen de Riesgos

0 CRITICO	3 ALTO	2 MEDIO	3 BAJO	39 INFO
--------------	-----------	------------	-----------	------------

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 90 dias
Cabeceras de Seguridad	60	AVISO	4/6 presentes. Faltan: Content-Security-Policy, ...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
Deteccion CMS	100	OK	No se detecto un CMS conocido
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	33	FALLO	csrftoken: falta HttpOnly; csrftoken: falta Secu...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 90 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
90 dias restantes (expira: 2026-07-05T13:56:14.000Z)
- INFO Fecha de emision
Emitido desde: 2026-04-06T13:56:15.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 60/100

Estado: AVISO

4/6 presentes. Faltan: Content-Security-Policy, Permissions-Policy

- BAJO Server header expuesto
Server: openresty — Revela tecnologia del servidor

- ALTO

Content-Security-Policy
Falta — Previene XSS y ataques de inyeccion de contenido
- INFO

X-Frame-Options
Presente: DENY
- INFO

Strict-Transport-Security
Presente: max-age=63072000; preload
- INFO

X-Content-Type-Options
Presente: nosniff
- INFO

Referrer-Policy
Presente: same-origin
- MEDIO

Permissions-Policy
Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO

HTTP !' HTTPS redireccion
HTTP 301 redirige a https://hospitalsch.sisvent.duckdns.org/
- INFO

HSTS (Strict-Transport-Security)
HSTS activo: max-age=63072000; preload
- BAJO

HSTS includeSubDomains
HSTS no cubre subdominios
- INFO

HSTS max-age
max-age=63072000 (730 dias)
- INFO

Respuesta HTTPS
HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

No se detecto un CMS conocido

- INFO

WordPress
No detectado
- INFO

Joomla
No detectado
- INFO

Drupal
No detectado
- INFO

Magento
No detectado
- INFO

Shopify
No detectado
- INFO

PrestaShop
No detectado
- INFO

Wix
No detectado
- INFO

Squarespace
No detectado

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

Seguridad de Cookies — 33/100

Estado: FALLO

csrftoken: falta HttpOnly; csrftoken: falta Secure

- INFO

Cookies detectadas
1 cookie(s) encontrada(s)
- ALTO

Cookie: csrftoken — HttpOnly
Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO

Cookie: csrftoken — Secure
Falta flag Secure — Cookie se envía en conexiones HTTP
- INFO

Cookie: csrftoken — SameSite
SameSite=lax

Contenido Mixto — 100/100

Estado: OK

No se detecto contenido mixto

- INFO

Contenido mixto
Todos los recursos se cargan por HTTPS

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 política de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

- INFO

Puerto 21 (FTP)
Cerrado — Transferencia de archivos sin cifrar
- MEDIO

Puerto 22 (SSH)
ABIERTO — 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

- [HIGH] Cookie csrftoken sin flag HttpOnly: Permite que la cookie de sesión sea accesible mediante scripts, facilitando ataques de robo de sesión vía XSS.
- [HIGH] Cookie csrftoken sin flag Secure: La falta de este flag permite que la cookie se transmita por canales no cifrados si el usuario sale de HTTPS.
- [HIGH] Content-Security-Policy (CSP) faltante: La ausencia de esta política deja al sitio desprotegido contra ataques de inyección de código y Cross-Site Scripting.
- [MEDIUM] Permissions-Policy faltante: No se restringe el acceso del navegador a funciones sensibles como la cámara, el micrófono o la geolocalización.
- [MEDIUM] Puerto 22 (SSH) abierto: La exposición de este puerto permite intentos de acceso remoto por fuerza bruta contra el servidor.
- [LOW] Cabecera Server expuesta: Se revela el uso de openresty, lo que ayuda a un atacante a identificar vulnerabilidades específicas de esa tecnología.
- [LOW] Archivo robots.txt no encontrado: La ausencia de este archivo impide dar instrucciones adecuadas a los motores de búsqueda sobre la indexación.
- [LOW] Archivo sitemap.xml no encontrado: La falta de un mapa del sitio dificulta la correcta navegación y rastreo de los recursos legítimos de la web.