EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://sonysportmagic.com/	Checks	9 pruebas
Dominio	sonysportmagic.com	Hallazgos	47 totales
Fecha	14 de julio de 2026 a las 12:18	Problemas	12 detectados

C

64/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio sonysportmagic.com arroja una puntuación exacta de 64/100, lo que corresponde a una nota de C. De los 9 checks pasivos ejecutados, se obtuvieron 5 resultados satisfactorios, 2 advertencias y 2 fallos críticos relacionados con la configuración del servidor. Se detectó una ausencia total de cabeceras de seguridad esenciales y una gestión de cookies mejorable que expone a los usuarios a riesgos de suplantación. Debido a estas carencias técnicas, el sitio se considera vulnerable a ataques de inyección y redirecciones maliciosas.

Resumen de Riesgos

0	4	5	3	35
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 156 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	CMS detectado: Joomla
Version CMS Expuesta	20	FALLO	WordPress 3. expuesta
Seguridad de Cookies	67	AVISO	f28a44de84f4cdf0c8cd86611ba0cb62: falta SameSite
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 156 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  156 dias restantes (expira: 2026-12-17T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-06T00:00:00.000Z
- 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: Apache — 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.)

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://sonysportmagic.com/
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 503

Deteccion CMS — 100/100

Estado: OK

CMS detectado: Joomla

- INFO **WordPress**
  No detectado
- INFO **Joomla**
  Detectado via HTML body
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  No detectado
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: Joomla! - Open Source Content Management

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 3. expuesta

- INFO **Archivo /readme.html**
  No accesible (correcto)
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS

Seguridad de Cookies — 67/100

Estado: AVISO

f28a44de84f4cdf0c8cd86611ba0cb62: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: f28a44de84f4cdf0c8cd86611ba0cb62 — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: f28a44de84f4cdf0c8cd86611ba0cb62 — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: f28a44de84f4cdf0c8cd86611ba0cb62 — SameSite**
  Falta SameSite — Vulnerable a CSRF

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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (836 bytes)
- INFO **Reglas robots.txt**
  15 Disallow, 0 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **sitemap.xml**
  Presente, 11 URLs
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

2 puerto(s) abierto(s), todos esperados

- 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)**
  Abierto (esperado) — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Abierto (esperado) — 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 — Previene XSS y ataques de inyeccion de contenido.
[HIGH] X-Frame-Options: Falta — Protege contra clickjacking al evitar que el sitio se cargue en frames externos.
[HIGH] Strict-Transport-Security: Falta — No se fuerza el uso de HTTPS mediante HSTS, permitiendo posibles degradaciones de conexión.
[HIGH] HSTS (Strict-Transport-Security): HSTS no configurado — El navegador no está instruido para forzar siempre conexiones seguras.
[MEDIUM] X-Content-Type-Options: Falta — No se evita el MIME-type sniffing, lo que podría permitir la ejecución de archivos maliciosos.
[MEDIUM] Referrer-Policy: Falta — No se controla la cantidad de información de referencia enviada a otros sitios.
[MEDIUM] Permissions-Policy: Falta — No hay restricciones sobre el uso de APIs del navegador como cámara o micrófono.
[MEDIUM] Cookie f28a44de84f4cdf0c8cd86611ba0cb62: Falta SameSite — La ausencia de este atributo hace al sitio vulnerable a ataques de falsificación de solicitud en sitios cruzados (CSRF).
[MEDIUM] Archivo /README.txt: Archivo accesible publicamente — Este archivo puede revelar la versión exacta y detalles técnicos del CMS WordPress 3 detectado.
[LOW] Server header expuesto: Server: Apache — Revela la tecnología y potencialmente la versión del servidor, facilitando el reconocimiento a atacantes.
[LOW] Meta generator: Joomla! - Open Source Content Management — Expone públicamente el CMS utilizado para la gestión del sitio.
[LOW] Ruta sensible en robots.txt: Referencia a admin — Facilita a posibles atacantes la localización de paneles de administración o rutas privadas.
[INFO] Respuesta HTTPS: El servidor responde con un estado 503, lo que indica una indisponibilidad temporal o error de configuración en el servicio.