EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.grupomedos.com/erpsystem/	Checks	9 pruebas
Dominio	www.grupomedos.com	Hallazgos	41 totales
Fecha	11 de junio de 2026 a las 15:17	Problemas	12 detectados

D

53/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web ha dado como resultado una puntuación de 53/100, obteniendo una calificación de nota D. Durante la auditoría se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios y 4 presentaron fallos críticos de configuración. A pesar de contar con un cifrado SSL válido, la carencia absoluta de cabeceras de seguridad y la falta de redirección automática a HTTPS exponen el sitio a riesgos evitables. La infraestructura actual no implementa medidas defensivas básicas contra ataques de interceptación o inyección. Por todo ello, se concluye que el sitio es actualmente vulnerable y requiere una intervención técnica prioritaria para elevar sus estándares de protección.

Resumen de Riesgos

0	5	4	3	29
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 72 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a HTTPS
Deteccion CMS	100	OK	No se detecto un CMS conocido
Version CMS Expuesta	20	FALLO	WordPress 2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto 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 72 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  72 dias restantes (expira: 2026-08-22T20:36:18.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-24T20:36:19.000Z
- 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: nginx/1.27.2 — 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 — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- 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 — 20/100

Estado: FALLO

WordPress 2 expuesta

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

Seguridad de Cookies — 100/100

Estado: OK

No se encontraron cookies

- INFO **Cookies detectadas**
  El sitio no establece cookies en la respuesta inicial

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 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] Fallo en Redirección HTTPS: El servidor no redirige el tráfico HTTP hacia HTTPS, permitiendo conexiones no cifradas propensas a la interceptación de datos.
[HIGH] Ausencia de Strict-Transport-Security: No se configura HSTS, por lo que el navegador no fuerza la conexión segura en visitas sucesivas.
[HIGH] Ausencia de Content-Security-Policy: Falta de control sobre los recursos que el navegador puede cargar, facilitando ataques de Cross-Site Scripting (XSS).
[HIGH] Ausencia de X-Frame-Options: El sitio no indica si puede ser embebido en marcos, lo que permite ataques de Clickjacking.
[MEDIUM] Ausencia de X-Content-Type-Options: El servidor no previene el sniffing de tipos MIME, lo que podría derivar en la ejecución de archivos maliciosos.
[MEDIUM] Ausencia de Referrer-Policy: No existe control sobre la información que se envía en la cabecera Referer al navegar hacia enlaces externos.
[MEDIUM] Ausencia de Permissions-Policy: No se restringe el acceso a funciones sensibles del navegador como la cámara, el micrófono o la geolocalización.
[MEDIUM] Exposición de archivo readme.html: Se detectó acceso público a un archivo que sugiere el uso de WordPress 2, revelando información técnica innecesaria.

[LOW] Cabecera Server expuesta: Se revela la tecnología y versión exacta del servidor (nginx/1.27.2), facilitando la búsqueda de exploits específicos.
[LOW] Ausencia de robots.txt y sitemap.xml: El servidor devuelve un error 404 para estos archivos, dificultando la gestión de indexación y seguridad por diseño.