EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://erp-prod.meda.team	Checks	9 pruebas
Dominio	erp-prod.meda.team	Hallazgos	51 totales
Fecha	22 de mayo de 2026 a las 23:27	Problemas	9 detectados

B

78/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del dominio erp-prod.meda.team arroja una puntuación de 78/100 con una calificación de nota B. Se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 3 presentaron advertencias y 1 falló debido a deficiencias en las cabeceras de seguridad. La ausencia de un pentest activo limita la visibilidad sobre vulnerabilidades lógicas de la aplicación, centrándose este informe en la configuración del servidor y el cifrado. En su estado actual, el sitio se considera moderadamente seguro pero vulnerable a ataques de inyección y secuestro de sesiones por configuraciones omitidas.

Resumen de Riesgos

0	4	2	3	42
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 300 dias
Cabeceras de Seguridad	30	FALLO	Solo 2/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
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	83	AVISO	XSRF-TOKEN: falta HttpOnly
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 300 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  300 dias restantes (expira: 2027-03-18T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-17T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 30/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, Strict-Transport-Security, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: nginx/1.22.1 — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.2.31 — Revela framework/lenguaje
- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- INFO **X-Content-Type-Options**
  Presente: nosniff
- 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://erp-prod.meda.team:443/
- 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
- INFO **Tecnologias detectadas**
  PHP/8.2.31

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 — 83/100

Estado: AVISO

XSRF-TOKEN: falta HttpOnly

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- ALTO **Cookie: XSRF-TOKEN — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: XSRF-TOKEN — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: XSRF-TOKEN — SameSite**
  SameSite=lax
- INFO **Cookie: meda_session — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: meda_session — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: meda_session — 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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (24 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- 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

[ALTA] Falta de Content-Security-Policy: La ausencia de esta cabecera facilita ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[ALTA] Falta de Strict-Transport-Security: Sin la directiva HSTS, el sitio es susceptible a ataques de degradación de protocolo y secuestro de cookies en conexiones inseguras.
[ALTA] Cookie XSRF-TOKEN sin atributo HttpOnly: Esta omisión permite que scripts maliciosos accedan al token de seguridad, aumentando el riesgo de robo de identidad.
[MEDIA] Falta de Referrer-Policy: No se controla la información de origen enviada a terceros, lo que podría filtrar datos sensibles presentes en las URLs.
[MEDIA] Falta de Permissions-Policy: El navegador no tiene restricciones sobre el uso de APIs como la cámara o el micrófono, ampliando la superficie de ataque potencial.
[BAJA] Exposición de cabecera Server: Se revela el uso de nginx/1.22.1, lo que permite a un atacante identificar vulnerabilidades específicas para esa versión del software.
[BAJA] Exposición de cabecera X-Powered-By: El servidor divulga que utiliza PHP/8.2.31, facilitando el perfilado tecnológico del entorno para ataques dirigidos.
[BAJA] Falta de sitemap.xml: La ausencia de este archivo dificulta la correcta auditoría de rutas y puede ser indicativo de una configuración de servidor incompleta.