

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://inventario-tic-edemsa-mzjbqbya3-jos24.vercel.app/login	Checks	9 pruebas
Dominio	inventario-tic-edemsa-mzjbqbya3-jos24.vercel.app	Hallazgos	45 totales
Fecha	7 de septiembre de 2026 a las 20:26	Problemas	11 detectados

B

80/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web ha arrojado una puntuación de 80/100, lo que equivale a una calificación de nota B. Se ejecutaron un total de 9 chequeos pasivos, obteniendo resultados satisfactorios en 7 de ellos y detectando fallos en 2 categorías críticas. El sitio demuestra una implementación sólida de cifrado SSL y redirección HTTPS, garantizando la privacidad de los datos en tránsito. Sin embargo, debido a la ausencia casi total de cabeceras de seguridad y la exposición de rutas sensibles, el sitio se considera vulnerable a ataques de inyección y suplantación de identidad.

Resumen de Riesgos

0	2	8	1	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 81 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
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	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	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 81 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
81 dias restantes (expira: 2026-11-27T19:48:08.000Z)
- INFO Fecha de emision
Emitido desde: 2026-08-29T19:48:09.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 20/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO Server header expuesto
Server: Vercel — 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
- INFO

Strict-Transport-Security
Presente: max-age=63072000; includeSubDomains; preload
- 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 — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO

HTTP !' HTTPS redireccion
HTTP 308 redirige a https://inventario-tic-edemsa-mzjbqbya3-jos24.vercel.app/
- INFO

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

HSTS includeSubDomains
HSTS 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

- MEDIO

Archivo /readme.html
Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO

Archivo /README.txt
Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO

Ruta /wp-login.php
Panel de login accesible publicamente

- MEDIO

Ruta /administrator/
Panel de login accesible publicamente
- MEDIO

Ruta /user/login
Panel de login accesible publicamente
- INFO

Version CMS
No se detecta ninguna version expuesta

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

- INFO

security.txt
Presente en /.well-known/security.txt — Buena practica

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: La ausencia de esta cabecera permite la ejecución de scripts maliciosos y ataques de inyección de contenido (XSS).

[HIGH] X-Frame-Options: Al no estar presente, el sitio es susceptible a ataques de clickjacking donde un atacante puede cargar la web en un marco invisible.

[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el MIME-type sniffing, lo que podría llevar a la ejecución de archivos con contenido inesperado.

[MEDIUM] Referrer-Policy: No existe control sobre la información de referencia enviada a otros sitios, lo que puede filtrar URLs internas.

[MEDIUM] Permissions-Policy: No se restringe el uso de APIs del navegador como cámara o micrófono, aumentando la superficie de exposición.

[MEDIUM] Archivos /readme.html y /README.txt: Estos archivos son accesibles públicamente y pueden revelar información técnica sobre la construcción del sitio.

[MEDIUM] Rutas administrativas expuestas (/wp-login.php, /administrator, /user/login): La visibilidad de estos paneles facilita intentos de acceso no autorizados mediante fuerza bruta.

[LOW] Cabecera de servidor expuesta: El servidor revela el uso de Vercel, proporcionando pistas a posibles atacantes sobre la infraestructura subyacente.

[LOW] Ausencia de robots.txt y sitemap.xml: La falta de estos archivos impide una gestión adecuada de la indexación y visibilidad del sitio.