EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://jew-ia.vercel.app/	Checks	9 pruebas
Dominio	jew-ia.vercel.app	Hallazgos	45 totales
Fecha	16 de abril de 2026 a las 23:26	Problemas	11 detectados

B

80/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado ha otorgado una puntuación de 80/100, lo que representa una nota B en la escala de cumplimiento. Se ejecutaron un total de 9 checks pasivos, obteniendo 7 resultados satisfactorios y 2 fallos relacionados con la configuración de cabeceras y archivos de sistema. A pesar de contar con una implementación robusta de SSL y redirección HTTPS, la ausencia de protecciones contra ataques de inyección y clickjacking eleva el perfil de riesgo. El sitio web se considera moderadamente seguro, aunque presenta vulnerabilidades críticas en su configuración de seguridad que deben ser atendidas para evitar explotaciones comunes.

Resumen de Riesgos

0	2	8	1	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 40 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 40 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  40 dias restantes (expira: 2026-05-27T06:28:02.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-26T06:28:03.000Z
- 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://jew-ia.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: Falta esta cabecera fundamental, lo que permite la ejecución de scripts maliciosos y ataques de inyección de contenido XSS.

[HIGH] X-Frame-Options: La ausencia de esta directiva facilita ataques de clickjacking, permitiendo que el sitio sea embebido en marcos externos fraudulentos.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el MIME-type sniffing, lo que puede llevar al navegador a interpretar archivos de forma insegura.
[MEDIUM] Referrer-Policy: No existe control sobre la información de procedencia enviada en las peticiones, pudiendo filtrar datos sensibles a otros dominios.
[MEDIUM] Permissions-Policy: No se restringe el acceso a APIs del navegador, permitiendo potencialmente el uso no autorizado de funciones como la cámara o el micrófono.
[MEDIUM] Archivos informativos expuestos: El acceso público a /readme.html y /README.txt revela detalles técnicos que facilitan el reconocimiento por parte de atacantes.
[MEDIUM] Paneles de gestión accesibles: Se detectó acceso público a rutas como /wp-login.php, /administrator/ y /user/login, aumentando el riesgo de ataques de fuerza bruta.
[LOW] Server header expuesto: El encabezado Server: Vercel revela la tecnología subyacente, permitiendo ataques dirigidos basados en vulnerabilidades de la plataforma.
[LOW] Ausencia de archivos de indexación: La falta de robots.txt y sitemap.xml indica una carencia en la gestión de visibilidad y estructura del sitio.