EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://emergencyvalladolid.net	Checks	9 pruebas
Dominio	emergencyvalladolid.net	Hallazgos	45 totales
Fecha	17 de agosto de 2026 a las 21:02	Problemas	8 detectados

B

80/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio emergencyvalladolid.net arroja una puntuación de 80/100 con una calificación final de B. Durante el proceso se ejecutaron un total de 9 checks pasivos, de los cuales 7 resultaron satisfactorios y 2 presentaron fallos críticos en la configuración de cabeceras y archivos de indexación. A pesar de contar con un cifrado SSL robusto y una correcta redirección HTTPS, la ausencia de políticas de seguridad en el servidor expone a los usuarios a riesgos vectoriales. No se realizó un pentest activo, por lo que el análisis se limita a la superficie de exposición pública inmediata. En conclusión, el sitio se considera mayoritariamente seguro en su infraestructura base, pero vulnerable ante ataques de inyección y suplantación de interfaz.

Resumen de Riesgos

0	2	3	3	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 39 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 39 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  39 dias restantes (expira: 2026-09-26T02:35:13.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-28T02:35:14.000Z
- 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: Netlify — 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=31536000
- 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 301 redirige a https://emergencyvalladolid.net/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 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
- INFO **Tecnologias detectadas**
  React, Next.js

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 — 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

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 no autorizados, facilitando ataques de XSS e inyección de contenido malicioso.

[HIGH] X-Frame-Options: Al no estar implementada, el sitio puede ser cargado dentro de marcos externos, lo que facilita ataques de secuestro de clics o clickjacking.
[MEDIUM] X-Content-Type-Options: La falta de esta política permite que el navegador intente adivinar el tipo de contenido, abriendo la puerta a ataques de sniffing de tipo MIME.
[MEDIUM] Referrer-Policy: No se controla la cantidad de información que el navegador envía al seguir enlaces externos, lo que podría filtrar datos de navegación privados.
[MEDIUM] Permissions-Policy: No se restringen las capacidades del navegador como la cámara o el micrófono, permitiendo que potenciales scripts maliciosos intenten acceder a estas funciones.
[LOW] Server header expuesto: Se detectó el valor Server: Netlify, lo cual facilita a un atacante identificar la tecnología subyacente para buscar exploits específicos.
[LOW] robots.txt: La ausencia de este archivo dificulta la gestión de rastreadores y no establece límites claros sobre qué directorios no deben ser indexados.
[LOW] sitemap.xml: No se encontró un mapa del sitio, lo cual afecta la visibilidad en motores de búsqueda y la organización estructural de la información pública.