EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://alerta13.com/	Checks	9 pruebas
Dominio	alerta13.com	Hallazgos	50 totales
Fecha	5 de agosto de 2026 a las 01:57	Problemas	9 detectados

B

80/100

puntos de seguridad

RESUMEN EJECUTIVO

El sitio web alerta13.com ha obtenido una puntuación de seguridad de 80/100 con una calificación de nota B. Durante el análisis se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 2 generaron advertencias y 1 fue identificado como fallo crítico. Si bien el sitio cuenta con un cifrado SSL robusto y redirecciones correctas, la exposición de versiones específicas del software y la falta de cabeceras de seguridad incrementan el riesgo. El sitio se considera moderadamente seguro, pero es vulnerable a ataques de reconocimiento y posibles exploits dirigidos debido a la visibilidad de su infraestructura interna.

Resumen de Riesgos

0	2	3	4	41
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 59 dias
Cabeceras de Seguridad	60	AVISO	4/6 presentes. Faltan: Content-Security-Policy, ...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
Deteccion CMS	100	OK	CMS detectado: WordPress
Version CMS Expuesta	20	FALLO	WordPress 7.0.2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	60	AVISO	1 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 59 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  59 dias restantes (expira: 2026-10-03T04:41:03.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-07-05T04:41:04.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 60/100

Estado: AVISO

4/6 presentes. Faltan: Content-Security-Policy, Permissions-Policy

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

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.2.32 — Revela framework/lenguaje
- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: no-referrer-when-downgrade
- 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://alerta13.com/
- 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

CMS detectado: WordPress

- INFO **WordPress**
  Detectado via HTML body
- 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
- BAJO **Meta generator**
  Expone: WordPress 7.0.2
- INFO **Tecnologias detectadas**
  Next.js, PHP/8.2.32

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 7.0.2 expuesta

- ALTO **WordPress version**
  Version 7.0.2 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- INFO **Archivo /readme.html**
  No accesible (correcto)
- INFO **Archivo /README.txt**
  No accesible (correcto)
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente

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 — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://+52295913388

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (113 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://alerta13.com/wp-sitemap.xml
- 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] WordPress version: La versión 7.0.2 se encuentra expuesta públicamente, lo que facilita a atacantes la búsqueda y ejecución de exploits para CVEs conocidos.
[HIGH] Content-Security-Policy: La ausencia de esta cabecera permite que el sitio sea más susceptible a ataques de Cross-Site Scripting (XSS) e inyecciones de contenido malicioso.
[MEDIUM] Permissions-Policy: No existen restricciones sobre el uso de APIs del navegador, dejando abierta la posibilidad de acceso no autorizado a funciones como la cámara o el micrófono.
[MEDIUM] Ruta /wp-login.php: El panel de acceso administrativo es visible para cualquier usuario, permitiendo intentos de intrusión mediante ataques de fuerza bruta.
[MEDIUM] Recurso HTTP (Contenido Mixto): Se detectó un enlace de hoja de estilo o referencia (http://+52295913388) que viaja por un canal no cifrado.
[LOW] Server header expuesto: El servidor revela el uso de nginx, lo que ayuda a los atacantes a perfilar las tecnologías utilizadas en la infraestructura.
[LOW] X-Powered-By expuesto: La cabecera revela el uso de PHP/8.2.32, proporcionando información técnica valiosa para ataques dirigidos al lenguaje de programación.
[LOW] Meta generator: La etiqueta meta en el código fuente expone directamente que el sitio utiliza WordPress 7.0.2.
[LOW] Ruta sensible en robots.txt: El archivo incluye una referencia directa a directorios de administración que facilita el mapeo del sitio por parte de bots maliciosos.