EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.grupheracles.com	Checks	9 pruebas
Dominio	www.grupheracles.com	Hallazgos	44 totales
Fecha	24 de abril de 2026 a las 18:14	Problemas	12 detectados

C

68/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio web presenta una puntuación de 68/100, lo que equivale a una calificación de nota C. Durante la evaluación se ejecutaron un total de 9 controles pasivos, resultando en 5 verificaciones satisfactorias, 2 advertencias y 2 fallos críticos. Se detectó una carencia total de cabeceras de seguridad esenciales y la exposición de un puerto de comunicaciones sensible. Debido a la combinación de configuraciones faltantes y servicios expuestos, se concluye que el sitio es actualmente vulnerable ante diversos vectores de ataque.

Resumen de Riesgos

0	5	3	4	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 314 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 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	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	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 21 (FTP)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 314 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  314 dias restantes (expira: 2027-03-04T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-02T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: Microsoft-IIS/10.0 — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: ASP.NET — Revela framework/lenguaje
- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://www.grupheracles.com/
- 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**
  Next.js, ASP.NET

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 — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 21 (FTP)

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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 Inteligencia Artificial

---RESUMEN EJECUTIVO---
El análisis de seguridad realizado al sitio web presenta una puntuación de 68/100, lo que equivale a una calificación de nota C. Durante la evaluación se ejecutaron un total de 9 controles pasivos, resultando en 5 verificaciones satisfactorias, 2 advertencias y 2 fallos críticos. Se detectó una carencia total de cabeceras de seguridad esenciales y la exposición de un puerto de comunicaciones sensible. Debido a la combinación de configuraciones faltantes y servicios expuestos, se concluye que el sitio es actualmente vulnerable ante diversos vectores de ataque.

---VULNERABILITIES---

[HIGH] Puerto 21 (FTP): El puerto de transferencia de archivos está abierto, lo que permite el intercambio de datos potencialmente sin cifrado y facilita ataques de fuerza bruta.
[HIGH] Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de ataques de Cross-Site Scripting (XSS) y la inyección de contenido malicioso.
[HIGH] X-Frame-Options: Al no estar configurada, el sitio es susceptible a ataques de clickjacking donde un atacante puede camuflar la interfaz bajo un marco transparente.
[HIGH] Strict-Transport-Security: La falta de HSTS permite que un atacante intente degradar la conexión del usuario de HTTPS a HTTP para interceptar datos.
[MEDIUM] X-Content-Type-Options: El navegador podría intentar adivinar el tipo de contenido, facilitando la ejecución de archivos maliciosos mediante MIME-sniffing.
[MEDIUM] Referrer-Policy: No existe control sobre la información de navegación que se comparte con sitios externos al hacer clic en enlaces.
[MEDIUM] Permissions-Policy: El servidor no restringe el acceso de las APIs del navegador a componentes de hardware o funciones de privacidad del usuario.
[LOW] Server header expuesto: La cabecera revela el uso de Microsoft-IIS/10.0, proporcionando información técnica específica que ayuda a un atacante a planificar exploits.
[LOW] X-Powered-By expuesto: El encabezado indica que el sitio utiliza el framework ASP.NET, limitando la seguridad por oscuridad y exponiendo la tecnología subyacente.
[LOW] Ausencia de robots.txt y sitemap.xml: La falta de estos archivos dificulta el control del rastreo por parte de buscadores y la auditoría de la estructura del sitio.