EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.chateagratis.net/	Checks	9 pruebas
Dominio	www.chateagratis.net	Hallazgos	47 totales
Fecha	26 de mayo de 2026 a las 05:44	Problemas	8 detectados

C

71/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado sobre el sitio web arroja una puntuación de 71/100, lo que equivale a una calificación de grado C. Se ejecutaron un total de 9 comprobaciones pasivas, de las cuales 6 resultaron satisfactorias, 1 generó una advertencia y 2 fueron calificadas como fallos críticos. Aunque el sitio posee un certificado SSL válido, existen deficiencias importantes en la configuración de cabeceras de seguridad y en la gestión del tráfico cifrado. La exposición de puertos alternativos y de versiones de software específicas incrementa la superficie de ataque. En su estado actual, el sitio se considera vulnerable debido a la falta de mecanismos proactivos de defensa contra ataques de inyección y la ausencia de redirección forzada a protocolos seguros.

Resumen de Riesgos

0	2	4	2	39
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 72 dias
Cabeceras de Seguridad	50	FALLO	Solo 3/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a HTTPS
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	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 72 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  72 dias restantes (expira: 2026-08-06T01:35:00.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-08T00:35:04.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 50/100

Estado: FALLO

Solo 3/6 presentes. Faltan: Content-Security-Policy, Referrer-Policy, Permissions-Policy

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

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.3.31 — 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=2592000; includeSubDomains
- INFO **X-Content-Type-Options**
  Presente: nosniff
- MEDIO **Referrer-Policy**
  Falta — Controla la informacion de referer enviada
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=2592000; includeSubDomains
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- MEDIO **HSTS max-age**
  max-age=2592000 (30 dias) — Recomendado minimo 180 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**
  Next.js, Astro, PHP/8.3.31

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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (156 bytes)
- INFO **Reglas robots.txt**
  0 Disallow, 0 Allow
- INFO **Sitemap en robots.txt**
  https://www.chateagratis.net/sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- 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
- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
  Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[HIGH] HTTP a HTTPS redireccion: El servidor no redirige automáticamente las conexiones inseguras a HTTPS, permitiendo que los usuarios naveguen sin cifrado.
[HIGH] Content-Security-Policy: La ausencia de esta cabecera impide prevenir ataques de Cross-Site Scripting (XSS) e inyecciones de contenido malicioso.
[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La presencia de este puerto expone un servidor web alternativo o proxy que podría ser explotado si no está debidamente protegido.
[MEDIUM] HSTS max-age insuficiente: El tiempo de persistencia de la política de seguridad estricta es de solo 30 días, por debajo de los 180 días recomendados por los estándares internacionales.
[MEDIUM] Referrer-Policy: Falta la cabecera que controla cuánta información de procedencia se envía a otros sitios al hacer clic en enlaces.
[MEDIUM] Permissions-Policy: No se han definido restricciones para el uso de APIs del navegador, como el acceso a la cámara, micrófono o geolocalización.
[LOW] X-Powered-By expuesto: El encabezado revela explícitamente el uso de PHP/8.3.31, facilitando a un atacante la búsqueda de exploits específicos para esa versión.
[LOW] Server header expuesto: Se confirma el uso de Cloudflare, lo que proporciona pistas sobre la infraestructura y la tecnología de red utilizada.