EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.gamesgx.net/	Checks	9 pruebas
Dominio	www.gamesgx.net	Hallazgos	44 totales
Fecha	15 de mayo de 2026 a las 04:57	Problemas	8 detectados

B

75/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web ha arrojado una puntuación de 75/100, lo que equivale a una calificación de nota B. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 2 generaron advertencias y 2 fueron marcados como fallos. Si bien el sitio presenta una base sólida en cuanto a cifrado de datos, existen deficiencias críticas en la configuración de cabeceras de seguridad y exposición de información del servidor. En conclusión, el sitio es moderadamente seguro, pero se considera vulnerable a ataques de suplantación de interfaz y explotación de versiones de software obsoletas.

Resumen de Riesgos

0	1	5	2	36
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 55 dias
Cabeceras de Seguridad	45	FALLO	Solo 2/6 presentes. Faltan: X-Frame-Options, X-C...
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	20	FALLO	WordPress 2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta robots.txt
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 55 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  55 dias restantes (expira: 2026-07-09T05:59:56.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-10T05:00:03.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 45/100

Estado: FALLO

Solo 2/6 presentes. Faltan: X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

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

- BAJO **X-Powered-By expuesto**
  X-Powered-By: - — Revela framework/lenguaje
- INFO **Content-Security-Policy**
  Presente: object-src 'none', object-src 'none'
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- INFO **Strict-Transport-Security**
  Presente: max-age=15768000;includeSubdomains, max-age=15768000;includeSubdomains, max-age=...
- 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://www.gamesgx.net/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=15768000;includeSubdomains, max-age=15768000;includeSubdomains, max-age=31536000;, max-age=31536000;
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=15768000 (183 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, -

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 2 expuesta

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS

- INFO **Archivo /README.txt**
  No accesible (correcto)

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 — 60/100

Estado: AVISO

Falta robots.txt

- INFO **sitemap.xml**
  Presente, ? URLs
- 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] X-Frame-Options: La falta de esta cabecera permite que el sitio sea embebido en otros portales, facilitando ataques de clickjacking para engañar a los usuarios.
[MEDIUM] X-Content-Type-Options: Al no estar presente, el navegador puede intentar interpretar el contenido de forma distinta al tipo MIME declarado, lo que permite la ejecución de scripts maliciosos.

[MEDIUM] Referrer-Policy: No se detectó esta cabecera, lo que provoca que información sensible de la URL de origen pueda filtrarse a dominios externos.
[MEDIUM] Permissions-Policy: La ausencia de esta directiva impide restringir el uso de APIs del navegador, como la cámara o geolocalización, en el contexto del sitio.
[MEDIUM] Archivo /readme.html expuesto: Este archivo es accesible públicamente y revela el uso de WordPress 2, una versión antigua que facilita a los atacantes identificar vulnerabilidades conocidas.
[MEDIUM] Puerto 8080 (HTTP-Alt) ABIERTO: La exposición de este puerto alternativo aumenta la superficie de ataque al dejar disponible un servicio web o proxy potencialmente vulnerable.
[LOW] Server header expuesto: El servidor revela el uso de Cloudflare, proporcionando información técnica que puede ser utilizada para dirigir ataques específicos.
[LOW] X-Powered-By expuesto: Se detectó esta cabecera que revela el framework o lenguaje de programación subyacente del servidor.
[LOW] Falta de robots.txt: El sitio no cuenta con este archivo, lo que impide dar instrucciones claras a los rastreadores sobre qué directorios no deben ser indexados.