EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://orion.gtahub.gg/	Checks	9 pruebas
Dominio	orion.gtahub.gg	Hallazgos	44 totales
Fecha	17 de mayo de 2026 a las 02:15	Problemas	12 detectados

C

68/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web arroja una puntuación de 68/100, lo que equivale a una nota de C. Se ejecutaron 9 checks pasivos, resultando en 5 verificaciones exitosas, 2 advertencias y 2 fallos críticos en la configuración del servidor. El sitio web presenta deficiencias significativas en la implementación de políticas de seguridad modernas y exposición de información técnica innecesaria. Con base en estos hallazgos, el sitio se clasifica actualmente como vulnerable ante ataques de interceptación y manipulación de contenido en el lado del cliente.

Resumen de Riesgos

0	4	4	4	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 51 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): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 51 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  51 dias restantes (expira: 2026-07-07T10:08:17.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-08T09:08:33.000Z
- 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: cloudflare — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: Express — 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://orion.gtahub.gg/
- 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**
  Express

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): 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] Content-Security-Policy: Falta esta cabecera, lo cual es peligroso porque permite ataques de inyección de contenido y Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options: La ausencia de esta política permite que el sitio sea cargado en marcos externos, facilitando ataques de clickjacking.
[HIGH] Strict-Transport-Security: No está configurada, permitiendo que un atacante intente degradar la conexión del usuario de HTTPS a HTTP.

[MEDIUM] Puerto 8080 (HTTP-Alt): El puerto se encuentra abierto, lo que representa un vector de ataque adicional al exponer un servicio web alternativo o proxy.
[MEDIUM] X-Content-Type-Options: Falta esta cabecera, permitiendo que los navegadores realicen sniffing de tipos MIME y ejecuten archivos maliciosos disfrazados.
[MEDIUM] Referrer-Policy: No está definida, lo que puede causar la fuga de información sensible en las URLs de origen hacia sitios externos.
[MEDIUM] Permissions-Policy: La falta de esta cabecera impide restringir el acceso del navegador a funciones sensibles como la cámara, el micrófono o la geolocalización.
[LOW] Server header expuesto: Revela el uso de Cloudflare, proporcionando pistas sobre la infraestructura a potenciales atacantes.
[LOW] X-Powered-By expuesto: Indica el uso del framework Express, permitiendo ataques dirigidos a vulnerabilidades específicas de dicha tecnología.
[LOW] robots.txt y sitemap.xml: La ausencia de estos archivos dificulta la auditoría de indexación y puede indicar una falta de mantenimiento en la estructura pública.