

Escanear Vulnerabilidades

Informe de Seguridad Web

URL: https://login.gtahub.gg/
Dominio: login.gtahub.gg
Fecha: 17 de mayo de 2026 a las 02:13

Checks: 9 pruebas
Hallazgos: 45 totales
Problemas: 7 detectados

B

81/100

puntos de seguridad

RESUMEN EJECUTIVO

El sitio web analizado presenta una puntuación de 81/100, lo que le otorga una calificación de nota B. Tras ejecutar 9 checks pasivos, se han obtenido 6 resultados satisfactorios, 1 advertencia y 2 fallos relacionados con la configuración de cabeceras y archivos de indexación. No se ha realizado un pentest activo, por lo que el análisis se limita a la superficie de exposición externa y la configuración del servidor. Aunque el cifrado de datos es excelente, la ausencia de directivas de seguridad en el navegador representa un riesgo para los usuarios finales. En conclusión, el sitio es mayormente seguro en su transporte de datos, pero vulnerable a ataques de inyección y suplantación de interfaz.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 51 dias
Cabeceras de Seguridad	45	FALLO	Solo 3/6 presentes. Faltan: Content-Security-Pol...
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	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 — 45/100

Estado: FALLO

Solo 3/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Permissions-Policy

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

- **ALTO** **Content-Security-Policy**
Falta — Previene XSS y ataques de inyección de contenido
- **ALTO** **X-Frame-Options**
Falta — Protege contra clickjacking
- **INFO** **Strict-Transport-Security**
Presente: max-age=15552000; includeSubDomains
- **INFO** **X-Content-Type-Options**
Presente: nosniiff
- **INFO** **Referrer-Policy**
Presente: no-referrer
- **MEDIO** **Permissions-Policy**
Falta — Restringe APIs del navegador (camara, micro, etc.)

Redirección HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- **INFO** **HTTP !' HTTPS redirección**
HTTP 301 redirige a https://login.gtahub.gg/
- **INFO** **HSTS (Strict-Transport-Security)**
HSTS activo: max-age=15552000; includeSubDomains
- **BAJO** **HSTS includeSubDomains**
HSTS cubre subdominios
- **INFO** **HSTS max-age**
max-age=15552000 (180 días)
- **INFO** **Respuesta HTTPS**
HTTPS responde con status 200

Detección CMS — 100/100

Estado: OK

No se detectó 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** **Tecnologías detectadas**
Next.js

Version CMS Expuesta — 100/100

Estado: OK

No se detectó versión 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: La ausencia de esta cabecera permite la ejecución de ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.

[HIGH] X-Frame-Options: Al no estar presente, el sitio es susceptible a ataques de clickjacking, donde un atacante puede cargar la web en un marco invisible para engañar al usuario.

[MEDIUM] Permissions-Policy: Falta de restricciones sobre las APIs del navegador, lo que permite potencialmente el uso no autorizado de funciones como la cámara, micrófono o geolocalización.

[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La exposición de este servidor web alternativo puede ser utilizada para explotar servicios de administración o proxies no protegidos.

[LOW] Server header expuesto: El servidor revela que utiliza tecnología Cloudflare, facilitando la fase de reconocimiento para un posible atacante.

[LOW] robots.txt no encontrado: La falta de este archivo impide gestionar correctamente el comportamiento de los rastreadores en áreas sensibles del sitio.

[LOW] sitemap.xml no encontrado: La ausencia de un mapa del sitio dificulta la auditoría de la estructura del portal y su correcta indexación.