

Escanear Vulnerabilidades

Informe de Seguridad Web

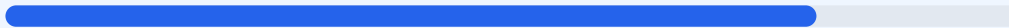
URL https://www.quantumgold.net
Dominio www.quantumgold.net
Fecha 18 de mayo de 2026 a las 09:56

Checks 9 pruebas
Hallazgos 45 totales
Problemas 8 detectados

B

80/100

puntos de seguridad



RESUMEN EJECUTIVO

La evaluación de seguridad de la plataforma arroja una puntuación de 80/100 con una calificación de grado B. El análisis consistió en 9 checks pasivos, de los cuales 7 resultaron satisfactorios y 2 presentaron fallos críticos en la configuración de directivas de seguridad. Se observa una implementación sólida en el cifrado de datos y transporte, pero una ausencia total de protecciones contra ataques de inyección y suplantación en el lado del cliente. Debido a estas omisiones en las cabeceras de seguridad, el sitio se considera vulnerable a ataques específicos del navegador a pesar de su buen puntaje general.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 60 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 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	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 60 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
60 dias restantes (expira: 2026-07-17T16:36:14.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-04-18T16:36:15.000Z
- INFO **Puerto 443**
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 20/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

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

- **ALTO** **Content-Security-Policy**
Falta — Previene XSS y ataques de inyeccion de contenido
- **ALTO** **X-Frame-Options**
Falta — Protege contra clickjacking
- **INFO** **Strict-Transport-Security**
Presente: max-age=63072000
- **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 308 redirige a https://www.quantumgold.net/
- **INFO** **HSTS (Strict-Transport-Security)**
HSTS activo: max-age=63072000
- **BAJO** **HSTS includeSubDomains**
HSTS no cubre subdominios
- **INFO** **HSTS max-age**
max-age=63072000 (730 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**
React, Next.js

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 — 100/100

Estado: OK

2 puerto(s) abierto(s), todos esperados

- 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
- INFO **Puerto 8080 (HTTP-Alt)**
Cerrado — 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 ejecucion de scripts no autorizados, facilitando ataques de Cross-Site Scripting (XSS) e inyeccion de datos.

[HIGH] X-Frame-Options: Al no estar presente, el sitio puede ser embebido en marcos de otras webs, lo que expone a los usuarios a ataques de robo de clics o clickjacking.

[MEDIUM] X-Content-Type-Options: La falta de esta directiva permite que el navegador intente adivinar el tipo de contenido, lo que podría derivar en la ejecución de archivos maliciosos disfrazados.

[MEDIUM] Referrer-Policy: No se controla la información de procedencia enviada a otros dominios, lo que podría filtrar rutas internas o datos de navegación sensibles.

[MEDIUM] Permissions-Policy: No se restringe el acceso a APIs sensibles del navegador como la cámara o el micrófono, dejando la privacidad del usuario a merced del navegador.

[LOW] Server header expuesto: La cabecera revela el uso de Vercel, proporcionando información técnica que un atacante podría usar para buscar vulnerabilidades específicas de esa plataforma.

[LOW] robots.txt: La inexistencia de este archivo dificulta el control sobre qué partes del sitio deben ser indexadas por los motores de búsqueda.

[LOW] sitemap.xml: No se encuentra un mapa del sitio, lo cual afecta la transparencia estructural y la correcta navegación de los rastreadores web.