EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://yoanlopez500-wq.github.io/aliance-hub/index.html	Checks	9 pruebas
Dominio	yoanlopez500-wq.github.io	Hallazgos	42 totales
Fecha	22 de junio de 2026 a las 03:25	Problemas	10 detectados

C

65/100

puntos de seguridad

RESUMEN EJECUTIVO

Este informe técnico detalla los resultados de la auditoría de seguridad realizada al sitio web, obteniendo una puntuación exacta de 65/100 y una calificación de grado C. El análisis consistió en 9 checks pasivos, de los cuales 6 resultaron satisfactorios y 3 presentaron fallos críticos o informativos. Debido a la ausencia de cabeceras de seguridad fundamentales y problemas en la redirección de tráfico, se concluye que el sitio es actualmente vulnerable a ataques comunes de la web. Es imperativo abordar las deficiencias en la capa de transporte y las políticas de seguridad del navegador para mitigar riesgos de interceptación y explotación de vulnerabilidades.

Resumen de Riesgos

0	4	3	3	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 73 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 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	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 73 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  73 dias restantes (expira: 2026-09-02T23:26:06.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-04T23:26:07.000Z
- 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: GitHub.com — 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=31556952
- 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 — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 404 — No redirige a HTTPS
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 404

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

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

[LOW] Server header expuesto: Revela el uso de GitHub.com, lo que proporciona información técnica que un atacante puede usar para dirigir ataques específicos contra la infraestructura.
[HIGH] Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de scripts maliciosos, aumentando el riesgo de ataques Cross-Site Scripting (XSS) e inyecciones de contenido.
[HIGH] X-Frame-Options: Al no estar configurada, el sitio es vulnerable a ataques de clickjacking, permitiendo que un tercero cargue la página en un marco oculto para engañar a los usuarios.
[MEDIUM] X-Content-Type-Options: Falta la directiva nosniff, lo que permite que el navegador realice MIME-type sniffing y ejecute archivos con formatos incorrectos o maliciosos.
[MEDIUM] Referrer-Policy: La falta de control sobre la información de referencia puede filtrar datos sensibles de la URL del sitio hacia dominios externos.

[MEDIUM] Permissions-Policy: No se restringe el acceso a APIs del navegador como la cámara o el micrófono, dejando abierta la posibilidad de abuso de estas funciones por parte de scripts de terceros.
[HIGH] Redireccion HTTPS: El sitio no redirige automáticamente las peticiones HTTP inseguras a la versión cifrada HTTPS, devolviendo un error 404 en la solicitud de prueba.
[HIGH] HSTS (Strict-Transport-Security): Al no estar configurado, el navegador no recuerda forzar siempre la conexión segura, facilitando ataques de degradación de protocolo y robo de sesiones.
[LOW] Archivos de indexación faltantes: No se encontraron robots.txt ni sitemap.xml, lo que dificulta la gestión adecuada del rastreo por parte de motores de búsqueda.