EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://aqua-gas-oeebb.ondigitalocean.app/b2b/login	Checks	9 pruebas
Dominio	aqua-gas-oeebb.ondigitalocean.app	Hallazgos	47 totales
Fecha	17 de mayo de 2026 a las 04:25	Problemas	10 detectados

C

72/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado en la plataforma arroja una puntuación de 72/100, lo que representa una calificación de grado C. Se ejecutaron un total de 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 1 generó una advertencia y 2 fueron identificados como fallos críticos. Aunque la base de cifrado y gestión de cookies es sólida, la ausencia total de cabeceras de protección en el servidor compromete la integridad del sitio. Se concluye que el sitio es vulnerable ante ataques dirigidos al navegador del usuario, como inyección de scripts y secuestro de clics. Es imperativo aplicar las correcciones de configuración recomendadas para mitigar riesgos de explotación inmediata.

Resumen de Riesgos

0	3	4	3	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 42 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 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	1 cookies, todas con flags correctos
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 42 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  42 dias restantes (expira: 2026-06-28T03:41:14.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-30T02:41:21.000Z
- 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

- 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 — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://aqua-gas-oeebb.ondigitalocean.app/
- 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 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

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

1 cookies, todas con flags correctos

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: __cf_bm — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: __cf_bm — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: __cf_bm — SameSite**
  SameSite=none

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 es fundamental para prevenir ataques de XSS y la inyección de contenido malicioso.
[HIGH] X-Frame-Options: Falta — Su ausencia permite que el sitio sea cargado en marcos externos, facilitando ataques de clickjacking.
[HIGH] Strict-Transport-Security: Falta — No se fuerza el uso de HSTS, lo que podría permitir ataques de degradación de protocolo (downgrade).
[MEDIUM] X-Content-Type-Options: Falta — Permite que el navegador ignore el tipo de contenido enviado, abriendo la puerta a ataques de MIME-sniffing.
[MEDIUM] Referrer-Policy: Falta — No se controla la información de procedencia enviada en las peticiones, lo que puede filtrar datos sensibles de la URL.
[MEDIUM] Permissions-Policy: Falta — El sitio no restringe el acceso a funciones sensibles del navegador como la cámara o el micrófono.
[MEDIUM] Puerto 8080 (HTTP-Alt): ABIERTO — La presencia de un puerto de servidor alternativo abierto aumenta la superficie de ataque y exposición de servicios.
[LOW] Server header expuesto: Server: cloudflare — Revelar la tecnología del servidor ayuda a los atacantes a buscar vulnerabilidades específicas del proveedor.
[LOW] robots.txt: No encontrado — La ausencia de este archivo dificulta la gestión del rastreo por parte de motores de búsqueda.
[LOW] sitemap.xml: No encontrado — La falta de un mapa del sitio impide una indexación estructurada y profesional del contenido web.