

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://bit.ly/p126n	Checks	9 pruebas
Dominio	bit.ly	Hallazgos	43 totales
Fecha	24 de marzo de 2026 a las 04:48	Problemas	8 detectados

B

76/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad del sitio web arroja una puntuación exacta de 76/100, lo que corresponde a una nota B. Se ejecutaron 9 checks pasivos, de los cuales 7 resultaron satisfactorios y 2 presentaron fallos críticos relacionados con la configuración de seguridad del servidor y archivos de indexación. El cifrado de datos es sólido, pero la ausencia total de cabeceras de protección expone a los usuarios a riesgos de inyección y suplantación. Los resultados indican que, aunque la base técnica es estable, el sitio es vulnerable ante ataques dirigidos al navegador del cliente. En conclusión, el estado actual requiere correcciones inmediatas en las políticas de seguridad para alcanzar un nivel de protección profesional.

Resumen de Riesgos

0	3	3	2	35
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 170 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	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 170 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
170 dias restantes (expira: 2026-09-09T23:59:59.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-02-24T00:00:00.000Z
- 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 302 redirige a https://bitly.com/
- INFO

HSTS (Strict-Transport-Security)
HSTS activo: max-age=31536000
- BAJO

HSTS includeSubDomains
HSTS no cubre subdominios
- INFO

HSTS max-age
max-age=31536000 (365 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

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

sitemap.xml
Error al acceder
- 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: Falta esta cabecera esencial para prevenir ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[HIGH] X-Frame-Options: Al no estar presente, el sitio es vulnerable a ataques de clickjacking donde un atacante puede cargar la web en un marco invisible.
[HIGH] Strict-Transport-Security: La ausencia de HSTS impide que el navegador fuerce siempre una conexión segura, facilitando ataques de degradación de protocolo.
[MEDIUM] X-Content-Type-Options: El sitio no previene el MIME-type sniffing, lo que podría permitir al navegador ejecutar archivos con contenido malicioso disfrazado.

[MEDIUM] Referrer-Policy: No existe control sobre la información de navegación que se envía a otros sitios, lo que puede comprometer la privacidad de los usuarios.

[MEDIUM] Permissions-Policy: No se restringen las APIs del navegador, permitiendo potencialmente el acceso no autorizado a funciones como la cámara o el micrófono.

[LOW] Server header expuesto: El encabezado revela el uso de Cloudflare, proporcionando información valiosa a un atacante sobre la infraestructura del servidor.

[LOW] sitemap.xml: El archivo de mapa del sitio no es accesible, lo que dificulta la auditoría de rutas y la indexación correcta de los contenidos.