EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://bitods.com/	Checks	9 pruebas
Dominio	bitods.com	Hallazgos	48 totales
Fecha	18 de abril de 2026 a las 01:17	Problemas	11 detectados

C

69/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web arroja una puntuación exacta de 69/100, lo que equivale a una nota de C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 4 resultaron satisfactorios, 3 generaron advertencias y 2 fueron calificados como fallos críticos. A pesar de contar con un certificado SSL válido y una gestión adecuada de contenidos mixtos, se detectaron deficiencias significativas en las cabeceras de seguridad y en la configuración de las cookies de sesión. Debido a la ausencia de políticas contra ataques de inyección y la exposición de puertos no estándar, se concluye que el sitio es actualmente vulnerable.

Resumen de Riesgos

0	4	5	2	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 45 dias
Cabeceras de Seguridad	30	FALLO	Solo 2/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
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	33	FALLO	JSESSIONID: falta Secure; JSESSIONID: falta Same...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 45 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  45 dias restantes (expira: 2026-06-01T19:31:52.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-03T19:31:53.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 30/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, Strict-Transport-Security, 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
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- INFO **X-Content-Type-Options**
  Presente: nosniff
- MEDIO **Referrer-Policy**
  Falta — Controla la informacion de referer enviada
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://bitods.com/
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- 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**
  Next.js, Nuxt

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 — 33/100

Estado: FALLO

JSESSIONID: falta Secure; JSESSIONID: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: JSESSIONID — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: JSESSIONID — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: JSESSIONID — SameSite**
  Falta SameSite — Vulnerable a CSRF

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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (1738 bytes)
- INFO **Reglas robots.txt**
  9 Disallow, 1 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- 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 indispensable para prevenir ataques XSS y la inyección de contenido malicioso en el navegador.
[HIGH] Strict-Transport-Security: No está configurada, lo que impide que el sitio fuerce conexiones HTTPS seguras mediante HSTS.
[HIGH] Cookie: JSESSIONID (Falta flag Secure): La cookie de sesión se envía sobre conexiones HTTP no cifradas, permitiendo el robo de credenciales en redes no seguras.
[MEDIUM] Cookie: JSESSIONID (Falta SameSite): La ausencia de este atributo hace que el sitio sea vulnerable a ataques de falsificación de solicitud entre sitios (CSRF).
[MEDIUM] Puerto 8080 (HTTP-Alt): El puerto se encuentra abierto, lo que representa una superficie de ataque adicional por el uso de servicios web alternativos o proxies.
[MEDIUM] Referrer-Policy: Falta esta cabecera para controlar cuánta información de procedencia se comparte con otros dominios al navegar.
[MEDIUM] Permissions-Policy: No se han restringido las APIs del navegador, permitiendo potencialmente el acceso no autorizado a periféricos como cámara o micrófono.
[MEDIUM] Bloqueo total en robots.txt: El archivo bloquea el rastreo de todo el sitio mediante la directiva Disallow: /, afectando la indexación legítima.
[LOW] Server header expuesto: Se revela el uso de la tecnología Cloudflare, facilitando información sobre la infraestructura a posibles atacantes.
[LOW] sitemap.xml: El archivo de mapa del sitio no fue encontrado (404), dificultando la auditoría de rutas y la navegación de motores de búsqueda.