EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.infobae.com/	Checks	9 pruebas
Dominio	www.infobae.com	Hallazgos	46 totales
Fecha	19 de mayo de 2026 a las 13:25	Problemas	5 detectados

B

89/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado a la plataforma arroja una puntuación exacta de 89/100, lo que representa una nota B según los estándares de auditoría. Se ejecutaron 9 checks pasivos, resultando 8 de ellos satisfactorios y solo 1 con fallos críticos en la configuración de cabeceras de seguridad. La infraestructura muestra una implementación sólida de cifrado y redirecciones, garantizando la integridad de la conexión inicial. Sin embargo, la falta de directivas de protección en el lado del cliente genera vectores de ataque conocidos. Se concluye que el sitio es mayoritariamente seguro, pero vulnerable a ataques de manipulación de interfaz y fuga de metadatos técnicos.

Resumen de Riesgos

0	1	3	1	41
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 82 dias
Cabeceras de Seguridad	45	FALLO	Solo 2/6 presentes. Faltan: X-Frame-Options, X-C...
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	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 82 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  82 dias restantes (expira: 2026-08-09T04:17:55.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-11T04:17:56.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 45/100

Estado: FALLO

Solo 2/6 presentes. Faltan: X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

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

- INFO **Content-Security-Policy**
  Presente: upgrade-insecure-requests; media-src https: blob:; child-src https: blob:; defau...
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; includeSubDomains; preload
- 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://www.infobae.com/america/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000; includeSubDomains; preload
- BAJO **HSTS includeSubDomains**
  HSTS 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
- INFO **Tecnologias detectadas**
  React, Astro

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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (1360 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- INFO **Sitemap en robots.txt**
  https://www.infobae.com/arc/outboundfeeds/sitemap2/
- 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] X-Frame-Options: La cabecera no está configurada, lo que permite que el sitio sea embebido en iframes externos facilitando ataques de clickjacking.
[MEDIUM] X-Content-Type-Options: La ausencia de esta directiva permite que el navegador realice sniffing de tipos MIME, lo que podría derivar en la ejecución de scripts maliciosos disfrazados de otros archivos.
[MEDIUM] Referrer-Policy: Al no estar definida, no se controla la información de referencia enviada a sitios de terceros, pudiendo exponer datos de navegación privados.
[MEDIUM] Permissions-Policy: No existe una política que restrinja el acceso de las APIs del navegador a funciones de hardware, permitiendo potencialmente el uso no autorizado de sensores o periféricos.
[LOW] Server header expuesto: El encabezado Server revela el uso de openresty, proporcionando información técnica innecesaria que ayuda a los atacantes en la fase de reconocimiento.