

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://alma1938.com/
Dominio alma1938.com
Fecha 18 de junio de 2026 a las 01:23

Checks 9 pruebas
Hallazgos 45 totales
Problemas 7 detectados

B

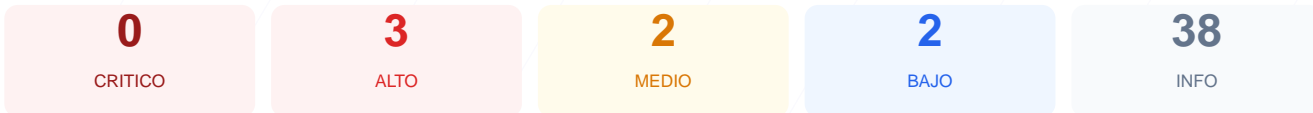
77/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado al dominio ha resultado en una puntuación exacta de 77/100, lo que le otorga una nota final de B. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 6 finalizaron correctamente, 2 generaron advertencias y 1 fue calificado como un fallo de seguridad. Aunque el sitio posee un cifrado de transporte válido, presenta deficiencias críticas en la implementación de políticas de redirección y cabeceras de endurecimiento. Por lo tanto, se concluye que el sitio es moderadamente vulnerable a ataques de interceptación y reconocimiento de infraestructura.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 64 dias
Cabeceras de Seguridad	80	AVISO	5/6 presentes. Faltan: Strict-Transport-Security
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	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 64 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
64 dias restantes (expira: 2026-08-20T21:59:46.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-05-22T21:02:51.000Z
- INFO **Puerto 443**
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 80/100

Estado: AVISO

5/6 presentes. Faltan: Strict-Transport-Security

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

- INFO **Content-Security-Policy**
Presente: default-src 'none'; script-src 'nonce-Kaw58dnaq8uDaRu8lbrZqz' 'unsafe-eval' http...
- INFO **X-Frame-Options**
Presente: SAMEORIGIN
- ALTO **Strict-Transport-Security**
Falta — Fuerza conexiones HTTPS (HSTS)
- INFO **X-Content-Type-Options**
Presente: nosniiff
- INFO **Referrer-Policy**
Presente: same-origin
- INFO **Permissions-Policy**
Presente: accelerometer=(),camera=(),clipboard-read=(),clipboard-write=(),geolocation=(),g...

Redireccion HTTPS — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
HTTP 403 — No dirige a HTTPS
- ALTO **HSTS (Strict-Transport-Security)**
HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
HTTPS responde con status 403

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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
Presente (427 bytes)
- INFO **Reglas robots.txt**
11 Disallow, 1 Allow
- MEDIO **Bloqueo total**
robots.txt bloquea todo el sitio con Disallow: /
- BAJO **Ruta sensible en robots.txt**
Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
<https://alma1938.com/sitemap.xml>
- 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

[ALTA] Redirección HTTP a HTTPS: El sitio no redirige automáticamente las peticiones inseguras a la versión cifrada, devolviendo un error 403.

[ALTA] HSTS (Strict-Transport-Security) ausente: La falta de esta cabecera impide que el navegador fuerce conexiones seguras, permitiendo ataques de degradación de protocolo.

[MEDIA] Puerto 8080 (HTTP-Alt) abierto: Se detectó un puerto alternativo accesible que suele utilizarse para servicios de administración o proxies, aumentando la superficie de ataque.

[MEDIA] Bloqueo total en robots.txt: El archivo está configurado para evitar que cualquier buscador indexe el contenido, lo cual puede indicar una configuración errónea o incompleta.

[BAJA] Server header expuesto: La respuesta del servidor revela el uso de Cloudflare, proporcionando información técnica a potenciales atacantes sobre la infraestructura.

[BAJA] Ruta sensible en robots.txt: Se hace referencia explícita a la ruta admin, facilitando el descubrimiento de paneles de gestión a entidades maliciosas.