EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.afirme.com/afirme	Checks	9 pruebas
Dominio	www.afirme.com	Hallazgos	86 totales
Fecha	11 de mayo de 2026 a las 04:02	Problemas	13 detectados

B

86/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web ha arrojado una puntuación de 86/100, lo que equivale a una nota B. Se ejecutaron un total de 9 comprobaciones pasivas, de las cuales 6 resultaron satisfactorias, 2 generaron advertencias y 1 fue calificada como fallo debido a la presencia de contenido mixto. Aunque el sitio demuestra una implementación sólida en su cifrado de transporte y redirecciones, existen debilidades importantes en la configuración de cabeceras de seguridad y en la protección de cookies de sesión. Concluimos que el sitio es mayormente seguro en su infraestructura básica, pero se encuentra en un estado vulnerable ante ataques de manipulación de sesiones y degradación de protocolos.

Resumen de Riesgos

0	1	11	1	73
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 306 dias
Cabeceras de Seguridad	75	AVISO	4/6 presentes. Faltan: Referrer-Policy, Permissi...
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	86	AVISO	dtCookie: falta HttpOnly; f5avraaaaaaaaaaaaaaaa_...
Contenido Mixto	20	FALLO	5 recursos HTTP en pagina HTTPS
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 306 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  306 dias restantes (expira: 2027-03-12T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-09T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 75/100

Estado: AVISO

4/6 presentes. Faltan: Referrer-Policy, Permissions-Policy

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

- INFO **Content-Security-Policy**
  Presente: default-src 'self' wss://widget-mediator.zopim.com/ https://www.linkedin.com htt...
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; includeSubDomains; preload
- 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 — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 302 redirige a https://www.afirme.com/
- 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**
  Next.js

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)

- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente
- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 86/100

Estado: AVISO

dtCookie: falta HttpOnly; f5avraaaaaaaaaaaaaaaa_session_: falta SameSite; TS014f6dad: falta SameSite; TS01582c3d: falta SameSite; TS01e7b11a: falta SameSite

- INFO **Cookies detectadas**
  12 cookie(s) encontrada(s)
- ALTO **Cookie: dtCookie — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: dtCookie — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: dtCookie — SameSite**
  SameSite=lax
- INFO **Cookie: JSESSIONID — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: JSESSIONID — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: JSESSIONID — SameSite**
  SameSite=lax
- INFO **Cookie: NEW_VISITOR — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: NEW_VISITOR — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: NEW_VISITOR — SameSite**
  SameSite=lax
- INFO **Cookie: VISITOR — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: VISITOR — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: VISITOR — SameSite**
  SameSite=lax
- INFO **Cookie: BIGipServer~PRD_www.afirme.com~POOL_PRD_www.afirme.com — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: BIGipServer~PRD_www.afirme.com~POOL_PRD_www.afirme.com — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: BIGipServer~PRD_www.afirme.com~POOL_PRD_www.afirme.com — SameSite**
  SameSite=lax
- INFO **Cookie: f5avraaaaaaaaaaaaaaaa_session_ — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: f5avraaaaaaaaaaaaaaaa_session_ — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: f5avraaaaaaaaaaaaaaaa_session_ — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: TS014f6dad — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: TS014f6dad — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: TS014f6dad — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: TS01582c3d — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: TS01582c3d — Secure**
  Flag Secure activo — Solo se envia por HTTPS

- MEDIO **Cookie: TS01582c3d — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: TS01e7b11a — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: TS01e7b11a — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: TS01e7b11a — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: TS01dc4fc6 — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: TS01dc4fc6 — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: TS01dc4fc6 — SameSite**
  SameSite=strict
- INFO **Cookie: TS01cb0e56 — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: TS01cb0e56 — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: TS01cb0e56 — SameSite**
  SameSite=strict
- INFO **Cookie: TS01749371 — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: TS01749371 — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: TS01749371 — SameSite**
  SameSite=strict

Contenido Mixto — 20/100

Estado: FALLO

5 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.afirme.com/Personas/TDC.html
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.afirme.com/Personas/Inversiones.html
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.afirme.com/Seguridad-y-Prevenci-n-de-Fraudes.html
- MEDIO **href (link/stylesheet)**
  ...y 2 mas del mismo tipo

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (219 bytes)
- INFO **Reglas robots.txt**
  4 Disallow, 0 Allow
- INFO **Sitemap en robots.txt**
  https://www.afirme.com/sitemap.xml
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

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] Cookie dtCookie sin bandera HttpOnly: La falta de esta bandera permite que la cookie sea accesible mediante scripts del lado del cliente, elevando el riesgo de robo de sesión vía ataques XSS.
[MEDIUM] Contenido mixto detectado: Se identificaron 5 recursos cargados mediante el protocolo inseguro HTTP dentro de la página HTTPS, lo que permite ataques de intermediario y debilita la integridad del cifrado.
[MEDIUM] Cookies sin atributo SameSite: Las cookies de sesión y control (f5avra, TS014f) carecen de este atributo, lo que hace al usuario vulnerable a ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] Falta de cabecera Referrer-Policy: El sitio no instruye al navegador sobre cuánta información de referencia debe enviarse al navegar hacia otros enlaces, comprometiendo potencialmente la privacidad.
[MEDIUM] Falta de cabecera Permissions-Policy: No se restringe el uso de APIs del navegador como la cámara o el micrófono, permitiendo que potenciales scripts maliciosos intenten acceder a estas funciones.
[MEDIUM] Ruta /wp-login.php expuesta: Se detectó un panel de acceso público que, aunque no se identifique un CMS específico, representa un punto de entrada para intentos de fuerza bruta.
[LOW] Exposición de cabecera Server: El servidor revela el uso de la tecnología volt-adc, proporcionando información técnica que facilita a un atacante la búsqueda de vulnerabilidades específicas para dicho software.