EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://aw-technology.com/	Checks	9 pruebas
Dominio	aw-technology.com	Hallazgos	41 totales
Fecha	14 de julio de 2026 a las 23:00	Problemas	8 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad del sitio web ha resultado en una puntuación de 73/100, lo que equivale a una nota C. Se realizaron 9 checks pasivos, obteniendo 5 resultados satisfactorios, 2 advertencias por configuraciones incompletas y 2 fallos críticos en la arquitectura de seguridad. A pesar de contar con un cifrado de transporte robusto, la ausencia de cabeceras defensivas y la exposición de puertos no estándar comprometen la integridad técnica. En conclusión, el sitio se considera vulnerable a ataques de interceptación y manipulación de contenido debido a la falta de políticas de seguridad activa en el servidor.

Resumen de Riesgos

0	3	3	2	33
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 60 dias
Cabeceras de Seguridad	25	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	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	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 60 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  60 dias restantes (expira: 2026-09-13T08:15:14.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-15T07:17:51.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 25/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, Strict-Transport-Security, X-Content-Type-Options, 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)
- MEDIO **X-Content-Type-Options**
  Falta — Evita MIME-type sniffing
- INFO **Referrer-Policy**
  Presente: same-origin
- 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://aw-technology.com/
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 526

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**
  No encontrado (HTTP 526)
- 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 (CSP) faltante: La ausencia de esta política permite la ejecución de scripts no autorizados y ataques de inyección de contenido (XSS).
[HIGH] Strict-Transport-Security (HSTS) no configurado: El servidor no obliga al navegador a usar conexiones seguras, permitiendo ataques de degradación de protocolo.
[MEDIUM] X-Content-Type-Options faltante: Esta omisión permite que el navegador realice MIME-sniffing, lo que podría llevar a la ejecución de archivos maliciosos disfrazados de contenido legítimo.
[MEDIUM] Permissions-Policy faltante: No se restringe el uso de funciones sensibles del navegador, como la ubicación o la cámara, aumentando el riesgo de privacidad para el usuario.
[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La visibilidad de este puerto sugiere la presencia de servicios de administración o proxies que podrían ser un vector de entrada para atacantes.
[LOW] Cabecera de servidor expuesta: El campo Server revela el uso de Cloudflare, lo cual facilita la fase de reconocimiento técnico a un actor malintencionado.
[LOW] Archivos robots.txt y sitemap.xml ausentes: La falta de estos archivos y la respuesta de error 526 indican una configuración deficiente en la estructura pública y la indexación del sitio.