

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://attarreal.com	Checks	9 pruebas
Dominio	attarreal.com	Hallazgos	43 totales
Fecha	20 de septiembre de 2026 a las 15:52	Problemas	10 detectados

C

61/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web ha arrojado una puntuación de 61/100, lo que resulta en una calificación de nota C. Durante la evaluación, se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 1 presentó advertencias y 2 fallaron de manera crítica. A pesar de contar con un certificado SSL válido, el sitio presenta deficiencias estructurales en la implementación de cabeceras de seguridad y en la gestión de protocolos de transporte. Se concluye que el sitio es vulnerable debido a la falta de protecciones esenciales contra ataques comunes de interceptación e inyección.

Resumen de Riesgos

0 CRITICO	5 ALTO	4 MEDIO	1 BAJO	33 INFO
--------------	-----------	------------	-----------	------------

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 87 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
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 87 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
87 dias restantes (expira: 2026-12-16T10:15:21.000Z)
- INFO Fecha de emision
Emitido desde: 2026-09-17T09:15:38.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, 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
- ALTO

X-Frame-Options
Falta — Protege contra clickjacking
- ALTO

Strict-Transport-Security
Falta — Fuerza conexiones HTTPS (HSTS)
- 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 — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO

HTTP !' HTTPS redireccion
HTTP 200 — No redirige a HTTPS
- 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

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 (67 bytes)
- INFO

Reglas robots.txt
0 Disallow, 1 Allow
- INFO

Sitemap en robots.txt
<https://attarreal.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

[HIGH] Redireccion HTTP a HTTPS: El sitio permite conexiones no cifradas (HTTP 200) sin redirigir al usuario automáticamente a una conexión segura, lo que facilita el robo de datos.

[HIGH] Strict-Transport-Security: La cabecera HSTS no está configurada, por lo que el navegador no obliga a utilizar conexiones HTTPS, permitiendo ataques de degradación de seguridad.

[HIGH] Content-Security-Policy: La ausencia de esta cabecera deja al sitio expuesto a ataques de Cross-Site Scripting (XSS) y de inyección de contenido malicioso.

[HIGH] X-Frame-Options: Al no estar presente, el sitio es susceptible a ataques de clickjacking donde un atacante puede cargar la web en un marco invisible para engañar al usuario.

[MEDIUM] Puerto 8080 (HTTP-Alt): Se detectó este puerto abierto, lo cual aumenta la superficie de ataque al exponer un servidor web alternativo o proxy que podría ser explotado.

[MEDIUM] X-Content-Type-Options: La falta de esta instrucción permite que los navegadores intenten adivinar el tipo de contenido, lo que puede derivar en la ejecución de scripts maliciosos.

[MEDIUM] Referrer-Policy: No existe un control sobre la información de navegación que se comparte con otros sitios al hacer clic en enlaces externos.

[MEDIUM] Permissions-Policy: El sitio no restringe el acceso a APIs sensibles del navegador como la cámara, el micrófono o la ubicación.

[LOW] Server header expuesto: La cabecera revela que se utiliza Cloudflare, proporcionando información técnica valiosa para un atacante en su fase de reconocimiento.