EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.astaragroup.com	Checks	9 pruebas
Dominio	www.astaragroup.com	Hallazgos	35 totales
Fecha	20 de abril de 2026 a las 01:38	Problemas	8 detectados

C

71/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada sobre el dominio astaragroup.com ha resultado en una puntuación de 71/100, lo que equivale a una nota de C. Durante el análisis se ejecutaron 9 checks pasivos, de los cuales 4 resultaron satisfactorios, 1 generó una advertencia y 1 se marcó como fallo crítico en la configuración de cabeceras. Aunque el sitio cuenta con un cifrado de transporte robusto, presenta carencias importantes en las políticas de seguridad del lado del cliente y en la gestión de contenidos mixtos. Debido a la ausencia de protecciones contra ataques de inyección y clickjacking, se concluye que el sitio es actualmente vulnerable. Es necesario mitigar los hallazgos para evitar riesgos de explotación por parte de actores externos.

Resumen de Riesgos

0	2	4	2	27
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 37 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
Deteccion CMS	100	OK	CMS detectado: WordPress
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	60	AVISO	1 recurso(s) HTTP en pagina HTTPS
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 37 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  37 dias restantes (expira: 2026-05-27T05:13:08.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-26T05:13:09.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 20/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: Apache — 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

- INFO **Strict-Transport-Security**
  Presente: max-age=63072000; includeSubdomains;
- 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.)

Deteccion CMS — 100/100

Estado: OK

CMS detectado: WordPress

- INFO **WordPress**
  Detectado via HTML body
- 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
- BAJO **Meta generator**
  Expone: WordPress 6.9.4
- INFO **Tecnologias detectadas**
  Next.js

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 — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://wa.me/+51981092824

Puertos Abiertos — 100/100

Estado: OK

No se detectaron puertos abiertos

- 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)**
  Cerrado — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Cerrado — 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] Content-Security-Policy: Falta — La ausencia de esta cabecera permite ataques de Cross-Site Scripting (XSS) e inyección de código malicioso.
[HIGH] X-Frame-Options: Falta — El sitio no restringe su carga en marcos, lo que facilita ataques de secuestro de clics o clickjacking.
[MEDIUM] Contenido Mixto: Se detectó un recurso HTTP (enlace a wa.me) en una página HTTPS, lo cual compromete la integridad del sitio y la confianza del navegador.
[MEDIUM] X-Content-Type-Options: Falta — Al no estar configurada, el navegador puede intentar interpretar archivos como un tipo MIME diferente, facilitando ataques de ejecución de scripts.
[MEDIUM] Referrer-Policy: Falta — No se controla cuánta información de referencia se envía al navegar hacia otros enlaces, lo que podría exponer datos de la URL.
[MEDIUM] Permissions-Policy: Falta — El sitio no limita el acceso del navegador a funciones sensibles como la cámara o el micrófono mediante políticas explícitas.
[LOW] Server header expuesto: La cabecera revela el uso de Apache, proporcionando información técnica que ayuda a un atacante a buscar vulnerabilidades específicas.
[LOW] Meta generator: Se expone la versión WordPress 6.9.4, una versión antigua que permite a terceros identificar fallos de seguridad conocidos para esa distribución.