EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://atalayaguard.com/audit/gobeo	Checks	9 pruebas
Dominio	atalayaguard.com	Hallazgos	41 totales
Fecha	3 de agosto de 2026 a las 12:10	Problemas	11 detectados

D

57/100

puntos de seguridad

RESUMEN EJECUTIVO

Tras realizar la auditoría de seguridad, el sitio web ha obtenido una puntuación de 57/100, lo que resulta en una nota de calificación D. Se han ejecutado un total de 9 checks pasivos, de los cuales 5 resultaron satisfactorios, se emitió 1 advertencia y 3 finalizaron en fallo crítico. A pesar de contar con un certificado SSL válido, la configuración del servidor presenta carencias graves en la protección de la sesión y en la defensa contra ataques de inyección. Debido a la ausencia total de cabeceras de seguridad y la falta de redirección forzada a HTTPS, se concluye que el sitio es actualmente vulnerable y requiere una intervención técnica inmediata.

Resumen de Riesgos

0	5	4	2	30
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 72 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	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 72 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  72 dias restantes (expira: 2026-10-14T19:45:52.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-07-16T18:45:55.000Z
- 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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- 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: La ausencia de esta cabecera permite la ejecución de scripts maliciosos y ataques de inyección de contenido (XSS).
[HIGH] X-Frame-Options: La falta de esta directiva expone el sitio a ataques de clickjacking, permitiendo que sea cargado en marcos externos no autorizados.
[HIGH] Strict-Transport-Security: No se ha configurado HSTS, lo que impide que el navegador fuerce conexiones seguras y facilita ataques de degradación de protocolo.
[HIGH] Redirección HTTPS: El servidor permite el acceso mediante el protocolo HTTP sin redirigir al usuario a la versión segura HTTPS.
[MEDIUM] X-Content-Type-Options: La falta de esta configuración permite el sniffing de tipos MIME, lo que podría derivar en la ejecución de archivos con contenido malicioso disfrazado.
[MEDIUM] Referrer-Policy: No se controla la información de referencia enviada a terceros, lo que podría filtrar datos de navegación sensibles.
[MEDIUM] Permissions-Policy: No se restringen las APIs del navegador como la cámara o el micrófono, aumentando la superficie de riesgo para el usuario.
[MEDIUM] Puerto 8080 (HTTP-Alt): Se detectó el puerto 8080 abierto, el cual suele ser utilizado para servicios alternativos o proxies y representa un punto de entrada adicional para atacantes.

[LOW] Server header expuesto: La cabecera revela el uso de Cloudflare, proporcionando información técnica sobre la infraestructura de red a posibles atacantes.
[LOW] Robots.txt y Sitemap: La inexistencia de estos archivos dificulta la correcta indexación y el control del rastreo por parte de motores de búsqueda.