EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://sagutweb.com/	Checks	9 pruebas
Dominio	sagutweb.com	Hallazgos	43 totales
Fecha	6 de septiembre de 2026 a las 08:01	Problemas	14 detectados

C

68/100

puntos de seguridad

RESUMEN EJECUTIVO

El analisis de seguridad realizado arroja una puntuacion exacta de 68/100, lo que otorga al sitio una nota C segun los estándares de auditoria. Durante el proceso se ejecutaron 9 checks pasivos, resultando en 5 verificaciones correctas, 2 advertencias y 2 fallos criticos en la configuracion de infraestructura. Aunque la conexion base esta cifrada, la ausencia total de politicas de seguridad en el servidor y la exposicion de servicios administrativos incrementan el riesgo de compromiso. Se concluye que el sitio es vulnerable ante ataques de inyeccion, suplantacion de identidad y accesos no autorizados por fuerza bruta.

Resumen de Riesgos

0	4	9	1	29
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 77 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 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): 22 (SSH)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 77 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  77 dias restantes (expira: 2026-11-22T09:01:14.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-08-24T09:01:15.000Z
- 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: nginx/1.28.0 — 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://sagutweb.com/
- 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

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente
- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente
- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente

- 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

- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

- INFO **Puerto 21 (FTP)**
  Cerrado — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — 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] Content-Security-Policy: Falta esta cabecera esencial, permitiendo potenciales ataques de Cross-Site Scripting (XSS) e inyeccion de contenido malicioso.
[HIGH] X-Frame-Options: La ausencia de esta directiva hace al sitio vulnerable a ataques de clickjacking, donde un tercero puede secuestrar clics del usuario.
[HIGH] Strict-Transport-Security: No esta configurada, lo que impide que el navegador fuerce conexiones seguras y deja la puerta abierta a ataques de degradacion de protocolo.
[HIGH] HSTS: El mecanismo de seguridad de transporte estricto no esta activo, debilitando la implementacion de la redireccion HTTPS.

[MEDIUM] X-Content-Type-Options: Falta esta cabecera, permitiendo que el navegador realice sniffing de tipos MIME, lo que podria ejecutar archivos maliciosos disfrazados.
[MEDIUM] Referrer-Policy: No existe control sobre la informacion de procedencia enviada en las peticiones, lo que puede filtrar URLs privadas a sitios externos.
[MEDIUM] Permissions-Policy: La ausencia de esta directiva permite el uso no restringido de APIs del navegador como la camara o el microfono si existieran vulnerabilidades.
[MEDIUM] Archivos informativos expuestos: El acceso publico a /readme.html y /README.txt puede revelar detalles tecnicos internos de la arquitectura del sitio.
[MEDIUM] Paneles de gestion expuestos: Rutas administrativas como /wp-login.php, /administrator/ y /user/login son accesibles, facilitando ataques de fuerza bruta.
[MEDIUM] Puerto 22 (SSH) abierto: La exposicion del puerto de acceso remoto aumenta significativamente la superficie de ataque para intrusiones a nivel de servidor.
[LOW] Server header expuesto: La cabecera revela el uso de nginx/1.28.0, proporcionando a posibles atacantes informacion especifica para explotar debilidades de esa version.
[FAIL] Robots.txt y Sitemap: La falta de estos archivos criticos indica una configuracion de servidor incompleta y afecta la visibilidad controlada del sitio.