EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://sillageonline.com/login	Checks	9 pruebas
Dominio	sillageonline.com	Hallazgos	49 totales
Fecha	30 de mayo de 2026 a las 01:13	Problemas	9 detectados

C

74/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web ha arrojado una puntuación de 74/100, lo que corresponde a una calificación de C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 4 resultaron satisfactorios, 4 generaron advertencias y 1 fue identificado como fallo crítico de configuración. Aunque la implementación del cifrado de transporte es correcta, se detectaron carencias importantes en las políticas de seguridad del servidor y en la protección de las cookies de sesión. En su estado actual, el sitio se considera vulnerable a ataques de inyección y secuestro de sesiones debido a la ausencia de cabeceras de seguridad fundamentales. Es necesario aplicar medidas correctivas para fortalecer la postura de seguridad frente a amenazas externas.

Resumen de Riesgos

0	4	3	2	40
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 86 dias
Cabeceras de Seguridad	30	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	83	AVISO	XSRF-TOKEN: falta HttpOnly
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 86 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  86 dias restantes (expira: 2026-08-24T01:34:51.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-26T01:34:52.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 30/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, Strict-Transport-Security, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: nginx/1.18.0 (Ubuntu) — 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)
- INFO **X-Content-Type-Options**
  Presente: nosniff
- 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://sillageonline.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

- 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 — 83/100

Estado: AVISO

XSRF-TOKEN: falta HttpOnly

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- ALTO **Cookie: XSRF-TOKEN — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: XSRF-TOKEN — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: XSRF-TOKEN — SameSite**
  SameSite=lax
- INFO **Cookie: laravel-session — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: laravel-session — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: laravel-session — SameSite**
  SameSite=lax

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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (24 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- 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): 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 faltante: La ausencia de esta cabecera permite la ejecución de ataques XSS y la inyección de contenido malicioso en el navegador del usuario.
[HIGH] Strict-Transport-Security (HSTS) no configurado: El servidor no instruye al navegador para que use siempre conexiones HTTPS, lo que facilita ataques de degradación de protocolo.
[HIGH] Cookie XSRF-TOKEN sin atributo HttpOnly: Esta cookie es accesible a través de scripts de cliente, lo que aumenta drásticamente el riesgo de robo de tokens de sesión mediante ataques XSS.
[MEDIUM] Referrer-Policy faltante: No se controla qué información de procedencia se envía a otros sitios, lo que podría exponer URLs internas o datos sensibles.
[MEDIUM] Permissions-Policy faltante: El sitio no restringe el acceso a APIs del navegador como la cámara, el micrófono o la geolocalización, dejando la puerta abierta a abusos de privacidad.
[MEDIUM] Puerto 22 (SSH) abierto: El puerto de acceso remoto está expuesto a internet, lo que permite intentos de intrusión mediante ataques de fuerza bruta.
[LOW] Server header expuesto: El servidor revela el uso de nginx/1.18.0 (Ubuntu), facilitando a los atacantes la búsqueda de exploits específicos para esa versión.
[LOW] sitemap.xml no encontrado: La falta de este archivo puede afectar la indexación y el reconocimiento de la estructura del sitio por parte de herramientas de seguridad.