EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://elmalecondelasalsa.com	Checks	9 pruebas
Dominio	elmalecondelasalsa.com	Hallazgos	59 totales
Fecha	17 de septiembre de 2026 a las 00:51	Problemas	16 detectados

B

82/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada al sitio elmalecondelasalsa.com arroja una puntuación de 82/100 con una calificación de grado B. El análisis se basó en la ejecución de 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 2 presentaron advertencias y 1 fue calificado como fallo crítico. Se han detectado deficiencias importantes en la configuración de las cookies y en las cabeceras de seguridad del servidor. Aunque la base de cifrado es sólida, el sitio se considera vulnerable debido a la exposición de datos de sesión y la falta de protecciones contra ataques de secuestro de clics.

Resumen de Riesgos

0	7	6	3	43
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 80 dias
Cabeceras de Seguridad	70	AVISO	4/6 presentes. Faltan: X-Frame-Options, Permissi...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
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	17	FALLO	frontend_lang: falta HttpOnly; frontend_lang: fa...
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): 22 (SSH)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 80 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  80 dias restantes (expira: 2026-12-05T20:51:52.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-09-06T20:51:53.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 70/100

Estado: AVISO

4/6 presentes. Faltan: X-Frame-Options, Permissions-Policy

- BAJO **Server header expuesto**
  Server: nginx — Revela tecnologia del servidor

- INFO **Content-Security-Policy**
  Presente: default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://*.go...
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: strict-origin-when-cross-origin
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://elmalecondelasalsa.com/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 dias)
- 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
- BAJO **Meta generator**
  Expone: Odoo

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 — 17/100

Estado: FALLO

frontend_lang: falta HttpOnly; frontend_lang: falta Secure; frontend_lang: falta SameSite; session_id: falta Secure; session_id: falta SameSite; frontend_lang: falta HttpOnly; frontend_lang: falta Secure; frontend_lang: falta SameSite; session_id: falta Secure; session_id: falta SameSite

- INFO **Cookies detectadas**
  4 cookie(s) encontrada(s)
- ALTO **Cookie: frontend_lang — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: frontend_lang — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: frontend_lang — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: session_id — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: session_id — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: session_id — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: frontend_lang — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: frontend_lang — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: frontend_lang — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: session_id — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: session_id — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: session_id — SameSite**
  Falta SameSite — Vulnerable a CSRF

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 (495 bytes)
- INFO **Reglas robots.txt**
  17 Disallow, 3 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://elmalecondelasalsa.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): 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] Cookie session_id y frontend_lang: Ausencia de los atributos Secure, HttpOnly y SameSite, lo que facilita el robo de sesiones y ataques de falsificación de peticiones.
[HIGH] X-Frame-Options: La cabecera de seguridad no está presente, permitiendo que el sitio sea cargado en marcos externos para realizar ataques de clickjacking.
[MEDIUM] Permissions-Policy: No se han definido restricciones para las APIs del navegador, dejando expuestas funcionalidades como cámara o micrófono.
[MEDIUM] Puerto 22 (SSH) abierto: La exposición de este puerto de administración remota incrementa el riesgo de intentos de intrusión por fuerza bruta.
[LOW] Server header expuesto: El servidor revela que utiliza la tecnología nginx, proporcionando información útil para que un atacante busque vulnerabilidades específicas.
[LOW] Meta generator Odoo: Se identifica el uso de Odoo a través de etiquetas meta, lo que facilita el reconocimiento de la plataforma.
[LOW] Ruta sensible en robots.txt: El archivo incluye una referencia directa a la ruta "admin", exponiendo un posible punto de acceso administrativo a indexadores y atacantes.