EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://altheaespaisalut.com	Checks	9 pruebas
Dominio	altheaespaisalut.com	Hallazgos	45 totales
Fecha	12 de mayo de 2026 a las 15:46	Problemas	15 detectados

D

49/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre altheaespaisalut.com ha otorgado una puntuación de 49/100, lo que resulta en una calificación de grado D. Durante el proceso se ejecutaron 9 comprobaciones pasivas, identificando 4 resultados correctos, 1 advertencia y 4 fallos críticos en la configuración. El sitio presenta carencias fundamentales en la implementación de cabeceras de seguridad y en el forzado de protocolos de transferencia segura. Por tanto, se concluye que el sitio es actualmente vulnerable y requiere una intervención inmediata para mitigar riesgos de interceptación y ataques de inyección.

Resumen de Riesgos

0	6	5	4	30
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 154 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	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 6.7.1 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	60	AVISO	2 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 154 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  154 dias restantes (expira: 2026-10-13T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-02T00:00:00.000Z
- 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: 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
- 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

CMS detectado: WordPress, PrestaShop

- INFO **WordPress**
  Detectado via HTML body
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  Detectado via HTML body
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: WordPress 6.7.1
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.7.1 expuesta

- ALTO **WordPress version**
  Version 6.7.1 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- INFO **Archivo /readme.html**
  No accesible (correcto)
- INFO **Archivo /README.txt**
  No accesible (correcto)

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

2 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://gmpg.org/xfn/11
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://fonts.googleapis.com/

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  No encontrado (HTTP 404)
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

2 puerto(s) abierto(s), todos esperados

- 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
- 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] Falta de Content-Security-Policy: La ausencia de esta cabecera facilita ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.

[HIGH] Falta de X-Frame-Options: El sitio es vulnerable a ataques de clickjacking al permitir que el contenido sea embebido en marcos externos sin control.
[HIGH] Falta de Strict-Transport-Security: No se comunica al navegador que debe usar exclusivamente conexiones HTTPS, permitiendo posibles ataques de degradación de protocolo.
[HIGH] Fallo en redirección HTTP a HTTPS: La web permite el acceso mediante HTTP sin cifrar, lo que expone los datos transmitidos a ser interceptados.
[HIGH] Versión de WordPress expuesta (6.7.1): La visualización pública de la versión exacta permite a potenciales atacantes buscar vulnerabilidades específicas y conocidas para este software.
[MEDIUM] Falta de X-Content-Type-Options: Al no estar presente, el navegador podría intentar interpretar el contenido de forma distinta a la declarada, facilitando el sniffing de tipos MIME.
[MEDIUM] Falta de Referrer-Policy: No se controla qué información de procedencia se envía a terceros, lo que podría filtrar rutas internas del sitio.
[MEDIUM] Falta de Permissions-Policy: El sitio no restringe el uso de APIs sensibles del navegador como la cámara o el micrófono por parte de scripts.
[MEDIUM] Contenido Mixto detectado: Se cargan recursos externos (gmpg.org y Google Fonts) mediante protocolos HTTP no seguros dentro de la página cifrada.
[LOW] Cabecera de servidor expuesta: El sistema revela el uso de Apache, facilitando la fase de reconocimiento de un atacante sobre la infraestructura.
[LOW] Meta generator expuesto: Se confirma públicamente que el sitio utiliza WordPress 6.7.1, aumentando la superficie de exposición.
[LOW] Ausencia de archivos robots.txt y sitemap.xml: La falta de estos archivos dificulta la auditoría de indexación y puede ocultar problemas de visibilidad de archivos sensibles.