EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://acacia-inversion.com/	Checks	9 pruebas
Dominio	acacia-inversion.com	Hallazgos	46 totales
Fecha	12 de agosto de 2026 a las 10:37	Problemas	10 detectados

B

75/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada al sitio acacia-inversion.com ha dado como resultado una puntuación de 75/100, lo que equivale a una calificación de grado B. El análisis se basó en 9 checks pasivos, de los cuales 5 fueron superados con éxito, 2 presentaron advertencias por configuraciones mejorables y 2 se identificaron como fallos de seguridad. Se detectaron debilidades críticas en la gestión de cabeceras de seguridad y en la exposición pública de versiones de software obsoletas. Aunque el cifrado base es correcto, la ausencia de mecanismos para forzar conexiones seguras y la visibilidad de datos técnicos sensibles comprometen la integridad del sitio. En conclusión, el portal se considera vulnerable a ataques dirigidos de reconocimiento y explotación de vulnerabilidades conocidas.

Resumen de Riesgos

0	3	5	2	36
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 82 dias
Cabeceras de Seguridad	55	FALLO	Solo 3/6 presentes. Faltan: Strict-Transport-Sec...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 5.9.15 expuesta, WordPress 2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	60	AVISO	1 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 82 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  82 dias restantes (expira: 2026-11-01T23:17:36.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-08-03T23:17:36.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 55/100

Estado: FALLO

Solo 3/6 presentes. Faltan: Strict-Transport-Security, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: Sucuri/Cloudproxy — Revela tecnologia del servidor

- INFO **Content-Security-Policy**
  Presente: upgrade-insecure-requests;
- 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://acacia-inversion.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

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 5.9.15
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 5.9.15 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 5.9.15 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- INFO **Archivo /README.txt**
  No accesible (correcto)

- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente

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

1 recurso(s) HTTP en pagina HTTPS

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

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (173 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- INFO **Sitemap en robots.txt**
  https://acacia-inversion.com/sitemap.xml
- 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] WordPress version: La versión 5.9.15 se encuentra expuesta públicamente, permitiendo a atacantes buscar vulnerabilidades específicas (CVEs) para este software.
[HIGH] Strict-Transport-Security: Falta la cabecera HSTS, lo que impide que el navegador fuerce automáticamente conexiones seguras por HTTPS.
[MEDIUM] Archivo /readme.html: Este archivo es accesible de forma pública y puede revelar información técnica detallada sobre la instalación del CMS.
[MEDIUM] Ruta /wp-login.php: El panel de acceso a la administración es visible, lo que facilita intentos de intrusión mediante ataques de fuerza bruta.
[MEDIUM] Referrer-Policy: No existe una política definida para controlar qué información de navegación se comparte con otros sitios web.
[MEDIUM] Permissions-Policy: La ausencia de esta cabecera permite que el navegador no restrinja el acceso a APIs potencialmente sensibles como cámara o micrófono.
[MEDIUM] Recurso HTTP: Se detectó el uso de contenido mixto a través de una hoja de estilo cargada mediante el protocolo inseguro HTTP.
[LOW] Server header expuesto: El servidor revela el uso de tecnología Sucuri/Cloudproxy, facilitando la fase de reconocimiento del entorno técnico.
[LOW] Meta generator: La etiqueta meta expone explícitamente el uso de WordPress 5.9.15 en el código fuente.