EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://arkano.shop/	Checks	9 pruebas
Dominio	arkano.shop	Hallazgos	49 totales
Fecha	28 de mayo de 2026 a las 18:09	Problemas	18 detectados

D

49/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio arkano.shop ha arrojado una puntuación de 49/100, lo que equivale a una calificación de grado D. Durante la auditoría se ejecutaron 9 comprobaciones pasivas, resultando en 4 verificaciones correctas, 2 advertencias y 3 fallos críticos en la configuración. El sitio presenta deficiencias severas en la implementación de cabeceras de seguridad y en la gestión de protocolos de conexión segura. Debido a la exposición de versiones del software y la falta de protecciones contra ataques comunes, se concluye que el sitio es actualmente vulnerable. Es urgente aplicar medidas correctivas para evitar el compromiso de la plataforma y sus usuarios.

Resumen de Riesgos

0	6	8	4	31
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 80 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 7.0 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	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

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: 2026-08-17T03:28:32.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-19T03:28:33.000Z
- 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: cloudflare — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.4.21 — Revela framework/lenguaje
- 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 7.0
- INFO **Tecnologias detectadas**
  Next.js, PHP/8.4.21

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 7.0 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 7.0 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://About%20Us

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (2052 bytes)
- INFO **Reglas robots.txt**
  15 Disallow, 2 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://arkano.shop/wp-sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- 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

- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
  Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[HIGH] Ausencia de Content-Security-Policy: La falta de esta cabecera permite ataques de inyección de contenido y scripts maliciosos (XSS).
[HIGH] Falta de X-Frame-Options: El sitio es vulnerable a ataques de clickjacking, permitiendo que la web sea cargada en marcos externos no autorizados.
[HIGH] Omisión de Strict-Transport-Security: No se fuerza el uso de conexiones cifradas, facilitando ataques de interceptación de datos.
[HIGH] Fallo de redirección HTTPS: El servidor permite el acceso por HTTP sin redirigir al protocolo seguro, exponiendo la comunicación.
[HIGH] Exposición de versión de WordPress: Se detectó la versión 7.0 expuesta, lo que permite a atacantes identificar vulnerabilidades conocidas (CVEs).
[MEDIUM] Falta de X-Content-Type-Options: La ausencia de esta directiva permite el sniffing de tipos MIME por parte del navegador.
[MEDIUM] Ausencia de Referrer-Policy: No se controla la información de referencia enviada a otros dominios al navegar.
[MEDIUM] Permissions-Policy no configurada: No se restringe el acceso de las APIs del navegador a funciones sensibles como cámara o micrófono.
[MEDIUM] Archivo readme.html accesible: La visibilidad de este archivo revela información técnica sobre la instalación del CMS.
[MEDIUM] Panel de login expuesto: La ruta /wp-login.php es accesible públicamente, facilitando ataques de fuerza bruta.
[MEDIUM] Contenido Mixto detectado: Se carga un recurso mediante HTTP (http://About%20Us) dentro de una sesión HTTPS, rompiendo el cifrado.
[MEDIUM] Puerto 8080 abierto: La disponibilidad de este puerto HTTP-Alt amplía la superficie de ataque del servidor.
[MEDIUM] Exposición en robots.txt: El archivo bloquea todo el sitio y referencia rutas administrativas sensibles.
[LOW] Cabecera de servidor expuesta: Se revela el uso de Cloudflare, proporcionando pistas sobre la infraestructura.
[LOW] X-Powered-By expuesto: El encabezado detalla el uso de PHP/8.4.21, facilitando el perfilado del sistema.
[LOW] Etiqueta meta generator visible: Expone directamente la tecnología y versión utilizada en el desarrollo.