EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://afphabitat.cl	Checks	9 pruebas
Dominio	afphabitat.cl	Hallazgos	50 totales
Fecha	26 de mayo de 2026 a las 17:26	Problemas	19 detectados

D

50/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio afphabitat.cl ha resultado en una puntuación de 50/100, lo que otorga una calificación de grado D. Se ejecutaron un total de 9 checks pasivos, de los cuales solo 3 resultaron satisfactorios, mientras que se identificaron 2 advertencias y 4 fallos críticos. La ausencia total de cabeceras de seguridad esenciales y el uso de una versión de CMS desactualizada representan riesgos significativos para la integridad de la plataforma. Debido a estas deficiencias técnicas, se concluye que el sitio es actualmente vulnerable ante ataques de interceptación y explotación dirigida.

Resumen de Riesgos

0	10	8	1	31
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	70	AVISO	Certificado expira en 14 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
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 6.0.2 expuesta
Seguridad de Cookies	11	FALLO	PHPSESSID: falta HttpOnly; PHPSESSID: falta Same...
Contenido Mixto	100	OK	No se detecto contenido mixto
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 — 70/100

Estado: AVISO

Certificado expira en 14 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- MEDIO **Dias hasta expiracion**
  14 dias restantes (expira: 2026-06-09T18:48:32.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-11T18:48:33.000Z
- 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

- 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 302 redirige a https://www.afphabitat.cl/
- 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 6.0.2
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.0.2 expuesta

- ALTO **WordPress version**
  Version 6.0.2 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS

Seguridad de Cookies — 11/100

Estado: FALLO

PHPSESSID: falta HttpOnly; PHPSESSID: falta SameSite; site_origen: falta HttpOnly; site_origen: falta Secure; site_origen: falta SameSite; TS01a992e1: falta

HttpOnly; TS01a992e1: falta Secure; TS01a992e1: falta SameSite

- INFO **Cookies detectadas**
  3 cookie(s) encontrada(s)
- ALTO **Cookie: PHPSESSID — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: PHPSESSID — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: PHPSESSID — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: site_origen — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: site_origen — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: site_origen — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: TS01a992e1 — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: TS01a992e1 — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: TS01a992e1 — 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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

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] Content-Security-Policy: Falta esta cabecera, lo que permite la ejecución de ataques XSS y la inyección de contenido malicioso en el navegador del usuario.
[HIGH] X-Frame-Options: La ausencia de esta directiva hace al sitio susceptible a ataques de clickjacking, donde un tercero puede superponer marcos invisibles para engañar al usuario.
[HIGH] Strict-Transport-Security: No se ha configurado HSTS, lo que impide forzar conexiones HTTPS seguras y facilita ataques de degradación de protocolo.
[HIGH] WordPress version: La exposición pública de la versión 6.0.2 permite a atacantes identificar rápidamente vulnerabilidades conocidas y exploits documentados para esa versión específica.
[HIGH] Cookie PHPSESSID: Falta el atributo HttpOnly, permitiendo que la cookie de sesión sea accesible mediante scripts, lo que eleva el riesgo de robo de identidad.
[HIGH] Cookie site_origen: No posee los flags HttpOnly ni Secure, lo que implica que la información viaja sin cifrado y es vulnerable a ataques de inyección.
[HIGH] Cookie TS01a992e1: Carece de protecciones HttpOnly y Secure, dejando este identificador expuesto a interceptación en redes no seguras.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el sniffing de tipos MIME, lo que podría derivar en la ejecución de archivos maliciosos disfrazados de elementos legítimos.
[MEDIUM] Referrer-Policy: No existe control sobre la información de referencia enviada a sitios externos, pudiendo filtrar datos de navegación privada.
[MEDIUM] Permissions-Policy: No se restringen las APIs del navegador, permitiendo que funciones como la cámara o el micrófono sean potencialmente invocadas por scripts no autorizados.
[MEDIUM] Archivos de documentación expuestos: Los archivos /readme.html y /README.txt son accesibles públicamente, revelando detalles técnicos de la instalación que facilitan el reconocimiento inicial.
[MEDIUM] Atributo SameSite: Las cookies de sesión no implementan SameSite, dejando la plataforma vulnerable a ataques de falsificación de solicitud en sitios cruzados (CSRF).
[LOW] Expiración de Certificado SSL: El certificado actual expira en 14 días, lo que representa un riesgo operativo de interrupción del servicio a muy corto plazo.
[LOW] Meta generator: El código fuente expone la tecnología WordPress 6.0.2 a través de etiquetas meta, simplificando la fase de recolección de información para posibles atacantes.
[LOW] Ausencia de archivos de indexación: No se detectaron los archivos robots.txt ni sitemap.xml, lo que dificulta la comunicación correcta con los motores de búsqueda y la gestión de la visibilidad.