EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://grupoacb.com/	Checks	9 pruebas
Dominio	grupoacb.com	Hallazgos	49 totales
Fecha	22 de mayo de 2026 a las 23:56	Problemas	13 detectados

C

64/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web arroja una puntuación de 64/100, lo que corresponde a una calificación de grado C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 2 generaron advertencias y 2 fueron marcados como fallos críticos. La infraestructura presenta una carencia total de cabeceras de seguridad y mantiene versiones de software desactualizadas con información técnica expuesta públicamente. Debido a estas deficiencias en la configuración del servidor y el mantenimiento del CMS, se concluye que el sitio es actualmente vulnerable ante ataques de inyección y suplantación.

Resumen de Riesgos

0	5	6	2	36
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 110 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 6.9.4 expuesta, WordPress 2 expuesta
Seguridad de Cookies	67	AVISO	__wpdm_client: falta SameSite
Contenido Mixto	100	OK	No se detecto contenido mixto
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 110 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  110 dias restantes (expira: 2026-09-09T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-08-26T00:00:00.000Z
- 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://grupoacb.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 6.9.4
- INFO **Tecnologias detectadas**
  React, Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.9.4 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 6.9.4 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 — 67/100

Estado: AVISO

__wpdm_client: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: __wpdm_client — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: __wpdm_client — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: __wpdm_client — 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 (170 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- INFO **Sitemap en robots.txt**
  https://grupoacb.com/sitemap_index.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] Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de scripts no autorizados y ataques de inyección de contenido XSS.
[HIGH] X-Frame-Options: La falta de esta política hace que el sitio sea susceptible a ataques de clickjacking mediante el uso de marcos.
[HIGH] Strict-Transport-Security: No se implementa HSTS, lo que impide forzar conexiones cifradas y facilita ataques de degradación de protocolo.
[HIGH] WordPress version: La exposición de la versión 6.9.4 permite a atacantes identificar y explotar CVEs específicos ya documentados.
[MEDIUM] X-Content-Type-Options: Al no estar configurada, el navegador puede intentar interpretar archivos de forma incorrecta mediante MIME-type sniffing.
[MEDIUM] Referrer-Policy: No se controla qué información de procedencia se envía a terceros, comprometiendo potencialmente la privacidad de la navegación.
[MEDIUM] Permissions-Policy: El sitio no restringe el acceso a APIs del navegador como la cámara, el micrófono o la geolocalización.
[MEDIUM] Cookie __wpdm_client: La falta del atributo SameSite en esta cookie de WordPress Download Manager aumenta el riesgo de ataques Cross-Site Request Forgery.
[MEDIUM] Archivo /readme.html: Este archivo es accesible de forma pública y revela detalles sobre la instalación y versión del CMS.
[MEDIUM] Ruta /wp-login.php: El acceso directo al panel de administración facilita intentos de intrusión mediante ataques de fuerza bruta.
[LOW] Server header expuesto: El servidor responde con la cabecera Apache, revelando la tecnología subyacente y facilitando el reconocimiento.
[LOW] Meta generator: La etiqueta meta en el código fuente confirma el uso de versiones antiguas de WordPress, asistiendo en la fase de enumeración del atacante.