EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.coalicionporelevangelio.org/	Checks	9 pruebas
Dominio	www.coalicionporelevangelio.org	Hallazgos	49 totales
Fecha	1 de mayo de 2026 a las 17:52	Problemas	16 detectados

C

60/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio web ha resultado en una puntuación de 60/100, lo que otorga una calificación de nota C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 4 fueron exitosos, 3 generaron advertencias y 2 resultaron en fallos críticos. A pesar de contar con un cifrado de conexión adecuado, la plataforma presenta deficiencias severas en la configuración de cabeceras de seguridad y exposición de información técnica. La ausencia de mecanismos de endurecimiento (hardening) permite concluir que el sitio es vulnerable a ataques de inyección y suplantación.

Resumen de Riesgos

0	5	7	4	33
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 34 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 6.6.5 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	60	AVISO	3 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 34 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  34 dias restantes (expira: 2026-06-05T00:09:56.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-06T23:09:59.000Z
- 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: WP Engine — 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://www.coalicionporelevangelio.org/
- 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: WPML ver:4.6.12 stt:1,2;
- INFO **Tecnologias detectadas**
  WP Engine

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.6.5 expuesta

- ALTO **WordPress version**
  Version 6.6.5 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

3 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://browsehappy.com/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.tgckorea.org/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.tgckorea.org/

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (75 bytes)
- INFO **Reglas robots.txt**
  2 Disallow, 0 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **sitemap.xml**
  Presente, ? URLs
- 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] Falta de Content-Security-Policy: La ausencia de esta cabecera permite ataques de Cross-Site Scripting (XSS) e inyección de datos maliciosos.
[HIGH] Falta de X-Frame-Options: El sitio es vulnerable a ataques de Clickjacking al permitir ser embebido en marcos de otras webs.
[HIGH] Falta de Strict-Transport-Security: No se fuerza el uso de HTTPS mediante HSTS, permitiendo ataques de degradación de protocolo (SSL Stripping).
[HIGH] Versión de WordPress expuesta: La versión 6.6.5 es visible públicamente, lo que facilita a atacantes la búsqueda de exploits específicos para este motor.
[MEDIUM] Falta de X-Content-Type-Options: El navegador podría intentar interpretar el contenido de forma distinta a la declarada, facilitando la ejecución de scripts.
[MEDIUM] Falta de Referrer-Policy: No se controla la información de origen que se envía a otros dominios al navegar por enlaces externos.
[MEDIUM] Falta de Permissions-Policy: El sitio no restringe el acceso a APIs sensibles del navegador como la cámara, el micrófono o la geolocalización.
[MEDIUM] Contenido Mixto detectado: Existen 3 recursos (enlaces a browsehappy.com y tgckorea.org) que se cargan vía HTTP dentro de la sesión segura.
[MEDIUM] Puerto 8080 abierto: El servicio HTTP-Alt está accesible, lo que representa un vector de ataque si aloja servicios de administración o proxies.
[LOW] Cabecera Server expuesta: Se revela el uso de Cloudflare, proporcionando información útil para la fase de reconocimiento de un ataque.
[LOW] Cabecera X-Powered-By expuesta: Indica el uso de WP Engine, lo cual ayuda a identificar la infraestructura y el proveedor de hosting.
[LOW] Meta generator expuesto: La etiqueta meta revela el uso de WPML versión 4.6.12, aportando detalles granulares sobre los componentes internos.
[LOW] Ruta sensible en robots.txt: El archivo menciona la ruta admin, facilitando a los atacantes la identificación de paneles de gestión.