EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://secuoyacontentgroup.com	Checks	9 pruebas
Dominio	secuoyacontentgroup.com	Hallazgos	53 totales
Fecha	1 de junio de 2026 a las 12:08	Problemas	18 detectados

C

60/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web arroja una puntuación de 60/100, obteniendo una nota final de C. Durante el proceso se ejecutaron 9 checks pasivos, resultando en 4 verificaciones exitosas, 3 advertencias y 2 fallos críticos relacionados con la configuración del servidor y la exposición de versiones de software. La ausencia total de cabeceras de seguridad esenciales y la presencia de contenido mixto comprometen la integridad de la plataforma. En su estado actual, el sitio se considera vulnerable a ataques de clickjacking, inyección de contenido y explotación de vulnerabilidades conocidas en el CMS.

Resumen de Riesgos

0	6	8	4	35
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 218 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 7.0 expuesta, WordPress 2 expuesta
Seguridad de Cookies	67	AVISO	pll_language: falta HttpOnly
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	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 218 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  218 dias restantes (expira: 2027-01-05T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-12-22T00:00:00.000Z
- 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: nginx — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.1.34, PleskLin — 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://secuoyacontentgroup.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 7.0
- INFO **Tecnologias detectadas**
  Next.js, PHP/8.1.34, PleskLin

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 — 67/100

Estado: AVISO

pll_language: falta HttpOnly

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: pll_language — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: pll_language — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: pll_language — SameSite**
  SameSite=lax

Contenido Mixto — 60/100

Estado: AVISO

3 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.twitter.com/gruposecuoya
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.twitter.com/gruposecuoya
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.twitter.com/gruposecuoya

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (124 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://secuoyacontentgroup.com/wp-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] Content-Security-Policy: Falta esta cabecera, lo que permite ataques de inyección de contenido y ejecución de scripts no autorizados (XSS).
[HIGH] X-Frame-Options: Su ausencia deja el sitio expuesto a ataques de clickjacking, permitiendo que un tercero cargue la web en un marco invisible.
[HIGH] Strict-Transport-Security: No se ha configurado HSTS, por lo que el navegador no obliga al uso de conexiones cifradas en todas las solicitudes.
[HIGH] WordPress version: La versión 7.0 del CMS se encuentra expuesta públicamente, facilitando a atacantes la búsqueda de CVEs y exploits específicos.
[HIGH] Cookie pll_language: Falta el atributo HttpOnly, lo que permite que la cookie sea accesible mediante scripts de cliente, aumentando el riesgo de robo de sesión.
[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.
[MEDIUM] Referrer-Policy: No hay una política definida para controlar cuánta información de referencia se envía al navegar hacia otros enlaces.
[MEDIUM] Permissions-Policy: No se restringe el acceso a funciones sensibles del navegador como la cámara, el micrófono o la geolocalización.
[MEDIUM] Archivo /readme.html: Este archivo es accesible públicamente y revela información técnica detallada sobre la instalación del CMS.
[MEDIUM] Ruta /wp-login.php: El panel de administración es accesible directamente, lo que facilita ataques de fuerza bruta.
[MEDIUM] Contenido Mixto: Se detectaron 3 recursos vinculados a Twitter mediante protocolo HTTP, debilitando la seguridad del cifrado SSL general.
[LOW] Server header expuesto: El encabezado revela que el servidor utiliza tecnología nginx, acotando el vector de ataque para un intruso.
[LOW] X-Powered-By expuesto: La cabecera muestra el uso de PHP/8.1.34 y PleskLin, proporcionando detalles técnicos innecesarios al exterior.
[LOW] Meta generator: El código fuente expone explícitamente la versión de WordPress utilizada.
[LOW] Ruta sensible en robots.txt: Se hace referencia directa a la ruta de administración, guiando a posibles atacantes hacia zonas restringidas.