EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://carper.com.uy	Checks	9 pruebas
Dominio	carper.com.uy	Hallazgos	45 totales
Fecha	28 de julio de 2026 a las 13:15	Problemas	12 detectados

C

64/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio carper.com.uy arroja una puntuación de 64/100, lo que equivale a una calificación de grado C. Durante la evaluación se ejecutaron 9 checks pasivos, resultando en 5 verificaciones correctas, 2 advertencias y 2 fallos críticos en la configuración. Aunque el sitio cuenta con un cifrado de transporte válido, la ausencia total de cabeceras de seguridad y la exposición de versiones de software representan un riesgo significativo. En su estado actual, el sitio se considera vulnerable a ataques de inyección, clickjacking y reconocimiento de infraestructura por parte de terceros.

Resumen de Riesgos

0	5	5	2	33
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 56 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 6.7.5 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	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 56 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  56 dias restantes (expira: 2026-09-22T11:11:33.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-24T11:11:34.000Z
- 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://carper.com.uy/
- 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 6.7.5
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.7.5 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 6.7.5 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)

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://instagram.com/carper.chevrolet

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (171 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- INFO **Sitemap en robots.txt**
  https://carper.com.uy/sitemap_index.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

No se detectaron puertos abiertos

- 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)**
  Cerrado — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Cerrado — 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 ataques de cross-site scripting (XSS) y la inyección de contenido malicioso.

[HIGH] X-Frame-Options: No se detectó esta cabecera, lo que expone el sitio a ataques de secuestro de clics o clickjacking.
[HIGH] Strict-Transport-Security: La falta de HSTS impide que el navegador fuerce conexiones HTTPS, facilitando ataques de degradación de protocolo.
[HIGH] WordPress version: La versión 6.7.5 se encuentra expuesta públicamente, permitiendo a atacantes buscar vulnerabilidades conocidas (CVEs) para ese motor.
[MEDIUM] X-Content-Type-Options: La falta de esta configuración permite que los navegadores realicen sniffing de tipos MIME, lo que puede derivar en la ejecución de scripts no autorizados.
[MEDIUM] Referrer-Policy: No existe una política definida para el control de la información de referencia enviada a otros dominios.
[MEDIUM] Permissions-Policy: El sitio no restringe el acceso a APIs sensibles del navegador como la cámara, el micrófono o la geolocalización.
[MEDIUM] Recurso HTTP: Se detectó un enlace hacia instagram.com bajo el protocolo HTTP, generando una advertencia de contenido mixto que degrada la integridad de la conexión.
[MEDIUM] Archivo /readme.html: Este archivo es accesible de forma pública y puede ser utilizado para obtener detalles técnicos sobre la instalación del CMS.
[LOW] Server header expuesto: La cabecera Server revela el uso de Apache, proporcionando información valiosa para la fase de reconocimiento de un ataque.
[LOW] Meta generator: La etiqueta meta expone explícitamente que el sitio utiliza WordPress 6.7.5, facilitando el perfilado tecnológico.