EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://casacastilla.com.uy	Checks	9 pruebas
Dominio	casacastilla.com.uy	Hallazgos	46 totales
Fecha	28 de julio de 2026 a las 13:11	Problemas	16 detectados

C

61/100

puntos de seguridad

RESUMEN EJECUTIVO

El analisis de ciberseguridad para casacastilla.com.uy arroja una puntuacion exacta de 61/100, lo que equivale a una nota C. Se ejecutaron 9 checks pasivos que resultaron en 4 validaciones exitosas, 1 advertencia y 4 fallos de seguridad detectados. El sitio presenta deficiencias notables en la configuracion de cabeceras de proteccion y exposicion de datos tecnicos sensibles. Se concluye que el sitio es actualmente vulnerable, principalmente debido a la falta de politicas de transporte seguro y la visibilidad publica de versiones de software.

Resumen de Riesgos

0	4	9	3	30
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 80 dias
Cabeceras de Seguridad	25	FALLO	Solo 1/6 presentes. Faltan: X-Frame-Options, Str...
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 9.0.1 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	20	FALLO	5 recursos HTTP en pagina HTTPS
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 — 100/100

Estado: OK

Certificado valido, expira en 80 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  80 dias restantes (expira: 2026-10-16T15:39:18.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-07-18T15:39:19.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 25/100

Estado: FALLO

Solo 1/6 presentes. Faltan: X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: hcdn — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.3.30 — Revela framework/lenguaje
- INFO **Content-Security-Policy**
  Presente: upgrade-insecure-requests
- 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://casacastilla.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: Powered by WPBakery Page Builder - drag and drop page builder for WordPress.
- INFO **Tecnologias detectadas**
  Next.js, Astro, PHP/8.3.30

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 9.0.1 expuesta

- ALTO **WordPress version**
  Version 9.0.1 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 — 100/100

Estado: OK

No se encontraron cookies

- INFO **Cookies detectadas**
  El sitio no establece cookies en la respuesta inicial

Contenido Mixto — 20/100

Estado: FALLO

5 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.casacastilla.uy/servicios/#bodas
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.casacastilla.uy/servicios/#ambientacion
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.casacastilla.uy/servicios/#paisajismo
- MEDIO **href (link/stylesheet)**
  ...y 2 mas del mismo tipo

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] WordPress version: La version 9.0.1 se encuentra expuesta publicamente, lo que facilita a atacantes la busqueda de exploits especificos.
[HIGH] X-Frame-Options: Esta cabecera falta por completo, dejando el sitio expuesto a ataques de secuestro de clics o clickjacking.
[HIGH] Strict-Transport-Security: No se ha configurado HSTS, por lo que el navegador no fuerza conexiones cifradas permanentemente.
[MEDIUM] Contenido Mixto: Se detectaron 5 recursos que cargan mediante HTTP dentro de la pagina HTTPS, lo que degrada la seguridad de la sesion.
[MEDIUM] X-Content-Type-Options: La ausencia de esta cabecera permite el MIME-type sniffing, aumentando el riesgo de ejecucion de scripts maliciosos.
[MEDIUM] Archivo /readme.html y /README.txt: Estos archivos son accesibles publicamente y pueden revelar informacion detallada sobre la estructura del CMS.
[MEDIUM] Referrer-Policy: Falta de control sobre la informacion que el sitio envia a terceros cuando un usuario hace clic en un enlace externo.
[MEDIUM] Permissions-Policy: No se restringen las APIs del navegador, permitiendo potencialmente el acceso no deseado a funciones como la camara o el microfono.
[LOW] Server header expuesto: El servidor responde con la cabecera hcdn, revelando detalles sobre la tecnologia de distribucion de contenido.
[LOW] X-Powered-By expuesto: La cabecera revela el uso exacto de PHP/8.3.30, ayudando a los atacantes a perfilar el entorno del servidor.
[LOW] Meta generator: El codigo fuente expone el uso de WPBakery Page Builder, proporcionando pistas sobre la superficie de ataque del sitio.
[LOW] Robots.txt y Sitemap: La falta de estos archivos dificulta la gestion adecuada del rastreo por parte de motores de busqueda y auditorias.