EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://casacastilla.uy/	Checks	9 pruebas
Dominio	casacastilla.uy	Hallazgos	50 totales
Fecha	28 de julio de 2026 a las 16:26	Problemas	15 detectados

C

65/100

puntos de seguridad

RESUMEN EJECUTIVO

El sitio web analizado ha obtenido una puntuación de 65/100, lo que resulta en una nota final de C según los estándares de auditoría externa. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 1 presentó advertencias y 3 fallaron debido a configuraciones de seguridad deficientes. Los hallazgos principales revelan una exposición innecesaria de versiones de software y una ausencia crítica de cabeceras de seguridad modernas. Se concluye que el sitio es actualmente vulnerable, principalmente debido a errores de configuración en el servidor y la falta de endurecimiento en el sistema de gestión de contenidos.

Resumen de Riesgos

0	4	7	4	35
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 86 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	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 86 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  86 dias restantes (expira: 2026-10-22T07:31:54.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-07-24T07:31:55.000Z
- 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.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
- 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 — 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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (443 bytes)
- INFO **Reglas robots.txt**
  7 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://casacastilla.uy/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

[ALTA] WordPress version: La versión 9.0.1 de WordPress se encuentra expuesta públicamente, lo que facilita que atacantes identifiquen vulnerabilidades conocidas (CVEs) para comprometer el sitio.
[ALTA] X-Frame-Options: Esta cabecera de seguridad está ausente, lo que permite que el sitio sea cargado en marcos (iframes) de sitios externos, facilitando ataques de clickjacking.
[ALTA] Strict-Transport-Security: No existe una política HSTS configurada, por lo que el navegador no obliga a realizar conexiones HTTPS, permitiendo posibles degradaciones de seguridad.
[MEDIA] Contenido Mixto: Se detectaron 5 recursos cargando a través de protocolos HTTP inseguros dentro de la página HTTPS, lo que rompe la integridad del cifrado en la navegación.
[MEDIA] X-Content-Type-Options: La falta de esta cabecera permite el sniffing de tipos MIME, lo que podría llevar a que el navegador ejecute archivos con contenido malicioso interpretándolos como scripts.
[MEDIA] Referrer-Policy: No hay control sobre la información de referencia enviada a otros dominios, lo que puede filtrar URLs privadas o sensibles a terceros.
[MEDIA] Permissions-Policy: No se han definido restricciones para las APIs del navegador, dejando abierta la posibilidad de que se soliciten accesos no deseados a la cámara, micrófono o ubicación.
[BAJA] Server header expuesto: La cabecera Server revela el uso de hcdn, proporcionando pistas sobre la infraestructura de red utilizada.
[BAJA] X-Powered-By expuesto: El servidor informa explícitamente el uso de PHP/8.3.30, ayudando a los atacantes a acotar los vectores de ataque según la versión del lenguaje.
[BAJA] Meta generator: Los metadatos exponen el uso de WPBakery Page Builder, revelando herramientas internas que podrían tener sus propias vulnerabilidades.
[BAJA] Ruta sensible en robots.txt: El archivo incluye una referencia directa a directorios de administración, lo cual facilita el reconocimiento de rutas críticas para ataques de fuerza bruta.