EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://razonesdecuba.cu	Checks	9 pruebas
Dominio	razonesdecuba.cu	Hallazgos	46 totales
Fecha	21 de mayo de 2026 a las 15:12	Problemas	16 detectados

D

58/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al dominio razonesdecuba.cu arroja una puntuación de 58/100, lo que equivale a una calificación de grado D. Durante la auditoría se ejecutaron 9 checks pasivos, de los cuales 4 resultaron correctos, 2 generaron advertencias y 3 fueron fallos críticos. La ausencia total de cabeceras de seguridad esenciales y la exposición de versiones del CMS representan riesgos significativos para la integridad del sitio. En su estado actual, se concluye que el sitio es vulnerable ante ataques de inyección, clickjacking y reconocimiento de infraestructura.

Resumen de Riesgos

0	5	9	2	30
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 32 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 6.6.1 expuesta, WordPress 9.7.0.1 expu...
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	20	FALLO	7 recursos HTTP en pagina HTTPS
Robots.txt y Sitemap	60	AVISO	Falta robots.txt
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 32 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  32 dias restantes (expira: 2026-06-22T13:30:06.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-24T13:30:07.000Z
- 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://razonesdecuba.cu/
- 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: AMP for WP 1.0.97
- INFO **Tecnologias detectadas**
  Next.js, Astro

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.6.1 expuesta, WordPress 9.7.0.1 expuesta

- ALTO **WordPress version**
  Version 6.6.1 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

7 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://razonesdecuba.cu/razones-en-datos/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.granma.cu/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.cubadebate.cu/
- MEDIO **href (link/stylesheet)**
  ...y 4 mas del mismo tipo

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta robots.txt

- INFO **sitemap.xml**
  Presente, 436 URLs
- 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

[ALTA] Content-Security-Policy (CSP) faltante: La ausencia de esta cabecera facilita ataques de Cross-Site Scripting (XSS) e inyección de datos.
[ALTA] X-Frame-Options faltante: El sitio es vulnerable a ataques de clickjacking al permitir ser cargado dentro de marcos o iframes externos.
[ALTA] Strict-Transport-Security (HSTS) faltante: El servidor no fuerza el uso de conexiones seguras, permitiendo posibles degradaciones de protocolo de HTTPS a HTTP.
[ALTA] Versión de WordPress expuesta (6.6.1): La visibilidad de la versión exacta permite a atacantes buscar vulnerabilidades específicas (CVEs) para comprometer el sitio.
[MEDIA] Contenido Mixto detectado: Se identificaron 7 recursos cargados mediante HTTP en una página HTTPS, lo que debilita el cifrado general.
[MEDIA] X-Content-Type-Options faltante: La falta de esta cabecera permite que el navegador realice sniffing de tipos MIME, facilitando la ejecución de archivos maliciosos.
[MEDIA] Referrer-Policy faltante: No se controla la información de referencia enviada a otros sitios, lo que puede filtrar URLs privadas.
[MEDIA] Archivos técnicos expuestos: Los archivos /readme.html y /README.txt son accesibles públicamente, revelando detalles internos del CMS.
[MEDIA] Permissions-Policy faltante: No se restringen las APIs del navegador como cámara o micrófono, aumentando la superficie de ataque.
[BAJA] Cabecera Server expuesta: El servidor revela el uso de Apache, lo que asiste en las fases de reconocimiento de un atacante.
[BAJA] Meta generator expuesto: Se detecta la versión AMP for WP 1.0.97, facilitando el perfilado tecnológico del sitio.