EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://solucionescuba.com	Checks	9 pruebas
Dominio	solucionescuba.com	Hallazgos	57 totales
Fecha	21 de mayo de 2026 a las 15:13	Problemas	12 detectados

C

74/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio solucionescuba.com arroja una puntuación de 74/100, lo que corresponde a una calificación de grado C. Se ejecutaron un total de 9 checks pasivos, resultando en 6 verificaciones satisfactorias, 2 advertencias y 1 fallo crítico en la configuración de seguridad. Si bien la base del cifrado de datos es sólida, la ausencia total de cabeceras de protección y la gestión deficiente de cookies exponen la plataforma a riesgos evitables. En su estado actual, el sitio se considera vulnerable a ataques de manipulación de sesión y ataques dirigidos al navegador del usuario.

Resumen de Riesgos

0	6	4	2	45
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 59 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	No se detecto un CMS conocido
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	83	AVISO	sc_vid: falta HttpOnly; sc_sid: falta HttpOnly
Contenido Mixto	100	OK	No se detecto contenido mixto
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 59 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  59 dias restantes (expira: 2026-07-19T17:02:35.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-20T17:02:36.000Z
- 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/8.4.21, 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://solucionescuba.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

No se detecto un CMS conocido

- INFO **WordPress**
  No detectado
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  No detectado
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- INFO **Tecnologias detectadas**
  PHP/8.4.21, PleskLin

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- INFO **Archivo /README.txt**
  No accesible (correcto)
- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 83/100

Estado: AVISO

sc_vid: falta HttpOnly; sc_sid: falta HttpOnly

- INFO **Cookies detectadas**
  4 cookie(s) encontrada(s)
- ALTO **Cookie: sc_vid — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: sc_vid — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: sc_vid — SameSite**
  SameSite=lax
- ALTO **Cookie: sc_sid — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: sc_sid — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: sc_sid — SameSite**
  SameSite=lax
- INFO **Cookie: sc_vid — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: sc_vid — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: sc_vid — SameSite**
  SameSite=lax
- INFO **Cookie: sc_sid — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: sc_sid — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: sc_sid — SameSite**
  SameSite=lax

Contenido Mixto — 100/100

Estado: OK

No se detecto contenido mixto

- INFO **Contenido mixto**
  Todos los recursos se cargan por HTTPS

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (72 bytes)
- INFO **Reglas robots.txt**
  0 Disallow, 1 Allow
- INFO **Sitemap en robots.txt**
  https://solucionescuba.com/sitemap.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] Falta de Content-Security-Policy: La ausencia de esta cabecera permite ataques de inyección de contenido y Cross-Site Scripting (XSS).
[HIGH] Falta de X-Frame-Options: Al no estar configurada, el sitio es susceptible a ataques de clickjacking mediante el uso de marcos externos.
[HIGH] Falta de Strict-Transport-Security: La carencia de HSTS impide que el sitio obligue a los navegadores a usar exclusivamente conexiones HTTPS seguras.
[HIGH] Cookies sc_vid y sc_sid sin flag HttpOnly: Estas cookies de sesión son accesibles vía scripts, facilitando el robo de identidad ante una vulnerabilidad XSS.
[MEDIUM] Falta de X-Content-Type-Options: Permite que el navegador realice sniffing de tipos MIME, lo que puede derivar en la ejecución de archivos maliciosos.
[MEDIUM] Falta de Referrer-Policy: No se controla qué información de navegación se envía a sitios externos cuando un usuario hace clic en un enlace.
[MEDIUM] Falta de Permissions-Policy: No se restringe el acceso a funciones sensibles del dispositivo del usuario como cámara, micrófono o geolocalización.
[MEDIUM] Archivo /readme.html accesible: La exposición de este archivo puede revelar detalles técnicos sobre la arquitectura interna del sitio.
[LOW] Cabecera Server expuesta: Revela explícitamente el uso de la tecnología nginx, ayudando a posibles atacantes a perfilar el servidor.
[LOW] Cabecera X-Powered-By expuesta: Indica el uso de PHP/8.4.21 y PleskLin, permitiendo identificar versiones específicas para buscar exploits conocidos.