EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.espac.com.cu	Checks	9 pruebas
Dominio	www.espac.com.cu	Hallazgos	49 totales
Fecha	4 de mayo de 2026 a las 17:48	Problemas	8 detectados

B

82/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web ha arrojado una puntuación de 82/100, lo que representa una calificación de grado B. Durante la auditoría se ejecutaron un total de 9 checks pasivos, obteniendo 6 resultados satisfactorios, 1 advertencia y 2 fallos críticos relacionados con la exposición de información y contenido mixto. Aunque la infraestructura de cifrado es robusta, la visibilidad de versiones específicas del software supone un riesgo de reconocimiento para posibles atacantes. Se concluye que el sitio es moderadamente seguro, pero se considera vulnerable debido a que la versión del CMS está expuesta públicamente. La ausencia de un pentest activo deja fuera del radar posibles vulnerabilidades en la lógica de la aplicación que deben ser evaluadas.

Resumen de Riesgos

0	1	4	3	41
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 48 dias
Cabeceras de Seguridad	100	OK	Todas las cabeceras de seguridad presentes
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
Deteccion CMS	100	OK	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 6.8.3 expuesta
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 48 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  48 dias restantes (expira: 2026-06-21T17:45:56.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-23T17:45:57.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 100/100

Estado: OK

Todas las cabeceras de seguridad presentes

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

- INFO **Content-Security-Policy**
  Presente: upgrade-insecure-requests;
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=63072000
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: strict-origin-when-cross-origin
- INFO **Permissions-Policy**
  Presente: accelerometer=(), autoplay=(), camera=(), cross-origin-isolated=(), display-capt...

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 302 redirige a https://www.espac.com.cu
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=63072000
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- INFO **HSTS max-age**
  max-age=63072000 (730 dias)
- 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 6.8.3
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.8.3 expuesta

- ALTO **WordPress version**
  Version 6.8.3 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

7 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://gmpg.org/xfn/11
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.espac.com.cu
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://instagram.com/espac.cuba
- MEDIO **href (link/stylesheet)**
  ...y 4 mas del mismo tipo

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta robots.txt

- BAJO **robots.txt**
  No encontrado (HTTP 403)
- INFO **sitemap.xml**
  Presente, ? 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

[HIGH] Versión de WordPress expuesta: La versión 6.8.3 es visible en el código fuente, permitiendo a los atacantes identificar vulnerabilidades específicas (CVEs) para esta versión.
[MEDIUM] Contenido mixto detectado: Existen 7 recursos cargados mediante protocolo HTTP inseguro dentro de la página HTTPS, lo que podría permitir ataques de degradación de seguridad.
[LOW] Falta de archivo robots.txt: No se encontró el archivo o el acceso está prohibido (403), lo que impide una gestión adecuada del rastreo de los motores de búsqueda.
[LOW] Cabecera de servidor expuesta: El servidor responde con la cabecera Server: Apache, revelando la tecnología subyacente del sistema a cualquier usuario.
[LOW] Meta generator expuesto: La etiqueta meta generator confirma el uso de WordPress 6.8.3, facilitando las labores de enumeración de tecnologías.