EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://cncs.gob.do/	Checks	9 pruebas
Dominio	cncs.gob.do	Hallazgos	46 totales
Fecha	1 de septiembre de 2026 a las 12:39	Problemas	6 detectados

B

87/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio cncs.gob.do ha arrojado una puntuación de 87/100, lo que corresponde a una calificación de grado B. Durante el proceso se ejecutaron 9 checks pasivos, resultando en 6 verificaciones satisfactorias, 1 advertencia por falta de archivos de configuración y 1 fallo crítico relacionado con la gestión de sesiones. A pesar de contar con una infraestructura de cifrado y cabeceras de seguridad impecable, la exposición de versiones de software y la configuración deficiente de las cookies representan un riesgo para la integridad de los usuarios. Se concluye que el sitio es generalmente seguro, pero presenta vulnerabilidades técnicas que deben ser mitigadas para evitar ataques de secuestro de sesión.

Resumen de Riesgos

0	2	1	3	40
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 39 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
Seguridad de Cookies	0	FALLO	PHPSESSID: falta HttpOnly; PHPSESSID: falta Secu...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta robots.txt
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 39 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  39 dias restantes (expira: 2026-10-11T00:04:27.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-07-13T00:04:28.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 100/100

Estado: OK

Todas las cabeceras de seguridad presentes

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.3.29 — Revela framework/lenguaje

- INFO **Content-Security-Policy**
  Presente: upgrade-insecure-requests;
- INFO **X-Frame-Options**
  Presente: sameorigin
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; includesubdomains
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: strict-origin
- INFO **Permissions-Policy**
  Presente: geolocation=(), camera=(), microphone=()

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://cncs.gob.do/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000; includesubdomains
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 dias)
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

CMS detectado: WordPress

- INFO **WordPress**
  Detectado via HTML body
- 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
- BAJO **Meta generator**
  Expone: WordPress 6.7.7
- INFO **Tecnologias detectadas**
  PHP/8.3.29

Seguridad de Cookies — 0/100

Estado: FALLO

PHPSESSID: falta HttpOnly; PHPSESSID: falta Secure; PHPSESSID: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)

- ALTO **Cookie: PHPSESSID — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: PHPSESSID — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: PHPSESSID — SameSite**
  Falta SameSite — Vulnerable a CSRF

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 — 60/100

Estado: AVISO

Falta robots.txt

- BAJO **robots.txt**
  No encontrado (HTTP 404)
- INFO **sitemap.xml**
  Presente, ? URLs
- 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

[HIGH] Falta de flag HttpOnly en cookie PHPSESSID: La ausencia de este atributo permite que la cookie de sesión sea accesible mediante scripts, aumentando el riesgo de ataques Cross-Site Scripting (XSS).
[HIGH] Falta de flag Secure en cookie PHPSESSID: Al no tener activado este flag, la cookie de sesión podría ser transmitida a través de conexiones no cifradas, facilitando su interceptación.

[MEDIUM] Falta de flag SameSite en cookie PHPSESSID: La omisión de este parámetro hace que el sitio sea susceptible a ataques de falsificación de solicitudes en sitios cruzados (CSRF).
[LOW] Exposición de cabecera X-Powered-By: El servidor revela el uso de PHP/8.3.29, proporcionando información valiosa a posibles atacantes sobre la tecnología subyacente.
[LOW] Exposición de versión de CMS vía Meta Generator: Se detectó el uso de WordPress 6.7.7, lo que permite identificar vulnerabilidades específicas asociadas a dicha versión.
[LOW] Ausencia de archivo robots.txt: No se encontró el archivo de directivas de rastreo (HTTP 404), lo que puede afectar la indexación y la gestión de bots.
[ERROR] Tiempo de espera agotado (Timeout): Un check no pudo completarse tras 15 segundos, lo que sugiere posibles bloqueos o latencia excesiva en ciertos servicios de red.