EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.radio26.icrt.cu	Checks	9 pruebas
Dominio	www.radio26.icrt.cu	Hallazgos	50 totales
Fecha	3 de mayo de 2026 a las 12:50	Problemas	13 detectados

C

62/100

puntos de seguridad

RESUMEN EJECUTIVO

Tras realizar el análisis de seguridad, el sitio web presenta una puntuación de 62/100 y una nota final de C. Se ejecutaron un total de 9 checks pasivos, de los cuales 5 resultaron correctos, 1 generó una advertencia y 3 finalizaron en fallo. No se llevó a cabo un pentest activo durante este ciclo de auditoría. Debido a la ausencia de cabeceras de seguridad críticas y a la gestión deficiente de las cookies de sesión, se concluye que el sitio es actualmente vulnerable a diversos vectores de ataque.

Resumen de Riesgos

0	4	7	2	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 58 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
Deteccion CMS	100	OK	CMS detectado: WordPress, Drupal, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 2 expuesta
Seguridad de Cookies	0	FALLO	PHPSESSID: falta HttpOnly; PHPSESSID: falta Secu...
Contenido Mixto	60	AVISO	2 recurso(s) HTTP en pagina HTTPS
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 58 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  58 dias restantes (expira: 2026-06-30T09:09:29.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-01T09:09:30.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 20/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: nginx — 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
- INFO **Strict-Transport-Security**
  Presente: max-age=15768000
- 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 — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://www.radio26.icrt.cu/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=15768000
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- INFO **HSTS max-age**
  max-age=15768000 (183 dias)
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

CMS detectado: WordPress, Drupal, PrestaShop

- INFO **WordPress**
  Detectado via HTML body
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  Detectado via HTML body
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  Detectado via HTML body
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 2 expuesta

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

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 — 60/100

Estado: AVISO

2 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://gmpg.org/xfn/11
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://twitter.com/share?text=INICIO&url=https://www.ra...

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (159 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://www.radio26.cu/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] Content-Security-Policy: La ausencia de esta cabecera permite ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[HIGH] X-Frame-Options: No está configurada, lo que expone a los usuarios a ataques de secuestro de clics o clickjacking.
[HIGH] Cookie PHPSESSID (HttpOnly): La falta de este flag permite que la cookie de sesión sea accesible mediante scripts, aumentando el riesgo de robo de identidad.
[HIGH] Cookie PHPSESSID (Secure): El flag Secure no está presente, permitiendo que la cookie se transmita por canales no cifrados.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite al navegador realizar MIME-type sniffing, lo que puede derivar en la ejecución de archivos no seguros.
[MEDIUM] Referrer-Policy: No existe control sobre la información de referencia enviada a otros sitios, lo que puede filtrar datos internos.
[MEDIUM] Permissions-Policy: No se restringe el acceso a las APIs del navegador como la cámara o el micrófono, afectando la privacidad.
[MEDIUM] Versión CMS Expuesta: El archivo /readme.html es accesible públicamente y revela el uso de una versión de WordPress, facilitando ataques dirigidos.
[MEDIUM] Cookie PHPSESSID (SameSite): La falta de este atributo hace que el sitio sea vulnerable a ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] Contenido Mixto: Se detectaron recursos cargados mediante HTTP (gmpg.org y twitter.com) dentro de la página protegida por HTTPS.
[LOW] Server header expuesto: El encabezado revela el uso de "nginx", proporcionando información técnica valiosa para un atacante.
[LOW] Ruta sensible en robots.txt: La referencia directa al directorio "admin" en el archivo de rastreo expone rutas de gestión del sitio.