EscanearVulnerabilidades

Informe de Seguridad Web

URL	http://certificacioninternacional.mijp.gob.ve/paginas/CU_responder_preguntas/index.php	Objetivo	pruebas
Dominio	certificacioninternacional.mijp.gob.ve	Hallazgos	38 totales
Fecha	15 de abril de 2026 a las 09:59	Problemas	8 detectados

C

74/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio web ha resultado en una puntuación de 74/100 y una nota C. Se ejecutaron un total de 9 checks pasivos, de los cuales 5 resultaron satisfactorios, se emitió 1 advertencia y se identificó 1 fallo crítico en la configuración de seguridad. La ausencia de un protocolo de transferencia segura y la falta de cabeceras de protección fundamentales exponen la plataforma a riesgos significativos. Debido a estas deficiencias técnicas, se concluye que el sitio es actualmente vulnerable ante ataques de interceptación y manipulación de datos.

Resumen de Riesgos

0	4	3	1	30
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

Cabeceras de Seguridad	35	FALLO	Solo 2/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion HTTPS
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	100	OK	No se encontraron cookies
Contenido Mixto	50	AVISO	El sitio no usa HTTPS, no aplica chequeo de cont...
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

Cabeceras de Seguridad — 35/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, X-Frame-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
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; includeSubDomains; preload
- INFO **X-Content-Type-Options**
  Presente: nosniff
- MEDIO **Referrer-Policy**
  Falta — Controla la informacion de referer enviada
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 0/100

Estado: ERROR

No se pudo verificar la redireccion HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 302 — No redirige a HTTPS

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

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- INFO **Archivo /readme.html**
  No accesible (correcto)
- INFO **Archivo /README.txt**
  No accesible (correcto)
- INFO **Version CMS**
  No se detecta ninguna version expuesta

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 — 50/100

Estado: AVISO

El sitio no usa HTTPS, no aplica chequeo de contenido mixto

- ALTO **Protocolo**
  El sitio no usa HTTPS

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (701 bytes)
- INFO **Reglas robots.txt**
  11 Disallow, 0 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /

- INFO **Sitemap en robots.txt**
  172.16.11.243/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] Ausencia de redirección HTTPS: El sitio web no utiliza cifrado SSL/TLS, permitiendo que la información transferida entre el usuario y el servidor sea capturada por terceros.
[HIGH] Falta de Content-Security-Policy (CSP): La ausencia de esta política facilita la ejecución de ataques Cross-Site Scripting (XSS) y la inyección de contenido malicioso.
[HIGH] Falta de X-Frame-Options: Al no tener configurada esta cabecera, el sitio es susceptible a ataques de clickjacking mediante el uso de marcos o iframes.
[MEDIUM] Ausencia de Referrer-Policy: No se controla la información de referencia enviada a otros dominios, lo que puede comprometer la privacidad de la navegación de los usuarios.
[MEDIUM] Ausencia de Permissions-Policy: El sitio no restringe el acceso a APIs del navegador, dejando abierta la posibilidad de acceso no autorizado a funciones como la cámara o el micrófono.
[MEDIUM] Bloqueo total en robots.txt: El archivo de configuración de rastreo bloquea activamente todo el contenido del sitio, lo que sugiere una configuración de visibilidad restrictiva.
[LOW] Cabecera Server expuesta: Se revela que el servidor utiliza tecnología Apache, proporcionando información técnica valiosa que un atacante podría usar para buscar vulnerabilidades específicas.