EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://minmujer.gob.ve	Checks	9 pruebas
Dominio	minmujer.gob.ve	Hallazgos	49 totales
Fecha	29 de agosto de 2026 a las 18:48	Problemas	12 detectados

C

72/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al portal minmujer.gob.ve ha resultado en una puntuación de 72/100, lo que otorga una calificación de grado C. Durante la evaluación se ejecutaron 9 comprobaciones pasivas, logrando 6 resultados satisfactorios, 1 advertencia y 2 fallos críticos en la configuración. El análisis revela una adecuada implementación del cifrado de datos, pero detecta carencias graves en las cabeceras de seguridad y la exposición de versiones de software. Debido a la visibilidad de la versión del CMS y la ausencia de políticas de protección contra inyecciones, el sitio se considera vulnerable a ataques dirigidos. Es imperativo corregir las brechas de información técnica para fortalecer la postura defensiva del sitio.

Resumen de Riesgos

0	3	5	4	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 64 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, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 7.1 expuesta, WordPress 2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	60	AVISO	1 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 64 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  64 dias restantes (expira: 2026-11-01T11:55:47.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-08-03T11:55:48.000Z
- 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: openresty — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.0.30 — Revela framework/lenguaje
- 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=63072000;includeSubDomains; preload
- 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://minmujer.gob.ve/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=63072000;includeSubDomains; preload
- BAJO **HSTS includeSubDomains**
  HSTS 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 7.1
- INFO **Tecnologias detectadas**
  Next.js, PHP/8.0.30

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 7.1 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 7.1 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- 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 — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://inamujer.gob.ve

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (116 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://minmujer.gob.ve/wp-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] Versión de WordPress expuesta: La versión 7.1 es pública, lo que permite a atacantes identificar y explotar CVEs conocidos específicamente para este software.
[HIGH] Falta de Content-Security-Policy: La ausencia de esta cabecera facilita ataques de Cross-Site Scripting (XSS) y la inyección de contenido malicioso.
[HIGH] Falta de X-Frame-Options: El sitio es vulnerable a ataques de clickjacking, permitiendo que un tercero cargue la web en marcos invisibles para engañar a los usuarios.
[MEDIUM] Falta de X-Content-Type-Options: La carencia de esta directiva permite el sniffing de tipos MIME, lo que podría derivar en la ejecución de scripts disfrazados de archivos estáticos.
[MEDIUM] Contenido Mixto detectado: El recurso http://inamujer.gob.ve se carga de forma insegura, comprometiendo la integridad de la sesión HTTPS.
[MEDIUM] Archivo /readme.html accesible: Este archivo se encuentra expuesto y puede revelar detalles internos y versiones precisas de la instalación del CMS.
[MEDIUM] Falta de Referrer-Policy: No se controla la cantidad de información de navegación que se envía a otros dominios mediante el encabezado referer.
[MEDIUM] Falta de Permissions-Policy: El servidor no restringe el acceso a APIs del navegador, dejando expuestas funcionalidades como la cámara o el micrófono.
[LOW] Cabecera de servidor expuesta: El encabezado Server: openresty revela la tecnología del servidor web, facilitando el reconocimiento previo a un ataque.
[LOW] X-Powered-By expuesto: Se detecta la versión PHP/8.0.30, lo que proporciona información valiosa sobre el framework a potenciales atacantes.
[LOW] Meta generator expuesto: El código fuente revela explícitamente WordPress 7.1, simplificando la tarea de inventariado para usuarios malintencionados.
[LOW] Ruta sensible en robots.txt: La mención directa a rutas de administración permite a los atacantes mapear áreas restringidas del sitio.