EscanearVulnerabilidades

Informe de Seguridad Web

URL	http://citasmedicas.espromedbio.gob.ve/salud/	Checks	9 pruebas
Dominio	citasmedicas.espromedbio.gob.ve	Hallazgos	37 totales
Fecha	30 de abril de 2026 a las 17:52	Problemas	12 detectados

D

59/100

puntos de seguridad

RESUMEN EJECUTIVO

El analisis de seguridad realizado al portal web ha arrojado una puntuacion de 59/100, obteniendo una nota de D. Durante la evaluacion se ejecutaron 9 checks pasivos, de los cuales 4 resultaron conformes, 1 presento advertencias y 2 fueron calificados como fallos criticos de seguridad. La infraestructura actual carece de protocolos de cifrado basicos y protecciones contra ataques web comunes mediante cabeceras de respuesta. Debido a la ausencia de certificados SSL y la exposicion de informacion del servidor, se concluye que el sitio es vulnerable y representa un riesgo para la privacidad de los datos.

Resumen de Riesgos

1	5	3	3	25
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	0	ERROR	No se pudo verificar SSL/TLS
Cabeceras de Seguridad	0	FALLO	Solo 0/6 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	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 0/100

Estado: ERROR

No se pudo verificar SSL/TLS

- CRITICO **Conexion SSL**
  No se pudo establecer conexion SSL/TLS

Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: Apache/2.4.66 (Debian) — 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
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)

- 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 — 0/100

Estado: ERROR

No se pudo verificar la redireccion HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — 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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  No encontrado (HTTP 404)
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- 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

[CRITICAL] Conexion SSL: No se pudo establecer una conexion cifrada SSL/TLS, permitiendo la interceptacion de trafico de red.
[HIGH] HTTP -> HTTPS redireccion: El servidor responde a peticiones bajo el protocolo HTTP sin forzar una conexion segura.
[HIGH] Protocolo: El sitio opera exclusivamente bajo HTTP, lo cual es una practica altamente insegura para el manejo de informacion.
[HIGH] Content-Security-Policy: La falta de esta cabecera permite la ejecucion de scripts no autorizados y ataques de inyeccion de contenido.
[HIGH] X-Frame-Options: Al no estar presente, el sitio es susceptible a ataques de clickjacking mediante el uso de iframes.
[HIGH] Strict-Transport-Security: No se aplica la politica HSTS, impidiendo que los navegadores exijan siempre una conexion cifrada.
[MEDIUM] X-Content-Type-Options: La ausencia de esta directiva permite que los navegadores realicen sniffing de tipos MIME, aumentando el riesgo de ejecucion de archivos maliciosos.
[MEDIUM] Referrer-Policy: No se controla la informacion de procedencia enviada a otros dominios en las peticiones salientes.
[MEDIUM] Permissions-Policy: El sitio no restringe el acceso de las APIs del navegador a componentes sensibles como camara o microfono.
[LOW] Server header expuesto: La cabecera revela el uso de Apache/2.4.66 (Debian), facilitando a posibles atacantes la busqueda de vulnerabilidades especificas de esa version.
[LOW] robots.txt y sitemap.xml: La ausencia de estos archivos dificulta el control de la indexacion y revela una falta de mantenimiento en la estructura publica del sitio.