EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://sibompps.farmapatria.com.ve/	Checks	9 pruebas
Dominio	sibompps.farmapatria.com.ve	Hallazgos	45 totales
Fecha	30 de abril de 2026 a las 17:46	Problemas	13 detectados

C

62/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado al dominio https://sibompps.farmapatria.com.ve/ arroja una puntuación de 62/100, lo que equivale a una calificación de grado C. Durante la evaluación se ejecutaron un total de 9 comprobaciones pasivas, de las cuales 5 resultaron satisfactorias, 1 generó una advertencia y 3 fueron clasificadas como fallos. Los resultados evidencian una carencia absoluta de cabeceras de seguridad esenciales y deficiencias críticas en la configuración de las cookies de sesión. Debido a la falta de protecciones contra ataques de inyección y suplantación, el sitio se considera actualmente vulnerable.

Resumen de Riesgos

0	6	4	3	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 34 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
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	0	FALLO	PHPSESSID: falta HttpOnly; PHPSESSID: falta Secu...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 34 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  34 dias restantes (expira: 2026-06-03T15:03:11.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-05T15:03:12.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

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 — 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://sibompps.farmapatria.com.ve/
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

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 — 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 — 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

[HIGH] Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de scripts maliciosos y ataques de inyección de contenido XSS.

[HIGH] X-Frame-Options: Al no estar configurada, el sitio es susceptible a ataques de clickjacking mediante el uso de marcos invisibles.
[HIGH] Strict-Transport-Security: La falta de HSTS impide que el navegador obligue a establecer conexiones seguras, permitiendo degradaciones a HTTP.
[HIGH] Cookie PHPSESSID - HttpOnly: La falta de este flag permite que scripts maliciosos accedan a la cookie de sesión, facilitando el robo de cuentas.
[HIGH] Cookie PHPSESSID - Secure: La cookie puede ser enviada a través de conexiones no cifradas, exponiendo el identificador de sesión a interceptores.
[MEDIUM] X-Content-Type-Options: La ausencia de la opción nosniff permite que el navegador interprete archivos con tipos MIME incorrectos, facilitando ataques de ejecución.
[MEDIUM] Cookie PHPSESSID - SameSite: La falta de este atributo hace que el sitio sea vulnerable a ataques de falsificación de petición en sitios cruzados o CSRF.
[MEDIUM] Referrer-Policy: No existe control sobre la información de navegación que se envía a terceros cuando el usuario hace clic en enlaces externos.
[MEDIUM] Permissions-Policy: No se restringe el acceso de las APIs del navegador a componentes sensibles como la cámara o el micrófono.
[LOW] Server header expuesto: El servidor revela el uso de Apache, lo que proporciona información técnica valiosa para un atacante potencial.
[LOW] Archivos ausentes: No se detectaron los archivos robots.txt ni sitemap.xml, lo que dificulta la auditoría y la gestión de indexación.