EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://spoo.me/Pagina-Correos	Checks	9 pruebas
Dominio	spoo.me	Hallazgos	50 totales
Fecha	3 de abril de 2026 a las 20:10	Problemas	11 detectados

C

69/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada sobre el sitio web ha dado como resultado una puntuación de 69/100, obteniendo una calificación de nota C. Durante el análisis se ejecutaron un total de 9 comprobaciones pasivas, de las cuales 6 resultaron satisfactorias, 1 generó una advertencia y 2 finalizaron con errores críticos. A pesar de contar con un cifrado de conexión adecuado, la ausencia total de cabeceras de protección y la configuración deficiente de las cookies de sesión representan un riesgo significativo. Se concluye que el sitio es actualmente vulnerable ante ataques de interceptación de datos, clickjacking e inyección de contenido. Es imperativo aplicar las correcciones técnicas detalladas para mejorar la postura de seguridad de la plataforma.

Resumen de Riesgos

0	4	5	2	39
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 33 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
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	33	FALLO	PHPSESSID: falta Secure; PHPSESSID: falta SameSi...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 33 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  33 dias restantes (expira: 2026-05-06T22:17:08.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-05T21:19:43.000Z
- 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

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.1.33 — Revela framework/lenguaje
- 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 — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://spoo.me/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=63072000
- BAJO **HSTS includeSubDomains**
  HSTS no 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

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
- INFO **Tecnologias detectadas**
  PHP/8.1.33

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 — 33/100

Estado: FALLO

PHPSESSID: falta Secure; PHPSESSID: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: PHPSESSID — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- 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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (60 bytes)
- INFO **Reglas robots.txt**
  0 Disallow, 1 Allow
- INFO **Sitemap en robots.txt**
  https://spoo.me/sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- 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)**
  Abierto (esperado) — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Abierto (esperado) — 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
- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — 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 código (XSS).
[HIGH] X-Frame-Options: El sitio permite ser cargado dentro de frames, lo que facilita ataques de secuestro de clics o clickjacking.
[HIGH] Strict-Transport-Security: No se fuerza el uso de conexiones seguras mediante HSTS, permitiendo ataques de degradación de protocolo.
[HIGH] Cookie PHPSESSID - Secure: La falta del flag Secure permite que la cookie de sesión se transmita a través de conexiones HTTP no cifradas.
[MEDIUM] X-Content-Type-Options: La falta de esta directiva permite que el navegador realice sniffing de tipos MIME, facilitando la ejecución de archivos maliciosos.
[MEDIUM] Referrer-Policy: No se controla la información de referencia enviada a otros dominios, lo que podría exponer rutas internas sensibles.
[MEDIUM] Permissions-Policy: No se restringen las capacidades del navegador como el acceso a la cámara o micrófono, aumentando la superficie de ataque.
[MEDIUM] Cookie PHPSESSID - SameSite: La ausencia de este atributo hace que las sesiones de los usuarios sean vulnerables a ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] Puerto 8080 (HTTP-Alt): Se detectó un puerto alternativo abierto que podría exponer servicios administrativos o proxies no protegidos.
[LOW] Server header expuesto: El servidor revela que utiliza tecnología Apache, ayudando a un atacante a identificar vulnerabilidades específicas de la versión.
[LOW] X-Powered-By expuesto: El sitio informa explícitamente el uso de PHP/8.1.33, lo cual facilita el reconocimiento de la infraestructura técnica.