EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.iumiukycursosveterinaria.com	Checks	9 pruebas
Dominio	www.iumiukycursosveterinaria.com	Hallazgos	57 totales
Fecha	13 de abril de 2026 a las 18:19	Problemas	16 detectados

C

70/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web arroja una puntuación de 70/100, lo que corresponde a una calificación de C. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 1 presentó advertencias y 2 fallaron críticamente. A pesar de contar con un cifrado SSL robusto, el sitio presenta deficiencias graves en la implementación de cabeceras de seguridad y en la protección de cookies de sesión. La ausencia de mecanismos de protección modernos expone a los usuarios a ataques de interceptación y suplantación. En su estado actual, el sitio se considera vulnerable debido a configuraciones de servidor incompletas.

Resumen de Riesgos

0	10	4	2	41
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 90 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	CMS detectado: PrestaShop
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	42	FALLO	configuracion: falta HttpOnly; configuracion: fa...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 90 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  90 dias restantes (expira: 2026-07-12T13:52:57.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-06-10T13:52:57.000Z
- 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/2.4.66 (Win64) OpenSSL/3.6.0 mod_fcgid/2.3.10-dev — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.5.1 — 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://www.iumiukycursosveterinaria.com/
- 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

CMS detectado: PrestaShop

- INFO **WordPress**
  No detectado
- 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
- INFO **Tecnologias detectadas**
  PHP/8.5.1

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 — 42/100

Estado: FALLO

configuracion: falta HttpOnly; configuracion: falta Secure; PHPSESSID: falta HttpOnly; PHPSESSID: falta Secure; PHPSESSID: falta SameSite; origenCaptacion: falta Secure; gMarketing: falta Secure

- INFO **Cookies detectadas**
  4 cookie(s) encontrada(s)
- ALTO **Cookie: configuracion — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: configuracion — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: configuracion — SameSite**
  SameSite=lax
- 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
- INFO **Cookie: origenCaptacion — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: origenCaptacion — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: origenCaptacion — SameSite**
  SameSite=lax
- INFO **Cookie: gMarketing — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: gMarketing — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: gMarketing — SameSite**
  SameSite=lax

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 (102 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 1 Allow
- INFO **Sitemap en robots.txt**
  http://www.galeriadelcoleccionista.com/sitemap
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

2 puerto(s) abierto(s), todos esperados

- 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
- 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] Strict-Transport-Security: Falta la configuración HSTS, lo que impide forzar conexiones HTTPS y permite ataques de degradación de protocolo.
[HIGH] Content-Security-Policy: Ausencia total de esta cabecera, dejando el sitio desprotegido frente a ataques de Cross-Site Scripting (XSS) e inyección de contenido.
[HIGH] X-Frame-Options: No se detectó esta cabecera, lo que hace al sitio susceptible a ataques de clickjacking mediante marcos maliciosos.
[HIGH] Cookie PHPSESSID insegura: La cookie de sesión carece de los flags HttpOnly y Secure, permitiendo su robo mediante scripts o tráfico no cifrado.
[HIGH] Cookies de terceros inseguras: Las cookies origenCaptacion y gMarketing no poseen el flag Secure, comprometiendo la privacidad en redes abiertas.
[MEDIUM] X-Content-Type-Options: Al no estar presente, el navegador podría interpretar archivos de forma incorrecta (MIME-sniffing), facilitando la ejecución de malware.
[MEDIUM] Referrer-Policy: La falta de esta política provoca que se envíe información sensible sobre la procedencia del usuario a sitios externos.
[MEDIUM] Permissions-Policy: No existen restricciones sobre el uso de hardware del navegador como la cámara, el micrófono o la ubicación.
[MEDIUM] Cookie PHPSESSID sin SameSite: La falta de este atributo aumenta el riesgo de ataques de falsificación de solicitud en sitios cruzados (CSRF).
[LOW] Exposición de cabecera Server: El servidor revela explícitamente el uso de Apache/2.4.66 y OpenSSL/3.6.0, facilitando el reconocimiento para exploits específicos.
[LOW] Exposición de cabecera X-Powered-By: Se muestra públicamente la versión PHP/8.5.1 utilizada por el sistema.