

EscanearVulnerabilidades

Informe de Seguridad Web

URL https://app.labpy.site
Dominio app.labpy.site
Fecha 2 de octubre de 2026 a las 20:11

Checks 9 pruebas
Hallazgos 41 totales
Problemas 11 detectados

D

57/100

puntos de seguridad



RESUMEN EJECUTIVO

La auditoría técnica realizada al sitio web arroja una puntuación exacta de 57/100, lo que equivale a una nota D. Durante el análisis se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 1 presenta advertencias y 3 fallaron de forma crítica. El sistema muestra una gestión adecuada del certificado digital, pero presenta deficiencias graves en la configuración de cabeceras de seguridad y en la redirección de tráfico cifrado. Debido a la ausencia de políticas de protección básicas y la exposición de servicios en puertos alternativos, el sitio se clasifica actualmente como vulnerable.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 67 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a 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	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 67 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
67 dias restantes (expira: 2026-12-08T15:58:21.000Z)
- INFO Fecha de emision
Emitido desde: 2026-09-09T15:09:11.000Z
- 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: cloudflare — 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: FALLO

No hay redireccion HTTP a HTTPS

- ALTO

HTTP !' HTTPS redireccion
HTTP 200 — No redirige a HTTPS
- 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 — 100/100

Estado: OK

No se encontraron cookies

● INFO **Cookies detectadas**
El sitio no establece cookies en la respuesta inicial

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 **sitemap.xml**
No encontrado (HTTP 404)

● 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] HTTP -> HTTPS redireccion: El servidor responde con código 200 en conexiones HTTP, lo que permite el acceso no cifrado y expone los datos del usuario a interceptaciones.

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

[HIGH] X-Frame-Options: La falta de esta configuración deja al sitio desprotegido ante ataques de clickjacking, permitiendo que la web sea cargada en marcos externos.

[HIGH] Strict-Transport-Security: No se ha configurado la política HSTS, por lo que el navegador no fuerza el uso de HTTPS de manera permanente.

[MEDIUM] X-Content-Type-Options: El sitio es vulnerable al MIME-type sniffing, permitiendo que el navegador interprete archivos de forma distinta a la declarada.

[MEDIUM] Referrer-Policy: No existe un control sobre la información de navegación que se envía a terceros cuando se hace clic en enlaces externos.

[MEDIUM] Permissions-Policy: No se restringen las capacidades del navegador, dejando abiertas APIs sensibles como la cámara, micrófono o geolocalización.

[MEDIUM] Puerto 8080 (HTTP-Alt): Este puerto se encuentra abierto y expone un servidor web alternativo que incrementa la superficie de ataque.

[LOW] Server header expuesto: Se revela el uso de Cloudflare como tecnología de servidor, proporcionando información técnica que puede ser usada por atacantes.

[LOW] sitemap.xml: El archivo de mapa del sitio no fue encontrado, lo que dificulta la auditoría de estructura y la indexación correcta.