

EscanearVulnerabilidades

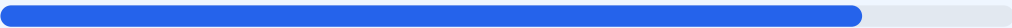
Informe de Seguridad Web

URL	https://yolmanamaya.com	Checks	9 pruebas
Dominio	yolmanamaya.com	Hallazgos	48 totales
Fecha	22 de julio de 2026 a las 22:49	Problemas	2 detectados

B

85/100

puntos de seguridad



RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web yolmanamaya.com arroja una puntuación de 85/100, lo que se traduce en una calificación de grado B. El análisis consistió en 9 comprobaciones pasivas, de las cuales 8 resultaron exitosas y 1 presentó un fallo crítico de configuración. Aunque el sitio cuenta con un certificado SSL válido y cabeceras de seguridad correctamente implementadas, la ausencia de una redirección forzada al protocolo seguro compromete la integridad de la conexión. Debido a este fallo específico en la gestión del tráfico, se concluye que el sitio es vulnerable a ataques de interceptación de datos. Es imperativo corregir la configuración del servidor para garantizar la navegación segura de los usuarios.

Resumen de Riesgos

0	1	0	1	46
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 89 dias
Cabeceras de Seguridad	100	OK	Todas las cabeceras de seguridad presentes
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	1 cookies, todas con flags correctos
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	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 89 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
89 dias restantes (expira: 2026-10-20T01:58:09.000Z)
- INFO Fecha de emision
Emitido desde: 2026-07-22T01:58:10.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 100/100

Estado: OK

Todas las cabeceras de seguridad presentes

- BAJO Server header expuesto
Server: Apache — Revela tecnologia del servidor

- INFO

Content-Security-Policy
Presente: default-src 'self'; base-uri 'self'; frame-ancestors 'self'; form-action 'self';...
- INFO

X-Frame-Options
Presente: SAMEORIGIN
- INFO

Strict-Transport-Security
Presente: max-age=31536000; includeSubDomains
- INFO

X-Content-Type-Options
Presente: nosniff
- INFO

Referrer-Policy
Presente: strict-origin-when-cross-origin
- INFO

Permissions-Policy
Presente: camera=(), microphone=(), geolocation=(), payment=()

Redireccion HTTPS — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO

HTTP !' HTTPS redireccion
HTTP 200 — No redirige a HTTPS
- INFO

HSTS (Strict-Transport-Security)
HSTS activo: max-age=31536000; includeSubDomains
- BAJO

HSTS includeSubDomains
HSTS cubre subdominios
- INFO

HSTS max-age
max-age=31536000 (365 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

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

1 cookies, todas con flags correctos

- INFO

Cookies detectadas
1 cookie(s) encontrada(s)
- INFO

Cookie: YACMSSESSID — HttpOnly
HttpOnly activo — No accesible via JavaScript
- INFO

Cookie: YACMSSESSID — Secure
Flag Secure activo — Solo se envía por HTTPS
- INFO

Cookie: YACMSSESSID — 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 (179 bytes)
- INFO

Reglas robots.txt
6 Disallow, 1 Allow
- INFO

Sitemap en robots.txt
<https://yolmanamaya.com/sitemap.xml>
- 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 — Envío 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

[ALTA] Ausencia de redirección HTTP a HTTPS: El servidor no redirige automáticamente el tráfico no cifrado al puerto seguro, permitiendo conexiones HTTP 200 que exponen los datos del usuario a ataques de intermediario.

[BAJA] Cabecera de servidor expuesta: Se detectó el campo Server con el valor Apache, lo cual revela la tecnología subyacente y facilita a un atacante la búsqueda de exploits específicos para esa versión de software.