

EscanearVulnerabilidades

Informe de Seguridad Web

URL https://robertoaranda.com
Dominio robertoaranda.com
Fecha 1 de octubre de 2026 a las 15:44

Checks 9 pruebas
Hallazgos 49 totales
Problemas 14 detectados

C

66/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio web arroja una puntuación de 66/100, lo que equivale a una nota de grado C. Durante la evaluación se ejecutaron un total de 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 2 generaron advertencias y 2 terminaron en fallo crítico. Aunque el cifrado de datos es correcto, la ausencia de cabeceras de seguridad y la exposición de versiones técnicas elevan el riesgo de explotación. Por lo tanto, se concluye que el sitio es vulnerable ante ataques de intermediarios y de inyección debido a configuraciones deficientes.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 115 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: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 7.0.6 expuesta, WordPress 2 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	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 115 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
115 dias restantes (expira: 2027-01-24T23:59:59.000Z)
- INFO Fecha de emision
Emitido desde: 2026-07-25T00:00:00.000Z
- 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://robertoaranda.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: WordPress, PrestaShop

- INFO

WordPress
Detectado via HTML body
- 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
- BAJO

Meta generator
Expone: WordPress 7.0.6

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 7.0.6 expuesta, WordPress 2 expuesta

- ALTO

WordPress version
Version 7.0.6 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- MEDIO

Archivo /readme.html
Archivo accesible publicamente — Puede revelar version e informacion del CMS
- INFO

Archivo /README.txt
No accesible (correcto)
- MEDIO

Ruta /wp-login.php
Panel de login accesible publicamente

Seguridad de Cookies — 100/100

Estado: OK

1 cookies, todas con flags correctos

- INFO

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

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

Cookie: PHPSESSID — Secure
Flag Secure activo — Solo se envia por HTTPS
- INFO

Cookie: PHPSESSID — 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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO

robots.txt
Presente (269 bytes)
- INFO

Reglas robots.txt
6 Disallow, 1 Allow
- BAJO

Ruta sensible en robots.txt
Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- BAJO

sitemap.xml
No encontrado (HTTP 404)
- 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] Content-Security-Policy: La ausencia de esta cabecera facilita ataques de XSS y de inyección de contenido malicioso.
- [HIGH] X-Frame-Options: Al no estar presente, el sitio es susceptible a ataques de clickjacking donde un atacante puede cargar la web en un marco invisible.
- [HIGH] Strict-Transport-Security: La falta de HSTS impide que el navegador fuerce siempre conexiones HTTPS, permitiendo posibles degradaciones de seguridad.
- [HIGH] WordPress version: La versión 7.0.6 se encuentra expuesta públicamente, lo que permite a atacantes identificar y explotar CVEs específicos conocidos.
- [MEDIUM] X-Content-Type-Options: Falta la protección contra el sniffing de tipos MIME, lo que podría llevar a la ejecución de archivos no seguros.
- [MEDIUM] Referrer-Policy: No existe control sobre la información que se envía en la cabecera referer al navegar hacia enlaces externos.
- [MEDIUM] Permissions-Policy: El sitio no restringe el acceso a APIs sensibles del navegador como la cámara o el micrófono.
- [MEDIUM] Archivo /readme.html: Este archivo es accesible públicamente y revela información técnica sensible sobre la instalación del CMS.
- [MEDIUM] Ruta /wp-login.php: El panel de acceso administrativo está expuesto a internet, facilitando intentos de ataques por fuerza bruta.
- [LOW] Server header expuesto: El servidor revela el uso de Apache, facilitando el reconocimiento de la infraestructura tecnológica por parte de atacantes.
- [LOW] Meta generator: La etiqueta meta expone explícitamente la versión de WordPress en el código fuente.
- [LOW] Ruta sensible en robots.txt: Se hace referencia directa a la ruta "admin", lo que guía a usuarios malintencionados hacia áreas restringidas.
- [LOW] sitemap.xml: No se encontró el archivo de mapa del sitio, lo que dificulta la auditoría de estructura y el indexado correcto.