EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://bautista.arandukasoft.com	Checks	9 pruebas
Dominio	bautista.arandukasoft.com	Hallazgos	50 totales
Fecha	22 de julio de 2026 a las 21:18	Problemas	10 detectados

B

78/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado a bautista.arandukasoft.com arroja una puntuación de 78/100 con una calificación final de B. Durante el proceso se ejecutaron un total de 9 checks pasivos, de los cuales 5 resultaron exitosos, 3 generaron advertencias y 1 fue calificado como fallo crítico. Aunque el sitio cuenta con una implementación de cifrado robusta, la gestión de sesiones y las cabeceras de protección presentan deficiencias importantes. En su estado actual, el sitio web se considera vulnerable debido a fallos en la configuración de cookies y exposición de servicios técnicos.

Resumen de Riesgos

0	4	4	2	40
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 66 dias
Cabeceras de Seguridad	60	AVISO	4/6 presentes. Faltan: Content-Security-Policy, ...
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	17	FALLO	XSRF-TOKEN: falta HttpOnly; XSRF-TOKEN: falta Se...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 66 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  66 dias restantes (expira: 2026-09-27T02:56:19.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-29T02:56:20.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 60/100

Estado: AVISO

4/6 presentes. Faltan: Content-Security-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: Apache/2.4.25 (Debian) — Revela tecnologia del servidor

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: DENY
- INFO **Strict-Transport-Security**
  Presente: max-age:31536000; includeSubDomains
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: no-referrer-when-downgrade
- 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://bautista.arandukasoft.com/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age:31536000; includeSubDomains
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- 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 — 17/100

Estado: FALLO

XSRF-TOKEN: falta HttpOnly; XSRF-TOKEN: falta Secure; XSRF-TOKEN: falta SameSite; laravel_session: falta Secure; laravel_session: falta SameSite

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- ALTO **Cookie: XSRF-TOKEN — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: XSRF-TOKEN — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: XSRF-TOKEN — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: laravel_session — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: laravel_session — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: laravel_session — 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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (24 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- 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): 22 (SSH)

- INFO **Puerto 21 (FTP)**
  Cerrado — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — 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] Cookie: XSRF-TOKEN - Falta flag HttpOnly: La cookie es accesible mediante scripts del navegador, facilitando el robo de sesiones mediante ataques XSS.
[HIGH] Cookie: XSRF-TOKEN - Falta flag Secure: La información de seguridad se transmite por canales no cifrados, permitiendo su interceptación.
[HIGH] Cookie: laravel_session - Falta flag Secure: La cookie de sesión principal no está protegida contra transmisiones en texto plano.
[HIGH] Content-Security-Policy: La ausencia de esta cabecera impide restringir el origen del contenido, dejando el sitio expuesto a inyecciones de código.
[MEDIUM] Cookie: XSRF-TOKEN - Falta flag SameSite: El sitio es vulnerable a ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] Cookie: laravel_session - Falta flag SameSite: No existe restricción para el envío de la cookie de sesión desde dominios externos.
[MEDIUM] Permissions-Policy: Falta esta cabecera, lo que impide limitar el acceso del navegador a funciones sensibles como cámara o micrófono.
[MEDIUM] Puerto 22 (SSH) abierto: La exposición de este puerto permite intentos de acceso remoto al servidor si no está debidamente restringido.
[LOW] Server header expuesto: El servidor revela el uso de Apache/2.4.25 (Debian), facilitando la búsqueda de exploits específicos para esa versión.
[LOW] sitemap.xml: El archivo no fue encontrado, lo que dificulta la indexación y visibilidad de la estructura del sitio.