EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.cafelindo.es	Checks	9 pruebas
Dominio	www.cafelindo.es	Hallazgos	48 totales
Fecha	1 de junio de 2026 a las 06:10	Problemas	10 detectados

B

78/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el dominio cafelindo.es ha resultado en una puntuación de 78/100, lo que equivale a una calificación de grado B. Durante el proceso se ejecutaron un total de 9 checks pasivos, de los cuales 7 finalizaron con éxito y 2 resultaron en fallo crítico. No se llevó a cabo un pentest activo, por lo que los resultados se limitan a la configuración externa y cabeceras visibles. Aunque el sitio web cuenta con una base sólida en cifrado y accesibilidad, se considera vulnerable debido a la ausencia de políticas de seguridad preventivas y la exposición de información técnica sensible.

Resumen de Riesgos

0	3	5	2	38
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 192 dias
Cabeceras de Seguridad	30	FALLO	Solo 2/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
Deteccion CMS	100	OK	CMS detectado: WordPress
Version CMS Expuesta	20	FALLO	WordPress 7.0 expuesta, WordPress 2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
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 192 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  192 dias restantes (expira: 2026-12-09T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-25T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 30/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, 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
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000
- MEDIO **X-Content-Type-Options**
  Falta — Evita MIME-type sniffing
- 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://www.cafelindo.es/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000
- BAJO **HSTS includeSubDomains**
  HSTS no 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

CMS detectado: WordPress

- INFO **WordPress**
  Detectado via HTML body
- 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
- BAJO **Meta generator**
  Expone: WordPress 7.0
- INFO **Tecnologias detectadas**
  React, Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 7.0 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 7.0 expuesta publicamente — Permite a atacantes buscar CVEs conocidos

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS

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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (311 bytes)
- INFO **Reglas robots.txt**
  7 Disallow, 1 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- INFO **Sitemap en robots.txt**
  https://www.cafelindo.es/?feed=xmlsitemap1611
- 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 permite la ejecución de scripts no autorizados, facilitando ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[HIGH] X-Frame-Options: Al no estar presente, el sitio es susceptible a ataques de clickjacking, donde un tercero puede cargar la web en un marco invisible para engañar al usuario.
[HIGH] Versión de WordPress expuesta: Se detecta públicamente que el sitio utiliza WordPress 7.0, lo que permite a posibles atacantes localizar vulnerabilidades específicas y exploits conocidos para dicha versión.
[MEDIUM] X-Content-Type-Options: La falta de esta directiva permite que los navegadores intenten adivinar el tipo de contenido (MIME sniffing), lo que puede derivar en la ejecución de archivos maliciosos disfrazados de elementos inofensivos.
[MEDIUM] Permissions-Policy: No se han restringido las APIs del navegador, dejando abierta la posibilidad de que scripts de terceros accedan a funciones como la cámara, el micrófono o la geolocalización.
[MEDIUM] Archivos informativos expuestos: Los archivos /readme.html y /README.txt son accesibles públicamente, revelando detalles sobre la instalación y el software del sistema.
[MEDIUM] Restricción total en robots.txt: El archivo de configuración bloquea la indexación de todo el sitio mediante la directiva Disallow: /, lo que podría ocultar configuraciones de desarrollo o pruebas dejadas en producción.
[LOW] Server header expuesto: El servidor revela el uso de Apache, lo cual otorga información de reconocimiento valiosa para un atacante sobre la infraestructura subyacente.
[LOW] Meta generator: La etiqueta meta en el código fuente expone explícitamente el uso de WordPress 7.0, facilitando la identificación de la tecnología empleada.