EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://caifiume.it	Checks	9 pruebas
Dominio	caifiume.it	Hallazgos	46 totales
Fecha	26 de julio de 2026 a las 01:17	Problemas	12 detectados

C

67/100

puntos de seguridad

RESUMEN EJECUTIVO

El analisis de seguridad realizado al sitio web ha resultado en una puntuacion de 67/100, lo que equivale a una nota de C. Durante la evaluacion se ejecutaron 9 checks pasivos, de los cuales 5 fueron superados con exito, 2 generaron advertencias y 2 resultaron en fallos criticos. Se han detectado debilidades importantes en la configuracion del servidor y en la exposicion de informacion sensible del CMS. Debido a la falta de cabeceras de seguridad esenciales y la presencia de servicios de transferencia de archivos no cifrados, se concluye que el sitio es vulnerable a ataques de interceptacion y explotacion de vulnerabilidades conocidas.

Resumen de Riesgos

0	6	3	3	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 33 dias
Cabeceras de Seguridad	15	FALLO	Solo 1/6 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 7.0.2 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	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 21 (FTP)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 33 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  33 dias restantes (expira: 2026-08-28T09:49:54.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-30T09:49:55.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 15/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy

- BAJO **Server header expuesto**
  Server: nginx — 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
- INFO **Permissions-Policy**
  Presente: private-state-token-redemption=(self "https://www.google.com" "https://www.gstat...

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://caifiume.it/
- 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 7.0.2
- INFO **Tecnologias detectadas**
  Next.js, Astro

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 7.0.2 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 7.0.2 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)

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 (162 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://www.caifiume.it/sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 21 (FTP)

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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] Puerto 21 (FTP): ABIERTO — El servicio FTP transfiere archivos y credenciales en texto plano, permitiendo el robo de datos.
[HIGH] Content-Security-Policy: Falta — La ausencia de esta cabecera facilita ataques de Cross-Site Scripting (XSS) e inyeccion de contenido malicioso.
[HIGH] X-Frame-Options: Falta — El sitio no bloquea la carga en marcos, lo que lo hace susceptible a ataques de clickjacking.
[HIGH] Strict-Transport-Security: Falta — Al no estar configurado, el navegador no obliga a realizar conexiones HTTPS, permitiendo ataques de degradacion de protocolo.
[HIGH] WordPress version: Version 7.0.2 expuesta publicamente — Revelar la version exacta permite a atacantes automatizar la busqueda de vulnerabilidades especificas (CVEs).
[MEDIUM] X-Content-Type-Options: Falta — Permite que el navegador intente adivinar el tipo de contenido, facilitando ataques de ejecucion de scripts.
[MEDIUM] Referrer-Policy: Falta — No se controla que informacion de navegacion se envia a otros sitios, comprometiendo la privacidad de los usuarios.
[MEDIUM] Archivo /readme.html: Archivo accesible publicamente — Este archivo confirma la infraestructura del sitio y puede ofrecer detalles adicionales sobre la instalacion.
[LOW] Server header expuesto: Server: nginx — Revelar el nombre del software del servidor ayuda a los atacantes a perfilar la infraestructura.
[LOW] Meta generator: Expone: WordPress 7.0.2 — Metadato que confirma nuevamente la version del software utilizado.
[LOW] Ruta sensible en robots.txt: Referencia a "admin" — Indica explicitamente a los rastreadores y atacantes donde se encuentran los paneles de gestion.