EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://intrasoft.es/	Checks	9 pruebas
Dominio	intrasoft.es	Hallazgos	52 totales
Fecha	22 de abril de 2026 a las 08:46	Problemas	16 detectados

C

62/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio web ha arrojado una puntuación de 62/100, otorgando una calificación de grado C. Se realizaron 9 comprobaciones pasivas, de las cuales 4 resultaron satisfactorias, 3 generaron advertencias y 2 fallaron críticamente. El escaneo revela debilidades significativas en la configuración de cabeceras de seguridad y la exposición pública de la versión del sistema de gestión de contenidos. Debido a la ausencia de protecciones esenciales contra ataques de inyección y la presencia de contenido mixto, el sitio se considera actualmente vulnerable ante amenazas externas.

Resumen de Riesgos

0	5	6	5	36
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 37 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 1.0.0 expuesta
Seguridad de Cookies	100	OK	1 cookies, todas con flags correctos
Contenido Mixto	60	AVISO	2 recurso(s) HTTP en pagina HTTPS
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 37 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  37 dias restantes (expira: 2026-05-29T01:03:58.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-28T01:03:59.000Z
- 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: cloudflare — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: WP Engine — Revela framework/lenguaje
- 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://intrasoft.es/
- 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: Elementor 4.0.3; features: additional_custom_breakpoints; settings: css_print_method-external, google_font-enabled, font_display-auto
- INFO **Tecnologias detectadas**
  Next.js, WP Engine

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 1.0.0 expuesta

- ALTO **WordPress version**
  Version 1.0.0 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- INFO **Archivo /readme.html**
  No accesible (correcto)

- 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: __cf_bm — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: __cf_bm — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: __cf_bm — SameSite**
  SameSite=none

Contenido Mixto — 60/100

Estado: AVISO

2 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.peris.es/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.willisnetworks.es/

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (82 bytes)
- INFO **Reglas robots.txt**
  1 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] Version de WordPress expuesta: La version 1.0.0 es visible publicamente, lo que permite a atacantes buscar vulnerabilidades (CVEs) especificas.
[HIGH] Content-Security-Policy: Falta esta cabecera esencial para prevenir ataques de inyeccion de codigo y XSS.
[HIGH] X-Frame-Options: Ausencia de proteccion contra ataques de clickjacking.
[HIGH] Strict-Transport-Security: No se ha configurado HSTS, por lo que el navegador no fuerza conexiones cifradas permanentemente.
[MEDIUM] Contenido Mixto: Se detectaron 2 recursos cargados mediante HTTP en una pagina segura, comprometiendo la integridad del sitio.
[MEDIUM] Ruta /wp-login.php accesible: El panel de acceso administrativo esta expuesto a ataques de fuerza bruta.
[MEDIUM] X-Content-Type-Options: Falta la cabecera para evitar que el navegador realice sniffing de tipos MIME.
[MEDIUM] Referrer-Policy: No existe control sobre la informacion de procedencia enviada en las peticiones salientes.
[MEDIUM] Permissions-Policy: No se restringen las APIs del navegador como la camara o el microfono.
[LOW] Cabeceras de servidor expuestas: Se revela el uso de Cloudflare y WP Engine, facilitando el reconocimiento de la infraestructura.
[LOW] Meta generator: Se exponen detalles de Elementor y configuraciones internas de diseño.
[LOW] Fallos en archivos de rastreo: Falta el archivo sitemap.xml y el robots.txt menciona rutas sensibles como "admin".