EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.incofisadigital.com	Checks	9 pruebas
Dominio	www.incofisadigital.com	Hallazgos	47 totales
Fecha	15 de septiembre de 2026 a las 12:43	Problemas	17 detectados

D

56/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre la plataforma web ha resultado en una puntuación de 56/100, lo que otorga una calificación de grado D. Durante la auditoría se ejecutaron 9 checks pasivos, de los cuales 4 resultaron satisfactorios, 2 generaron advertencias y 3 fallaron debido a configuraciones críticas erróneas. Los hallazgos muestran una exposición severa de servicios de infraestructura y una ausencia total de políticas de seguridad en las cabeceras HTTP. Debido a la visibilidad de la base de datos y versiones del sistema de gestión de contenidos, se concluye que el sitio es actualmente vulnerable y presenta un riesgo elevado de compromiso.

Resumen de Riesgos

1	6	7	3	30
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 50 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
Version CMS Expuesta	20	FALLO	WordPress 4494 expuesta, WordPress 2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	60	AVISO	1 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	20	FALLO	3 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 50 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  50 dias restantes (expira: 2026-11-05T00:20:42.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-08-07T00:20:43.000Z
- 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://www.incofisadigital.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

- 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: Elementor 3.33.1; features: e_font_icon_svg, additional_custom_breakpoints; settings: css_print_method-external, google_font-enabled, font_display-swap
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 4494 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 4494 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

No se encontraron cookies

- INFO **Cookies detectadas**
  El sitio no establece cookies en la respuesta inicial

Contenido Mixto — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://espaciopymes.com/

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (998 bytes)
- INFO **Reglas robots.txt**
  10 Disallow, 2 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://www.incofisadigital.com/sitemap_index.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 20/100

Estado: FALLO

3 puertos riesgosos abiertos

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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
- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — 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

[CRITICAL] Puerto 3306 (MySQL): La base de datos del sitio está expuesta directamente a internet, lo que permite intentos de conexión externa y ataques de fuerza bruta.
[HIGH] Puerto 21 (FTP): Servicio de transferencia de archivos abierto sin cifrado, facilitando la intercepción de credenciales de administración.
[HIGH] Versión de WordPress expuesta: La versión 4494 y la versión 2 son visibles públicamente, permitiendo a atacantes identificar vulnerabilidades específicas ya documentadas.
[HIGH] Content-Security-Policy: Cabecera ausente, lo que deja al sitio sin protección contra inyecciones de código malicioso y ataques XSS.
[HIGH] X-Frame-Options: Falta de configuración contra clickjacking, permitiendo que el sitio sea embebido en marcos externos fraudulentos.
[HIGH] Strict-Transport-Security (HSTS): El servidor no obliga al navegador a usar HTTPS, aumentando el riesgo de ataques de degradación de seguridad.
[MEDIUM] Contenido Mixto: Se detectó un recurso stylesheet cargado mediante protocolo inseguro HTTP desde espaciopymes.com.
[MEDIUM] Archivo /readme.html y ruta /wp-login.php: Archivos de instalación y paneles de acceso expuestos que facilitan el reconocimiento del sistema por parte de terceros.
[MEDIUM] X-Content-Type-Options: Ausencia de protección contra el sniffing de tipos MIME, lo que podría llevar a la ejecución de archivos maliciosos.
[MEDIUM] Referrer-Policy y Permissions-Policy: No existen controles sobre la información de origen enviada ni restricciones sobre el uso de hardware del usuario como cámara o micrófono.
[MEDIUM] Puerto 22 (SSH): Acceso remoto para administración abierto, lo que supone un vector de ataque si no existen políticas de bloqueo de IP.
[LOW] Cabecera Server expuesta: El servidor revela que utiliza tecnología Apache, lo que acota las herramientas de ataque para un adversario.
[LOW] Meta generator: Exposición de detalles de Elementor 3.33.1 y sus configuraciones internas de tipografía y puntos de ruptura.
[LOW] Ruta sensible en robots.txt: El archivo indica la existencia de directorios admin, orientando a rastreadores malintencionados hacia áreas restringidas.