EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://inveralsoluciones.com	Checks	9 pruebas
Dominio	inveralsoluciones.com	Hallazgos	42 totales
Fecha	14 de septiembre de 2026 a las 18:42	Problemas	10 detectados

B

75/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al dominio arroja una puntuación de 75/100, lo que equivale a una calificación de grado B. Se ejecutaron un total de 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 3 generaron advertencias por configuraciones incompletas y 1 se identificó como fallo de seguridad. No se realizó un pentest activo, centrando el estudio en la superficie expuesta y las cabeceras del servidor. Aunque la base del cifrado es sólida, el sitio se considera vulnerable debido a la exposición de servicios críticos de infraestructura en puertos públicos.

Resumen de Riesgos

1	4	3	2	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 65 dias
Cabeceras de Seguridad	25	FALLO	Solo 1/6 presentes. Faltan: X-Frame-Options, Str...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
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	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta robots.txt
Puertos Abiertos	60	AVISO	2 puerto(s) potencialmente riesgoso(s): 21 (FTP)...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 65 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  65 dias restantes (expira: 2026-11-18T12:42:10.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-08-20T12:42:11.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 25/100

Estado: FALLO

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

- BAJO **Server header expuesto**
  Server: LiteSpeed — Revela tecnologia del servidor

- INFO **Content-Security-Policy**
  Presente: upgrade-insecure-requests
- 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://inveralsoluciones.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

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 — 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 — 60/100

Estado: AVISO

Falta robots.txt

- BAJO **robots.txt**
  No encontrado (HTTP 404)
- INFO **sitemap.xml**
  Presente, 10 URLs
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

2 puerto(s) potencialmente riesgoso(s): 21 (FTP), 3306 (MySQL)

- 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
- 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 se encuentra abierta al tráfico externo, permitiendo ataques directos de fuerza bruta y posibles fugas de información.
[HIGH] Puerto 21 (FTP): El servicio de transferencia de archivos está accesible de forma pública y no utiliza cifrado, lo que facilita la interceptación de datos sensibles.
[HIGH] X-Frame-Options: La ausencia de esta cabecera hace que el sitio sea susceptible a ataques de clickjacking, permitiendo que terceros carguen la web en marcos maliciosos.
[HIGH] Strict-Transport-Security (HSTS): No se fuerza el uso de HTTPS a nivel de navegador, dejando a los usuarios expuestos a ataques de degradación de protocolo.
[MEDIUM] X-Content-Type-Options: Al faltar esta directiva, el navegador podría procesar archivos con tipos MIME incorrectos, facilitando ataques de inyección de código.

[MEDIUM] Referrer-Policy: No hay control sobre la información que el navegador envía a otros sitios al seguir enlaces externos, comprometiendo la privacidad de la navegación.
[MEDIUM] Permissions-Policy: El sitio no restringe el acceso a funciones sensibles del navegador como la cámara o la geolocalización mediante cabeceras de seguridad.
[LOW] Server header expuesto: La respuesta del servidor revela explícitamente el uso de LiteSpeed, proporcionando información valiosa a posibles atacantes para identificar vulnerabilidades específicas.
[LOW] robots.txt: No se encontró el archivo de gestión de rastreo, lo que puede provocar una indexación ineficiente o la exposición involuntaria de rutas en buscadores.