EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.feinsa.com	Checks	9 pruebas
Dominio	www.feinsa.com	Hallazgos	50 totales
Fecha	6 de agosto de 2026 a las 02:31	Problemas	16 detectados

C

62/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web feinsa.com ha arrojado una puntuación de 62/100, obteniendo una nota de C. Se ejecutaron un total de 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 1 presentó advertencias y 3 fallaron significativamente. El análisis revela deficiencias críticas en la configuración de cabeceras de seguridad y la exposición de información sensible del sistema. Debido a la presencia de contenido mixto y la visibilidad de versiones de software, el sitio se clasifica actualmente como vulnerable frente a ataques dirigidos y automatizados.

Resumen de Riesgos

0	5	9	2	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 57 dias
Cabeceras de Seguridad	10	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
Version CMS Expuesta	20	FALLO	WordPress 7.0.2 expuesta, WordPress 2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	20	FALLO	14 recursos HTTP en pagina HTTPS
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 57 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  57 dias restantes (expira: 2026-10-01T23:55:23.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-07-03T23:55:24.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 10/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, 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
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://www.feinsa.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: All in One SEO (AIOSEO) 5.0.0.1
- INFO **Tecnologias detectadas**
  Next.js

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 — 20/100

Estado: FALLO

14 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (src (script/img/iframe))**
  http://www.feinsa.com/wp-content/uploads/2020/01/Logo.png
- MEDIO **Recurso HTTP (src (script/img/iframe))**
  http://www.feinsa.com/wp-content/uploads/2020/01/Logo.png
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.feinsa.com/vigas/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.feinsa.com/avci/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.feinsa.com/planchas/
- MEDIO **href (link/stylesheet)**
  ...y 9 mas del mismo tipo

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (262 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- INFO **Sitemap en robots.txt**
  https://www.feinsa.com/sitemap.xml
- 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: Falta esta cabecera esencial para prevenir ataques de ejecución de scripts maliciosos y ataques de inyección de contenido.
[HIGH] X-Frame-Options: La ausencia de esta directiva permite que el sitio sea cargado en marcos externos, facilitando ataques de clickjacking.
[HIGH] Strict-Transport-Security: No se encuentra configurado el mecanismo HSTS, por lo que el navegador no obliga a realizar conexiones exclusivamente seguras.
[HIGH] WordPress version: La versión 7.0.2 del CMS se encuentra expuesta públicamente, permitiendo que atacantes identifiquen exploits conocidos para dicha versión.
[HIGH] HSTS no configurado: El servidor realiza redirección pero no instruye al navegador para mantener siempre la conexión bajo protocolo HTTPS.
[MEDIUM] Contenido Mixto: Se detectaron 14 recursos, incluyendo el logo principal y enlaces a secciones de vigas o planchas, que cargan mediante HTTP inseguro dentro de la página cifrada.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite que el navegador realice sniffing de tipos MIME, lo que puede derivar en la ejecución de archivos maliciosos disfrazados.
[MEDIUM] Permissions-Policy: No se restringe el acceso a APIs del navegador, dejando abierta la posibilidad de uso de funciones como cámara o micrófono por parte de terceros.
[MEDIUM] Archivo /readme.html: Este archivo es accesible públicamente y puede revelar información detallada sobre la estructura y configuración del CMS.
[LOW] Server header expuesto: El servidor responde identificándose como Apache, lo que otorga información técnica valiosa sobre la infraestructura del host a un atacante.
[LOW] Meta generator: Se expone el uso de All in One SEO 5.0.0.1, facilitando la identificación de plugins específicos instalados.