EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://360constructionjn.com/	Checks	9 pruebas
Dominio	360constructionjn.com	Hallazgos	42 totales
Fecha	12 de agosto de 2026 a las 04:39	Problemas	14 detectados

D

53/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoria de seguridad realizada al sitio web muestra un desempeño insuficiente, obteniendo una puntuacion de 53/100 y una calificacion de D. El analisis se baso en 9 checks pasivos, de los cuales 5 resultaron satisfactorios y 4 presentaron fallos criticos que comprometen la integridad del servidor. Se detectaron debilidades graves en la configuracion de las cabeceras de seguridad y una exposicion peligrosa de servicios de base de datos a internet. Debido a la falta de protecciones basicas contra ataques de inyeccion y la ausencia de cifrado obligatorio, se concluye que el sitio es vulnerable y requiere medidas correctivas urgentes.

Resumen de Riesgos

1	6	4	3	28
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 198 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a HTTPS
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	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	20	FALLO	3 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 198 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  198 dias restantes (expira: 2027-02-26T03:51:10.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-08-12T03:51:10.000Z
- 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 — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS
- 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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  No encontrado (HTTP 404)
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- 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) ABIERTO: La base de datos esta expuesta directamente a internet, lo que permite intentos de acceso no autorizados y ataques de fuerza bruta.
[HIGH] Content-Security-Policy (CSP) FALTA: La ausencia de esta politica facilita la ejecucion de ataques Cross-Site Scripting (XSS) y la inyeccion de contenido malicioso.
[HIGH] X-Frame-Options FALTA: El sitio es vulnerable a ataques de clickjacking, permitiendo que atacantes carguen la web en frames externos para engañar a los usuarios.
[HIGH] Strict-Transport-Security (HSTS) FALTA: No se obliga al navegador a usar conexiones HTTPS, facilitando ataques de degradacion de cifrado y robo de sesiones.
[HIGH] Redireccion HTTP a HTTPS INEXISTENTE: El servidor permite conexiones por el puerto 80 sin redirigirlas a la version segura, exponiendo los datos en transito.

[HIGH] Puerto 21 (FTP) ABIERTO: Este protocolo transmite credenciales y archivos en texto plano, siendo vulnerable a la interceptacion de datos.
[MEDIUM] X-Content-Type-Options FALTA: La ausencia de la directiva nosniff permite que los navegadores interpreten archivos de forma incorrecta, facilitando la ejecucion de scripts.
[MEDIUM] Referrer-Policy FALTA: No existe control sobre la informacion de procedencia enviada a otros dominios, lo que puede filtrar URLs privadas.
[MEDIUM] Permissions-Policy FALTA: El sitio no restringe el acceso a funciones sensibles del navegador como la camara, el microfono o la geolocalizacion.
[MEDIUM] Puerto 22 (SSH) ABIERTO: Un servicio de acceso remoto visible aumenta la superficie de ataque para intentos de intrusion al sistema operativo.
[LOW] Cabecera Server expuesta: Se revela que el servidor utiliza Apache, informacion que ayuda a los atacantes a buscar vulnerabilidades especificas para ese software.
[LOW] Ausencia de robots.txt y sitemap.xml: El servidor devuelve un error 404 para estos archivos, lo que dificulta la gestion del rastreo y la indexacion.