EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://huevosanjuan.com.mx	Checks	9 pruebas
Dominio	huevosanjuan.com.mx	Hallazgos	51 totales
Fecha	26 de marzo de 2026 a las 00:06	Problemas	15 detectados

C

63/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio web https://huevosanjuan.com.mx arroja una puntuación de 63/100, lo que resulta en una calificación de grado C. Durante la evaluación, se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 2 generaron advertencias y 2 fueron clasificados como fallos críticos. Se detectó una ausencia total de cabeceras de seguridad modernas y una configuración deficiente en la protección de las cookies de sesión. Debido a estas vulnerabilidades técnicas en la configuración del servidor, el sitio se considera actualmente vulnerable ante ataques de interceptación y suplantación. Es imperativo aplicar medidas correctivas para elevar el estándar de protección de la plataforma.

Resumen de Riesgos

0	7	6	2	36
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 282 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	No se detecto un CMS conocido
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	17	FALLO	XSRF-TOKEN: falta HttpOnly; XSRF-TOKEN: falta Se...
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	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 282 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  282 dias restantes (expira: 2027-01-01T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-12-01T00:00:00.000Z
- 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

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/7.4.33 — 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://huevosanjuan.com.mx/
- 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
- INFO **Tecnologias detectadas**
  Next.js, PHP/7.4.33

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 — 17/100

Estado: FALLO

XSRF-TOKEN: falta HttpOnly; XSRF-TOKEN: falta Secure; XSRF-TOKEN: falta SameSite; laravel_session: falta Secure; laravel_session: falta SameSite

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- ALTO **Cookie: XSRF-TOKEN — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: XSRF-TOKEN — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: XSRF-TOKEN — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: laravel_session — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: laravel_session — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: laravel_session — SameSite**
  Falta SameSite — Vulnerable a CSRF

Contenido Mixto — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

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

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (108914 bytes)
- INFO **Reglas robots.txt**
  0 Disallow, 1 Allow
- INFO **Sitemap en robots.txt**
  http://huevosanjuan.com/indentation1.xml.gz
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

No se detectaron puertos abiertos

- 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)**
  Cerrado — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Cerrado — 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 crítica que previene ataques de inyección de código y Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options: La ausencia de esta directiva permite que el sitio sea cargado en iframes ajenos, facilitando ataques de clickjacking.
[HIGH] Strict-Transport-Security: No se ha configurado el protocolo HSTS, por lo que el navegador no fuerza la conexión cifrada permanentemente.
[HIGH] Cookie XSRF-TOKEN insegura: Carece de los atributos HttpOnly y Secure, lo que permite que sea interceptada en tránsito o leída por scripts maliciosos.
[HIGH] Cookie laravel_session insegura: No utiliza el flag Secure, permitiendo que la sesión del usuario viaje por canales no cifrados si el usuario accede vía HTTP.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el sniffing de tipos MIME, lo que podría derivar en la ejecución de archivos con contenido malicioso.
[MEDIUM] Referrer-Policy: No existe control sobre la información que el navegador envía a otros sitios al hacer clic en enlaces externos.
[MEDIUM] Permissions-Policy: No se restringe el acceso a las APIs del navegador, dejando abierta la posibilidad de que scripts de terceros accedan a funciones del dispositivo.
[MEDIUM] Contenido Mixto: Se detectó un recurso vinculado mediante HTTP (proan.com) dentro de la página protegida por HTTPS, debilitando la integridad del sitio.
[MEDIUM] Falta de SameSite en cookies: Tanto XSRF-TOKEN como laravel_session no definen esta política, aumentando el riesgo de ataques Cross-Site Request Forgery (CSRF).
[LOW] Servidor expuesto: La cabecera Server revela el uso de Apache, proporcionando información técnica útil para un posible atacante.
[LOW] Tecnología expuesta: Se detectó la cabecera X-Powered-By indicando el uso de PHP/7.4.33, revelando la versión exacta del lenguaje de programación.