EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.joal.net	Checks	9 pruebas
Dominio	www.joal.net	Hallazgos	43 totales
Fecha	3 de junio de 2026 a las 15:05	Problemas	10 detectados

C

63/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis técnico de seguridad realizado al dominio ha dado como resultado una puntuación de 63/100, lo que equivale a una calificación de grado C. Durante la auditoría se ejecutaron un total de 9 comprobaciones pasivas, de las cuales 6 resultaron satisfactorias, 1 generó una advertencia y 2 fueron clasificadas como fallos de seguridad. A pesar de contar con un cifrado SSL válido, la carencia absoluta de cabeceras de protección y la falta de redirección segura de tráfico comprometen la integridad del sitio. Por lo tanto, se concluye que el sitio es actualmente vulnerable ante ataques de interceptación de datos y manipulación de interfaz.

Resumen de Riesgos

0	5	3	2	33
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 51 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	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 51 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  51 dias restantes (expira: 2026-07-24T08:55:26.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-25T08:55:27.000Z
- 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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (90 bytes)
- INFO **Reglas robots.txt**
  3 Disallow, 0 Allow
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- 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

[ALTA] Redirección HTTP a HTTPS: El sitio permite conexiones inseguras a través del puerto 80 sin redirigir automáticamente al usuario a la versión cifrada.
[ALTA] Content-Security-Policy: La ausencia de esta cabecera facilita la ejecución de ataques de inyección de contenido y scripts maliciosos (XSS).
[ALTA] X-Frame-Options: Al no estar configurada, el sitio es susceptible a ataques de Clickjacking, permitiendo que sea embebido en marcos externos fraudulentos.
[ALTA] Strict-Transport-Security: La falta de HSTS impide que el navegador fuerce siempre una conexión segura, dejando la comunicación expuesta a ataques de degradación.

[MEDIA] X-Content-Type-Options: La falta de esta cabecera permite que el navegador intente adivinar el tipo de contenido, lo que puede derivar en la ejecución de archivos maliciosos.
[MEDIA] Referrer-Policy: No existe control sobre la información de referencia que se envía al navegar hacia enlaces externos, lo que podría filtrar rutas internas.
[MEDIA] Permissions-Policy: El sitio no restringe el acceso a funciones sensibles del navegador como la cámara, el micrófono o la geolocalización.
[BAJA] Server header expuesto: Se detectó el encabezado Server: Apache, lo cual revela la tecnología subyacente y facilita a un atacante la búsqueda de vulnerabilidades específicas.
[BAJA] sitemap.xml: El archivo de mapa del sitio no fue encontrado, lo que dificulta la auditoría de estructura y el reconocimiento de endpoints.