

Escanear Vulnerabilidades

Informe de Seguridad Web

URL	https://bocajuniors.queue-it.net/?c=bocajuniors&e=e20261013ple&Ver=3-javascript-3.7.10&cver=326&man=Proteccion+Boca+Socios+-+BocaSocios+Trigger&https%3A%2F%2Fbocasocios-	9 pruebas
Dominio	bocajuniors.queue-it.net	49 totales
Fecha	8 de octubre de 2026 a las 15:30	Problemas 8 detectados

C

70/100

puntos de seguridad



RESUMEN EJECUTIVO

Tras realizar el análisis de seguridad, el sitio web ha obtenido una puntuación de 70/100, lo que equivale a una nota de C. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 1 presentó advertencias y 2 fueron calificados como fallidos. A pesar de contar con un cifrado SSL sólido, la ausencia de cabeceras de protección críticas deja el entorno expuesto a vectores de ataque conocidos. Se concluye que el sitio es vulnerable ante técnicas de inyección de contenido y suplantación de identidad debido a configuraciones de servidor incompletas.

Resumen de Riesgos

0	3	3	2	41
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 189 dias
Cabeceras de Seguridad	35	FALLO	Solo 2/6 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	1 cookies, todas con flags correctos
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 189 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
189 dias restantes (expira: 2027-04-15T23:59:59.000Z)
- INFO Fecha de emision
Emitido desde: 2026-09-30T00:00:00.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 35/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Referrer-Policy, Permissions-Policy

- BAJO Server header expuesto
Server: Kestrel — 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
- INFO

Strict-Transport-Security
Presente: max-age=2592000
- INFO

X-Content-Type-Options
Presente: nosniiff
- 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 404 — No redirige a HTTPS
- INFO

HSTS (Strict-Transport-Security)
HSTS activo: max-age=31536000; includeSubDomains
- BAJO

HSTS includeSubDomains
HSTS cubre subdominios
- INFO

HSTS max-age
max-age=31536000 (365 dias)
- INFO

Respuesta HTTPS
HTTPS responde con status 404

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

1 cookies, todas con flags correctos

- INFO

Cookies detectadas
1 cookie(s) encontrada(s)
- INFO

Cookie: Queue-it-visitorsession — HttpOnly
HttpOnly activo — No accesible via JavaScript
- INFO

Cookie: Queue-it-visitorsession — Secure
Flag Secure activo — Solo se envía por HTTPS
- INFO

Cookie: Queue-it-visitorsession — SameSite
SameSite=strict

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 (110 bytes)
- INFO

Reglas robots.txt
1 Disallow, 1 Allow
- MEDIO

Bloqueo total
robots.txt bloquea todo el sitio con Disallow: /
- BAJO

sitemap.xml
No encontrado (HTTP 404)
- 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 — Envío 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 que previene ataques de Cross-Site Scripting (XSS) e inyección de datos.

[HIGH] X-Frame-Options: La ausencia de esta directiva permite que el sitio sea cargado en frames externos, facilitando ataques de clickjacking.

[HIGH] Redirección HTTP a HTTPS: No existe una redirección automática desde conexiones no cifradas, lo que compromete la integridad de la sesión inicial.

[MEDIUM] Referrer-Policy: No se detectó una política de referencia, lo que puede filtrar información sensible de la URL a dominios de terceros.

[MEDIUM] Permissions-Policy: El sitio no restringe el acceso de las APIs del navegador a componentes de hardware como la cámara o el micrófono.

[MEDIUM] Bloqueo en robots.txt: El archivo está configurado para bloquear el rastreo de todo el sitio, lo cual puede ser un error de visibilidad o una medida restrictiva extrema.

[LOW] Server header expuesto: El servidor responde con la cabecera Kestrel, revelando información técnica que ayuda a un atacante a dirigir sus esfuerzos.

[LOW] Sitemap.xml: No se encontró el archivo de mapa del sitio, lo que dificulta la indexación estructurada por parte de motores de búsqueda.