EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://porra.bocatadecalamares.com/	Checks	9 pruebas
Dominio	porra.bocatadecalamares.com	Hallazgos	44 totales
Fecha	24 de junio de 2026 a las 05:32	Problemas	15 detectados

D

57/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio web arroja una puntuación de 57/100 con una nota final de D. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios, se emitió 1 advertencia y se identificaron 3 fallos críticos en la configuración del servidor. El sitio presenta una carencia total de cabeceras de seguridad esenciales y una gestión deficiente de las conexiones cifradas. Debido a la falta de redirección automática a HTTPS y la exposición de puertos innecesarios, se concluye que el sitio es actualmente vulnerable a ataques de interceptación de datos y manipulación de contenido.

Resumen de Riesgos

0	5	9	1	29
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 76 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	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 76 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  76 dias restantes (expira: 2026-09-07T18:19:04.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-09T18:19:05.000Z
- 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: cloudflare — 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
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente
- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente

- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente
- 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

- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- 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
- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
  Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[HIGH] Falta de redirección HTTP a HTTPS: El sitio permite conexiones no cifradas, lo que facilita ataques de interceptación de tráfico (Man-in-the-Middle).
[HIGH] Falta de cabecera Content-Security-Policy: La ausencia de esta política permite la ejecución de scripts maliciosos y ataques de inyección de contenido XSS.

[HIGH] Falta de cabecera X-Frame-Options: El sitio es vulnerable a ataques de clickjacking, permitiendo que sea cargado dentro de marcos externos para engañar al usuario.
[HIGH] Falta de Strict-Transport-Security (HSTS): El servidor no instruye al navegador para que utilice exclusivamente conexiones seguras en futuras visitas.
[MEDIUM] Falta de cabecera X-Content-Type-Options: El navegador puede intentar adivinar el tipo de contenido, permitiendo la ejecución de archivos maliciosos camuflados.
[MEDIUM] Puerto 8080 (HTTP-Alt) Abierto: Se detectó un puerto alternativo abierto que podría exponer servicios administrativos o de depuración vulnerables.
[MEDIUM] Exposición de archivos de información: Los archivos /readme.html y /README.txt son accesibles, lo que podría revelar detalles técnicos sobre la infraestructura interna.
[MEDIUM] Paneles de login accesibles: Rutas administrativas comunes como /wp-login.php o /administrator están expuestas, facilitando ataques de fuerza bruta.
[MEDIUM] Falta de cabecera Referrer-Policy: No se controla la información de navegación que se envía a sitios externos cuando un usuario hace clic en un enlace.
[MEDIUM] Falta de cabecera Permissions-Policy: El sitio no restringe el uso de funciones sensibles del navegador como la cámara, el micrófono o la ubicación.
[LOW] Exposición de cabecera Server: El servidor revela que utiliza la tecnología Cloudflare, ayudando a los atacantes en la fase de reconocimiento.