EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://bdvenlinea.banvenez.com/	Checks	9 pruebas
Dominio	bdvenlinea.banvenez.com	Hallazgos	47 totales
Fecha	25 de mayo de 2026 a las 03:25	Problemas	10 detectados

B

77/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web arroja una puntuación de 77/100 con una calificación de grado B. Durante la evaluación se ejecutaron 9 checks pasivos, resultando en 5 satisfactorios y 3 fallos críticos relacionados con la configuración de cabeceras y gestión de sesiones. A pesar de contar con un cifrado SSL robusto, la ausencia de políticas de seguridad modernas y deficiencias en las propiedades de las cookies comprometen la integridad de la plataforma. Se concluye que el sitio es actualmente vulnerable a ataques de inyección de código y falsificación de peticiones en sitios cruzados. Por lo tanto, se requiere una intervención técnica inmediata para alcanzar un nivel de seguridad óptimo.

Resumen de Riesgos

0	3	5	2	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 271 dias
Cabeceras de Seguridad	50	FALLO	Solo 3/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion 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	44	FALLO	BIGipServerpool_bdvenlinea_pro: falta SameSite; ...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	1 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 271 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  271 dias restantes (expira: 2027-02-19T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-19T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 50/100

Estado: FALLO

Solo 3/6 presentes. Faltan: Content-Security-Policy, Referrer-Policy, Permissions-Policy

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido

- INFO **X-Frame-Options**
  Presente: DENY
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000 ; includeSubDomains
- INFO **X-Content-Type-Options**
  Presente: nosniff
- MEDIO **Referrer-Policy**
  Falta — Controla la informacion de referer enviada
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

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 — 44/100

Estado: FALLO

BIGipServerpool_bdvenlinea_pro: falta SameSite; f5avraaaaaaaaaaaaaaaa_session_: falta SameSite; TS0177b05a: falta HttpOnly; TS0177b05a: falta Secure; TS0177b05a: falta SameSite

- INFO **Cookies detectadas**
  3 cookie(s) encontrada(s)
- INFO **Cookie: BIGipServerpool_bdvenlinea_pro — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: BIGipServerpool_bdvenlinea_pro — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: BIGipServerpool_bdvenlinea_pro — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: f5avraaaaaaaaaaaaaaaa_session_ — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: f5avraaaaaaaaaaaaaaaa_session_ — Secure**
  Flag Secure activo — Solo se envia por HTTPS

- MEDIO **Cookie: f5avraaaaaaaaaaaaaaa_session_ — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: TS0177b05a — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: TS0177b05a — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: TS0177b05a — SameSite**
  Falta SameSite — Vulnerable a CSRF

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 — 100/100

Estado: OK

1 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 — Envio de correo
- INFO **Puerto 80 (HTTP)**
  Cerrado — 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: La ausencia de esta cabecera permite la ejecución de scripts no autorizados, facilitando ataques de XSS e inyección de contenido malicioso.

[HIGH] Cookie TS0177b05a (HttpOnly/Secure): La falta de los flags HttpOnly y Secure permite que la cookie sea accesible mediante scripts y se envíe por canales no cifrados, aumentando el riesgo de robo de sesión.
[MEDIUM] Referrer-Policy: La falta de esta política puede provocar la filtración involuntaria de información sensible en las cabeceras de navegación hacia sitios externos.
[MEDIUM] Permissions-Policy: Al no estar definida, el sitio no restringe el acceso de las APIs del navegador a funciones sensibles como la cámara o el micrófono.
[MEDIUM] Cookies SameSite: Las cookies de sesión carecen del atributo SameSite, lo que deja a los usuarios expuestos a ataques de Cross-Site Request Forgery (CSRF).
[LOW] Redirección HTTPS: No se pudo verificar la redirección automática de tráfico no cifrado, lo que podría permitir conexiones inseguras iniciales.
[LOW] Archivos robots.txt y sitemap.xml: La inexistencia de estos archivos dificulta la correcta indexación y el control sobre los rastreadores web en el servidor.