EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://biosaludbol.com/chop/admin/historiasClinicas	Checks	9 pruebas
Dominio	biosaludbol.com	Hallazgos	51 totales
Fecha	10 de julio de 2026 a las 22:47	Problemas	14 detectados

B

75/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web arroja una puntuación de 75/100, lo que equivale a una calificación de grado B. De los 9 checks pasivos ejecutados, 5 resultaron satisfactorios, mientras que se identificaron 2 advertencias y 2 fallos críticos relacionados principalmente con la configuración de cabeceras y la seguridad de las cookies. Aunque el cifrado SSL es correcto y los puertos están bien gestionados, la ausencia de políticas de transporte seguro y la exposición de versiones tecnológicas elevan el riesgo de explotación. El análisis concluye que el sitio es parcialmente vulnerable, especialmente ante ataques de interceptación de sesión y clickjacking. Se recomienda una intervención inmediata en las configuraciones del servidor para alcanzar un nivel de seguridad óptimo.

Resumen de Riesgos

0	4	7	3	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 34 dias
Cabeceras de Seguridad	25	FALLO	Solo 1/6 presentes. Faltan: X-Frame-Options, Str...
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	83	AVISO	XSRF-TOKEN: falta HttpOnly
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	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 34 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  34 dias restantes (expira: 2026-08-13T18:47:12.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-15T18:47:13.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 25/100

Estado: FALLO

Solo 1/6 presentes. Faltan: X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: hcdn — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/7.4.33 — Revela framework/lenguaje
- INFO **Content-Security-Policy**
  Presente: upgrade-insecure-requests
- 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://biosaludbol.com/
- 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
- BAJO **Meta generator**
  Expone: CRUDBooster
- INFO **Tecnologias detectadas**
  PHP/7.4.33

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 /user/login**
  Panel de login accesible publicamente
- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 83/100

Estado: AVISO

XSRF-TOKEN: falta HttpOnly

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- ALTO **Cookie: XSRF-TOKEN — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: XSRF-TOKEN — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: XSRF-TOKEN — SameSite**
  SameSite=lax
- INFO **Cookie: optisoft_session — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: optisoft_session — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: optisoft_session — SameSite**
  SameSite=lax

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 — 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 — 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
- 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] X-Frame-Options faltante: El sitio puede ser cargado en marcos externos, facilitando ataques de clickjacking para engañar a los usuarios.
[HIGH] Strict-Transport-Security (HSTS) no configurado: El servidor no obliga al navegador a usar conexiones HTTPS, permitiendo ataques de degradación de SSL.
[HIGH] Cookie XSRF-TOKEN sin atributo HttpOnly: La cookie de sesión es accesible mediante scripts de cliente, lo que aumenta significativamente el riesgo de robo de identidad vía XSS.
[MEDIUM] X-Content-Type-Options faltante: El navegador podría interpretar archivos como tipos MIME incorrectos, abriendo la puerta a la ejecución de código malicioso oculto.
[MEDIUM] Referrer-Policy y Permissions-Policy no configurados: No existe control sobre la información enviada a sitios externos ni sobre el acceso a funciones del navegador como la cámara o el micrófono.
[MEDIUM] Archivos técnicos expuestos: La presencia de archivos como readme.html y README.txt revela detalles sobre la arquitectura interna del sistema.
[MEDIUM] Paneles de login accesibles: Las rutas /wp-login.php y /user/login están abiertas al público, lo que facilita intentos de acceso no autorizado mediante fuerza bruta.
[LOW] Server header expuesto: La cabecera revela el uso de hcdn, proporcionando información valiosa a un atacante para buscar exploits específicos.
[LOW] X-Powered-By expuesto: Se divulga el uso de PHP/7.4.33, una versión específica que permite a terceros identificar vulnerabilidades conocidas asociadas a dicho lenguaje.
[LOW] Meta generator visible: El uso de CRUDBooster es detectable, lo que reduce el esfuerzo de reconocimiento para un atacante externo.