EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://doradobet.com/deportes	Checks	9 pruebas
Dominio	doradobet.com	Hallazgos	44 totales
Fecha	28 de abril de 2026 a las 17:35	Problemas	8 detectados

C

69/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre doradobet.com arroja una puntuación de 69/100, lo que equivale a una calificación de grado C. Durante la evaluación se ejecutaron 9 checks pasivos, resultando en 5 verificaciones exitosas, 2 advertencias por configuraciones incompletas y 2 fallos de seguridad críticos. Se han detectado debilidades importantes en la gestión del tráfico cifrado y la ausencia de cabeceras de seguridad fundamentales. En su estado actual, el sitio se considera vulnerable debido a que no garantiza una conexión segura obligatoria para todos los usuarios.

Resumen de Riesgos

0	2	3	3	36
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 48 dias
Cabeceras de Seguridad	60	AVISO	4/6 presentes. Faltan: Content-Security-Policy, ...
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 48 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  48 dias restantes (expira: 2026-06-16T02:26:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-18T01:27:05.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 60/100

Estado: AVISO

4/6 presentes. Faltan: Content-Security-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
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=2592000; includeSubDomains
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: same-origin
- 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 403 — No redirige a HTTPS
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=2592000; includeSubDomains
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- MEDIO **HSTS max-age**
  max-age=2592000 (30 dias) — Recomendado minimo 180 dias
- INFO **Respuesta HTTPS**
  HTTPS responde con status 403

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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  No encontrado (HTTP 403)
- BAJO **sitemap.xml**
  No encontrado (HTTP 403)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

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] Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de scripts no autorizados, aumentando drásticamente el riesgo de ataques Cross-Site Scripting (XSS) e inyección de contenido.
[HIGH] HTTP -> HTTPS redireccion: El servidor no redirige automáticamente a los usuarios desde HTTP a una conexión cifrada (responde con error 403), lo que expone los datos a intercepciones.

[MEDIUM] Permissions-Policy: La falta de esta cabecera impide al servidor restringir el acceso del navegador a funciones sensibles como la cámara, el micrófono o la geolocalización.
[MEDIUM] HSTS max-age: El valor actual de 30 días es insuficiente según los estándares de la industria, que recomiendan al menos 180 días para proteger la comunicación de forma persistente.
[MEDIUM] Puerto 8080 (HTTP-Alt): El puerto se encuentra abierto y podría exponer servicios administrativos o servidores proxy que no deberían ser accesibles públicamente.
[LOW] Server header expuesto: La cabecera revela el uso de Cloudflare, lo que facilita a un atacante potencial información sobre la infraestructura tecnológica utilizada.
[LOW] robots.txt: El archivo no es accesible debido a un error 403, lo que impide una correcta gestión de los rastreadores de motores de búsqueda.
[LOW] sitemap.xml: El mapa del sitio no está disponible por errores de permisos, dificultando la indexación y auditoría de la estructura web.