EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.football-data.org/	Checks	9 pruebas
Dominio	www.football-data.org	Hallazgos	47 totales
Fecha	23 de marzo de 2026 a las 22:14	Problemas	13 detectados

C

63/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio football-data.org arroja una puntuación de 63/100, lo que equivale a una calificación de grado C. El análisis se basó exclusivamente en 9 verificaciones pasivas, de las cuales 4 resultaron satisfactorias, 3 presentaron advertencias y 2 fallaron críticamente. El sitio demuestra una implementación sólida del cifrado de transporte, pero carece de protecciones esenciales contra ataques de inyección y secuestro de sesiones. Debido a la ausencia de cabeceras de seguridad modernas y a la configuración inadecuada de cookies, el sitio se considera vulnerable ante ataques convencionales de la web.

Resumen de Riesgos

0	5	6	2	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 66 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
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	33	FALLO	JSESSIONID: falta Secure; JSESSIONID: falta Same...
Contenido Mixto	60	AVISO	1 recurso(s) HTTP en pagina HTTPS
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 66 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  66 dias restantes (expira: 2026-05-28T15:25:43.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-27T15:25:44.000Z
- 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: nginx/1.14.2 — 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://www.football-data.org/
- 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

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 — 33/100

Estado: FALLO

JSESSIONID: falta Secure; JSESSIONID: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: JSESSIONID — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: JSESSIONID — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: JSESSIONID — SameSite**
  Falta SameSite — Vulnerable a CSRF

Contenido Mixto — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://football-data.org

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (31 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 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 — 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] Content-Security-Policy: Falta esta cabecera, lo que permite la ejecución de scripts maliciosos y ataques de inyección de contenido (XSS).
[HIGH] X-Frame-Options: La ausencia de esta directiva expone el sitio a ataques de clickjacking al permitir que sea cargado en marcos externos.
[HIGH] Strict-Transport-Security: No se ha configurado HSTS, por lo que el navegador no fuerza conexiones cifradas, permitiendo ataques de degradación de protocolo.
[HIGH] Cookie Secure Flag: La cookie JSESSIONID carece del atributo Secure, lo que permite que sea enviada a través de conexiones HTTP no cifradas.
[MEDIUM] Cookie SameSite: La cookie JSESSIONID no implementa el atributo SameSite, aumentando el riesgo de ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el MIME-type sniffing, facilitando que archivos de datos sean interpretados como ejecutables.
[MEDIUM] Referrer-Policy: No existe una política definida para controlar cuánta información de referencia se comparte con otros dominios.
[MEDIUM] Permissions-Policy: No se restringen las APIs del navegador, permitiendo potencialmente el acceso no deseado a funciones del dispositivo del usuario.
[MEDIUM] Contenido Mixto: Se detectó un recurso cargado mediante el protocolo inseguro HTTP, comprometiendo la integridad de la página cifrada.
[MEDIUM] Configuración de robots.txt: El archivo bloquea el acceso a todo el sitio mediante la directiva Disallow, lo que puede afectar el rastreo legítimo.
[LOW] Server Header Expuesto: La cabecera revela la versión exacta del servidor (nginx/1.14.2), facilitando a los atacantes la búsqueda de exploits específicos.
[LOW] Sitemap: No se encontró el archivo sitemap.xml, lo que dificulta la indexación y el análisis de la estructura del sitio.