EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://fifa.com	Checks	9 pruebas
Dominio	fifa.com	Hallazgos	50 totales
Fecha	4 de julio de 2026 a las 16:42	Problemas	8 detectados

B

89/100

puntos de seguridad

RESUMEN EJECUTIVO

El sitio web analizado ha obtenido una puntuación de 89/100 con una calificación de grado B, lo que indica un nivel de seguridad sólido pero con áreas de mejora críticas. Se ejecutaron un total de 9 checks pasivos, de los cuales 7 resultaron satisfactorios, uno generó una advertencia y uno fue clasificado como fallo. El sistema demuestra una implementación robusta de cifrado y redirecciones, aunque presenta debilidades en la configuración de cabeceras y la gestión de cookies. En conclusión, fifa.com es un sitio mayoritariamente seguro, aunque se considera vulnerable a ataques específicos de sesión y de intermediación debido a la falta de atributos de seguridad en sus identificadores.

Resumen de Riesgos

0	3	5	0	42
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 75 dias
Cabeceras de Seguridad	85	AVISO	5/6 presentes. Faltan: Permissions-Policy
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
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	17	FALLO	ak_bmsc: falta Secure; ak_bmsc: falta SameSite; ...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 75 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  75 dias restantes (expira: 2026-09-17T10:57:31.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-19T10:57:32.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 85/100

Estado: AVISO

5/6 presentes. Faltan: Permissions-Policy

- INFO **Content-Security-Policy**
  Presente: script-src 'self' 'unsafe-inline' 'unsafe-eval' *.2mdn.net *.theoplayer.com *.yo...

- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=15552000; includeSubDomains
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: no-referrer
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://www.fifa.com/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=15552000; includeSubDomains
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=15552000 (180 dias)
- 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

- 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
- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 17/100

Estado: FALLO

ak_bmsc: falta Secure; ak_bmsc: falta SameSite; bm_sz: falta HttpOnly; bm_sz: falta Secure; bm_sz: falta SameSite

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- INFO **Cookie: ak_bmsc — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: ak_bmsc — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: ak_bmsc — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: bm_sz — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: bm_sz — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: bm_sz — 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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (82 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- INFO **Sitemap en robots.txt**
  https://www.fifa.com/sitemap
- 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] Cookie bm_sz: Falta el atributo HttpOnly, lo que permite que la cookie sea accesible mediante scripts del lado del cliente, aumentando el riesgo de robo de sesión vía XSS.
[HIGH] Cookies ak_bmsc y bm_sz: Falta el flag Secure, lo que permite que estas cookies sean enviadas a través de conexiones HTTP no cifradas, exponiéndolas a ataques de interceptación.
[MEDIUM] Cookies ak_bmsc y bm_sz: Falta el atributo SameSite, lo que deja el sitio vulnerable a ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] Permissions-Policy: Cabecera de seguridad ausente, lo que impide al servidor restringir el acceso del navegador a APIs sensibles como la cámara, el micrófono o la geolocalización.
[MEDIUM] Archivos /readme.html y /README.txt: Archivos técnicos accesibles públicamente que pueden revelar información sobre la infraestructura o versiones de software subyacente.