EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.smithfieldgolfclub.com/golf/index2.php	Checks	9 pruebas
Dominio	www.smithfieldgolfclub.com	Hallazgos	45 totales
Fecha	12 de mayo de 2026 a las 17:33	Problemas	13 detectados

C

62/100

puntos de seguridad

RESUMEN EJECUTIVO

Tras realizar la auditoría de seguridad, el sitio web presenta una puntuación de 62/100, lo que equivale a una calificación de grado C. El análisis se basó exclusivamente en 9 checks pasivos, de los cuales 5 resultaron satisfactorios, se emitió 1 advertencia y se detectaron 3 fallos críticos en la configuración. A pesar de contar con un cifrado SSL válido, la carencia total de cabeceras de seguridad modernas y la gestión insegura de las cookies de sesión exponen el sitio a riesgos considerables. En su estado actual, el sitio se considera vulnerable ante ataques de interceptación de datos y manipulación de sesiones.

Resumen de Riesgos

0	6	4	3	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 60 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	0	FALLO	PHPSESSID: falta HttpOnly; PHPSESSID: falta Secu...
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	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 60 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  60 dias restantes (expira: 2026-07-11T20:57:05.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-12T20:57:06.000Z
- 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: Apache/2.4.58 (Ubuntu) — 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.smithfieldgolfclub.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

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 — 0/100

Estado: FALLO

PHPSESSID: falta HttpOnly; PHPSESSID: falta Secure; PHPSESSID: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: PHPSESSID — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: PHPSESSID — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: PHPSESSID — 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

No se detectaron puertos abiertos

- 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)**
  Cerrado — 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 maliciosos y ataques de inyección de contenido en el navegador del usuario.

[HIGH] X-Frame-Options: Al no estar configurada, el sitio es susceptible a ataques de clickjacking, permitiendo que atacantes oculten la web dentro de marcos invisibles.
[HIGH] Strict-Transport-Security: Falta la directiva HSTS, lo que impide que el sitio obligue a los navegadores a utilizar siempre una conexión segura HTTPS.
[HIGH] Cookie PHPSESSID (HttpOnly): La cookie de sesión no tiene el flag HttpOnly, permitiendo que sea robada mediante scripts maliciosos (XSS).
[HIGH] Cookie PHPSESSID (Secure): La cookie de sesión carece del flag Secure, lo que significa que podría ser transmitida a través de conexiones no cifradas.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite a los navegadores interpretar archivos de forma distinta a la declarada, facilitando ataques de tipo MIME-sniffing.
[MEDIUM] Referrer-Policy: No hay control sobre la información de navegación que se envía a sitios externos cuando un usuario hace clic en un enlace.
[MEDIUM] Permissions-Policy: No se restringe el acceso de la web a funciones sensibles del dispositivo del usuario como la cámara o el micrófono.
[MEDIUM] Cookie PHPSESSID (SameSite): La ausencia de este atributo facilita ataques de falsificación de peticiones en sitios cruzados (CSRF).
[LOW] Server header expuesto: El servidor revela el uso de Apache/2.4.58 sobre Ubuntu, lo que ayuda a atacantes a identificar vulnerabilidades específicas de esa versión.
[LOW] Ficheros de control ausentes: No se encontraron los archivos robots.txt ni sitemap.xml, necesarios para una correcta gestión del rastreo y la indexación.