

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://fapyc.es	Checks	9 pruebas
Dominio	fapyc.es	Hallazgos	53 totales
Fecha	1 de octubre de 2026 a las 15:52	Problemas	25 detectados

D

49/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre fapyc.es ha dado como resultado una puntuación de 49/100, lo que equivale a una calificación de grado D. Durante el proceso se ejecutaron 9 comprobaciones pasivas, de las cuales 3 resultaron satisfactorias, 2 generaron advertencias y 4 finalizaron en fallo crítico. La infraestructura presenta debilidades importantes en la configuración del servidor y en la protección de los datos de sesión de los usuarios. Se concluye que el sitio es actualmente vulnerable y requiere medidas correctivas inmediatas para proteger su integridad y la de sus visitantes.

Resumen de Riesgos

1 CRITICO	8 ALTO	15 MEDIO	1 BAJO	28 INFO
--------------	-----------	-------------	-----------	------------

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 30 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	17	FALLO	hooskcsrf_cookie_name: falta HttpOnly; hooskcsrf...
Contenido Mixto	20	FALLO	4 recursos HTTP en pagina HTTPS
Robots.txt y Sitemap	60	AVISO	Falta robots.txt
Puertos Abiertos	20	FALLO	3 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 30 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
30 dias restantes (expira: 2026-10-31T07:29:20.000Z)
- INFO Fecha de emision
Emitido desde: 2026-08-02T07:29:21.000Z
- 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: HTTPd — 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://fapyc.es/
- 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

- 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 /administrator/
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 — 17/100

Estado: FALLO

hooskcsrf_cookie_name: falta HttpOnly; hooskcsrf_cookie_name: falta Secure; hooskcsrf_cookie_name: falta SameSite; hoosk_session: falta Secure; hoosk_session: falta SameSite

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

Contenido Mixto — 20/100

Estado: FALLO

4 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
http://startbootstrap.com/template-overviews/creative/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
http://www.csd.gob.es/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
http://www.cips-fips.com
- MEDIO **href (link/stylesheet)**
...y 1 mas del mismo tipo

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta robots.txt

- INFO **sitemap.xml**
Presente, 222 URLs
- BAJO **security.txt**
No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 20/100

Estado: FALLO

3 puertos riesgosos abiertos

- ALTO **Puerto 21 (FTP)**
ABIERTO — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
ABIERTO — 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

●	CRITICO	Puerto 3306 (MySQL) ABIERTO — 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 autentificacion 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

[CRITICAL] Puerto 3306 (MySQL): Base de datos expuesta directamente a internet, permitiendo intentos de acceso y ataques externos.

[HIGH] Puerto 21 (FTP): Servicio de transferencia de archivos sin cifrar abierto, lo que facilita la interceptación de credenciales.

[HIGH] Content-Security-Policy: La ausencia de esta cabecera permite ataques de inyección de código y XSS.

[HIGH] X-Frame-Options: La falta de esta protección hace que el sitio sea susceptible a ataques de clickjacking.

[HIGH] Strict-Transport-Security: No se fuerza la conexión segura HSTS, permitiendo posibles degradaciones de protocolo.

[HIGH] Cookie hooskcsrf_cookie_name: Carece de los atributos Secure y HttpOnly, permitiendo su robo mediante scripts o redes no cifradas.

[HIGH] Cookie hoosk_session: No tiene el atributo Secure, por lo que la sesión se envía por canales potencialmente inseguros.

[MEDIUM] Puerto 22 (SSH): Acceso remoto administrativo detectado, lo que representa un vector de ataque por fuerza bruta.

[MEDIUM] X-Content-Type-Options: Falta de protección contra el rastreo de tipos MIME (MIME-sniffing).

[MEDIUM] Referrer-Policy: No se controla la información de origen enviada a terceros al hacer clic en enlaces.

[MEDIUM] Permissions-Policy: No se restringe el acceso del navegador a funciones sensibles como cámara o micrófono.

[MEDIUM] Archivos informativos: Los archivos /readme.html y /README.txt son accesibles y pueden revelar detalles técnicos internos.

[MEDIUM] Paneles de login expuestos: Las rutas /wp-login.php, /administrator/ y /user/login son accesibles públicamente.

[MEDIUM] Contenido Mixto: Se detectaron 4 recursos que cargan por HTTP en lugar de HTTPS, comprometiendo la seguridad del candado SSL.

[MEDIUM] Cookies sin SameSite: Las cookies de la plataforma no previenen ataques de falsificación de petición en sitios cruzados (CSRF).

[LOW] Server header expuesto: El servidor revela que utiliza HTTPd, facilitando la búsqueda de vulnerabilidades específicas para esa tecnología.

[LOW] Falta de robots.txt: No existe un archivo de instrucciones para los rastreadores de búsqueda.