

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://fbf.com
Dominio fbf.com
Fecha 7 de mayo de 2026 a las 20:42

Checks 9 pruebas
Hallazgos 45 totales
Problemas 13 detectados

C

65/100

puntos de seguridad



RESUMEN EJECUTIVO

El sitio web fbf.com ha obtenido una puntuación de 65/100, lo que se traduce en una calificación de nota C. Durante la auditoría se realizaron 9 checks pasivos, resultando en 7 verificaciones correctas y 2 fallos críticos relacionados con la configuración del servidor y la seguridad de las cabeceras. La ausencia de mecanismos de protección modernos y la falta de redirección forzada a protocolos seguros indican debilidades estructurales importantes. Por lo tanto, se concluye que el sitio es actualmente vulnerable a diversos vectores de ataque comunes en la web.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 95 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
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	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 95 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
95 dias restantes (expira: 2026-08-10T22:28:14.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-01-24T22:28:14.000Z
- 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

- 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 — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- **ALTO** **HTTP !' HTTPS redireccion**
HTTP 200 — No redirige a HTTPS
- **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 — 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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
Presente (66 bytes)
- INFO **Reglas robots.txt**
0 Disallow, 1 Allow
- INFO **Sitemap en robots.txt**
/sitemap.xml
- 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] Ausencia de Content-Security-Policy: Esta cabecera es inexistente, lo que permite la ejecución de ataques de inyección de código y XSS.

[HIGH] Ausencia de X-Frame-Options: El sitio no previene el clickjacking, permitiendo que atacantes carguen la web en marcos externos para engañar a los usuarios.

[HIGH] Ausencia de Strict-Transport-Security: No se implementa HSTS, lo que impide que el navegador fuerce conexiones seguras y facilita ataques de interceptación.

[HIGH] Error de redirección HTTP a HTTPS: El servidor permite conexiones no cifradas sin redirigirlas automáticamente, exponiendo los datos de tráfico.

[MEDIUM] Ausencia de X-Content-Type-Options: La falta de esta cabecera permite el MIME-type sniffing, lo que puede llevar a la ejecución de archivos maliciosos.

[MEDIUM] Ausencia de Referrer-Policy: No se controla la información de procedencia enviada en las peticiones, lo que compromete la privacidad de la navegación.

[MEDIUM] Ausencia de Permissions-Policy: El sitio no restringe el acceso a APIs sensibles del navegador como la cámara o el micrófono.

[MEDIUM] Archivos informativos expuestos: Se detectó acceso público a /readme.html y /README.txt, los cuales suelen revelar detalles técnicos de la infraestructura.

[MEDIUM] Paneles de gestión accesibles: Rutas críticas como /wp-login.php, /administrator/ y /user/login están abiertas, facilitando intentos de acceso no autorizado.