EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://bffweb.factoringsecurity.cl	Checks	9 pruebas
Dominio	bffweb.factoringsecurity.cl	Hallazgos	45 totales
Fecha	24 de julio de 2026 a las 16:31	Problemas	13 detectados

C

62/100

puntos de seguridad

RESUMEN EJECUTIVO

Tras realizar el análisis de seguridad en la plataforma, se ha obtenido una puntuación de 62/100, lo que corresponde a una calificación de grado C. Durante la evaluación se ejecutaron un total de 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 1 presentó advertencias y 3 fallaron críticamente. La ausencia total de cabeceras de seguridad y la configuración incorrecta de las cookies de sesión representan los mayores riesgos para la infraestructura. En su estado actual, el sitio se considera vulnerable a ataques de suplantación de identidad y robo de sesiones. Es necesaria una intervención técnica inmediata para elevar los estándares de protección del activo digital.

Resumen de Riesgos

0	6	5	2	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 45 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	TS019f3786: falta HttpOnly; TS019f3786: falta Se...
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 45 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  45 dias restantes (expira: 2026-09-07T22:16:01.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-08-06T22:16:02.000Z
- 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 302 redirige a https://bffweb.factoringsecurity.cl/
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 404

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)
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente
- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 0/100

Estado: FALLO

TS019f3786: falta HttpOnly; TS019f3786: falta Secure; TS019f3786: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: TS019f3786 — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: TS019f3786 — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: TS019f3786 — 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] Falta de Content-Security-Policy: Ausencia de una política que prevenga ataques de inyección de código y Cross-Site Scripting (XSS).

[HIGH] Falta de X-Frame-Options: El sitio es vulnerable a ataques de clickjacking al permitir que el contenido sea embebido en marcos externos.
[HIGH] Falta de Strict-Transport-Security: No se obliga al navegador a mantener conexiones seguras, permitiendo posibles ataques de degradación de HTTPS.
[HIGH] Cookies sin flag HttpOnly: La cookie TS019f3786 puede ser leída por scripts maliciosos, facilitando el robo de sesiones de usuario.
[HIGH] Cookies sin flag Secure: La cookie TS019f3786 se transmite a través de canales no cifrados si el usuario accede por HTTP accidentalmente.
[MEDIUM] Cookies sin flag SameSite: No existe protección contra ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] Falta de X-Content-Type-Options: El servidor no previene que el navegador realice sniffing de tipos MIME, lo que puede derivar en ejecución de código.
[MEDIUM] Falta de Referrer-Policy: La plataforma no controla la cantidad de información que se envía a otros sitios al navegar desde sus enlaces.
[MEDIUM] Falta de Permissions-Policy: No se restringe el uso de funcionalidades del navegador como la cámara o el micrófono mediante políticas de seguridad.
[MEDIUM] Exposición de ruta de login: La dirección /wp-login.php es accesible públicamente, lo que facilita intentos de acceso no autorizado.
[LOW] Ausencia de archivos de gestión: No se encontraron los archivos robots.txt ni sitemap.xml, afectando la auditoría de rastreo del sitio.