EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://msaltobind.github.io/CAFSI_SGR_BUSINNES/	Checks	9 pruebas
Dominio	msaltobind.github.io	Hallazgos	42 totales
Fecha	3 de julio de 2026 a las 13:44	Problemas	10 detectados

C

65/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad del sitio web ha arrojado una puntuación de 65/100, lo que equivale a una calificación de nota C. Durante la evaluación se ejecutaron 9 checks pasivos, obteniendo 6 resultados satisfactorios y 3 fallos críticos en la configuración de seguridad. A pesar de contar con un cifrado SSL adecuado, la ausencia casi total de cabeceras de protección y fallos en la redirección HTTPS comprometen la integridad de la plataforma. En su estado actual, el sitio se considera vulnerable ante ataques de inyección y suplantación de identidad. Se requiere una intervención inmediata para elevar los estándares de seguridad web básicos.

Resumen de Riesgos

0	4	3	3	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 61 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 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	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 61 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  61 dias restantes (expira: 2026-09-02T23:26:06.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-04T23:26:07.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 20/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: GitHub.com — 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
- INFO **Strict-Transport-Security**
  Presente: max-age=31556952
- 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 404 — No redirige a HTTPS
- 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)
- 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 — 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

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] Content-Security-Policy ausente: La falta de esta cabecera permite la ejecución de scripts maliciosos y ataques de Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options ausente: El sitio es vulnerable a ataques de clickjacking, permitiendo que atacantes carguen la página en marcos invisibles para engañar al usuario.
[HIGH] Redirección HTTP a HTTPS fallida: El servidor no fuerza el uso de conexiones seguras, exponiendo el tráfico a posibles interceptaciones.
[HIGH] HSTS no configurado: Al no implementar Strict-Transport-Security, los navegadores no obligan de forma permanente el uso de HTTPS en este dominio.
[MEDIUM] X-Content-Type-Options ausente: La falta de esta directiva permite el sniffing de tipos MIME, lo que puede llevar a la ejecución de archivos con contenido inesperado.
[MEDIUM] Referrer-Policy ausente: No se controla la información de referencia enviada a terceros, lo que puede comprometer la privacidad de la navegación.

[MEDIUM] Permissions-Policy ausente: El sitio no restringe el acceso del navegador a funciones sensibles como la cámara, micrófono o geolocalización.
[LOW] Server header expuesto: El encabezado revela que el servidor es GitHub.com, facilitando información técnica a potenciales atacantes sobre la infraestructura.
[LOW] Archivos robots.txt y sitemap.xml no encontrados: La ausencia de estos archivos dificulta el control de la indexación y la gestión del tráfico de rastreadores.