EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://sisuca.github.io/barcelona-viability-insights/	Checks	9 pruebas
Dominio	sisuca.github.io	Hallazgos	42 totales
Fecha	9 de abril de 2026 a las 19:31	Problemas	10 detectados

C

61/100

puntos de seguridad

RESUMEN EJECUTIVO

El sitio web analizado presenta una puntuacion de seguridad de 61/100, lo que equivale a una nota C segu0 â Æ÷2 W7F æF &W2 FR VF—F÷ ia. Durante el analisis se ejecutaron 9 checks pasivos, resultando en 5 comprobaciones satisfactorias, 1 advertencia y 3 fallos en configuraciones criticas. La ausencia de cabeceras de seguridad fundamentales y la falta de una redireccion automatica hacia protocolos seguros impactan negativamente en la proteccion del usuario. Se concluye que el sitio es actualmente vulnerable ante ataques de inyeccion de contenido, suplantacion de identidad y ataques de intermediario.

Resumen de Riesgos

0	4	3	3	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	70	AVISO	Certificado expira en 28 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 — 70/100

Estado: AVISO

Certificado expira en 28 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- MEDIO **Dias hasta expiracion**
  28 dias restantes (expira: 2026-05-07T21:41:52.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-06T21:41:53.000Z
- 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: Falta esta cabecera esencial que previene ataques de Cross-Site Scripting (XSS) y la inyeccion de contenido malicioso.
[HIGH] X-Frame-Options: La ausencia de esta directiva permite que el sitio sea embebido en marcos de otras webs, facilitando ataques de clickjacking.
[HIGH] HTTP a HTTPS redireccion: El servidor no redirige automaticamente el trafico inseguro al canal cifrado, dejando las comunicaciones expuestas.
[HIGH] HSTS (Strict-Transport-Security): No se ha configurado esta politica que obliga al navegador a utilizar siempre conexiones HTTPS, incrementando el riesgo de interceptacion.
[MEDIUM] X-Content-Type-Options: Al no estar presente, el sitio es vulnerable a ataques basados en MIME-type sniffing, donde el navegador ejecuta archivos con formatos incorrectos.

[MEDIUM] Referrer-Policy: No se controla la informacion de procedencia enviada en las peticiones externas, lo que puede comprometer la privacidad del usuario.
[MEDIUM] Permissions-Policy: No se restringe el acceso a APIs sensibles del navegador como la camara o el microfono, permitiendo potenciales abusos de funcionalidad.
[LOW] Server header expuesto: Se detecto la cabecera Server con el valor GitHub.com, lo que revela informacion tecnica innecesaria sobre la infraestructura subyacente.
[LOW] Archivos de indexacion faltantes: No se encontraron los archivos robots.txt ni sitemap.xml, lo que dificulta el control sobre el rastreo de los motores de busqueda.
[WARN] Caducidad de SSL/TLS: El certificado de seguridad actual es valido pero expirara en 28 dias, lo que requiere una renovacion proxima para evitar advertencias de seguridad.