EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://signrequest.carrerasresearch.org/	Checks	9 pruebas
Dominio	signrequest.carrerasresearch.org	Hallazgos	59 totales
Fecha	14 de abril de 2026 a las 13:48	Problemas	5 detectados

B

86/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el dominio evaluado arroja una puntuación de 86/100 con una calificación de grado B. De los 9 checks pasivos ejecutados, 7 finalizaron correctamente y 2 presentaron fallos relacionados con la configuración de cabeceras y archivos de sistema. Se ha verificado una implementación excelente del cifrado SSL y la gestión de cookies, lo que garantiza la privacidad de los datos en tránsito. No obstante, la ausencia de políticas de seguridad de contenido incrementa el riesgo de ataques por inyección. El sitio se considera seguro en su base técnica, pero vulnerable ante vectores de explotación web específicos debido a configuraciones incompletas.

Resumen de Riesgos

0	1	4	0	54
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 319 dias
Cabeceras de Seguridad	50	FALLO	Solo 3/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
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	6 cookies, todas con flags correctos
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 319 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  319 dias restantes (expira: 2027-02-27T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-01-27T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 50/100

Estado: FALLO

Solo 3/6 presentes. Faltan: Content-Security-Policy, Referrer-Policy, Permissions-Policy

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido

- INFO **X-Frame-Options**
  Presente: DENY
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; includeSubDomains
- INFO **X-Content-Type-Options**
  Presente: nosniff
- MEDIO **Referrer-Policy**
  Falta — Controla la informacion de referer enviada
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 307 redirige a https://signrequest.carrerasresearch.org/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000; includeSubDomains
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 dias)
- 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
- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 100/100

Estado: OK

6 cookies, todas con flags correctos

- INFO **Cookies detectadas**
  6 cookie(s) encontrada(s)
- INFO **Cookie: buid — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: buid — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: buid — SameSite**
  SameSite=none
- INFO **Cookie: esctx — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: esctx — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: esctx — SameSite**
  SameSite=none
- INFO **Cookie: esctx-sE86IAQ6hN0 — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: esctx-sE86IAQ6hN0 — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: esctx-sE86IAQ6hN0 — SameSite**
  SameSite=none
- INFO **Cookie: fpc — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: fpc — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: fpc — SameSite**
  SameSite=none
- INFO **Cookie: x-ms-gateway-slice — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: x-ms-gateway-slice — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: x-ms-gateway-slice — SameSite**
  SameSite=none
- INFO **Cookie: stsservicecookie — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: stsservicecookie — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: stsservicecookie — SameSite**
  SameSite=none

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

- 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

[ALTA] Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de scripts no autorizados, facilitando ataques de Cross-Site Scripting (XSS) e inyección de contenido.
[MEDIA] Referrer-Policy: La falta de esta política impide controlar qué información de origen se envía a otros sitios, lo que podría filtrar rutas internas privadas.
[MEDIA] Permissions-Policy: No se restringen las capacidades del navegador, permitiendo potencialmente que scripts maliciosos accedan a funciones como la cámara o el micrófono.
[MEDIA] Exposición de archivos informativos: Los archivos /readme.html y /README.txt son accesibles públicamente, lo que puede revelar información técnica sobre la infraestructura del sitio.
[BAJA] Ausencia de Robots.txt y Sitemap.xml: La falta de estos archivos dificulta el control sobre qué partes del sitio deben ser indexadas por los motores de búsqueda.