EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://crisal.dev	Checks	9 pruebas
Dominio	crisal.dev	Hallazgos	42 totales
Fecha	24 de abril de 2026 a las 07:55	Problemas	10 detectados

C

72/100

puntos de seguridad

RESUMEN EJECUTIVO

El analisis de seguridad realizado en el dominio crisal.dev arrojo una puntuacion exacta de 72/100, lo que otorga al sitio una calificacion de grado C. Durante la evaluacion se ejecutaron 9 checks pasivos, resultando en 6 validaciones correctas, 1 advertencia por configuracion incompleta y 2 fallos criticos en la infraestructura de cabeceras. Aunque el cifrado de datos es robusto, la ausencia total de politicas de seguridad activa en el servidor representa un riesgo significativo. Se concluye que el sitio es vulnerable a ataques de inyeccion de contenido y suplantacion de identidad debido a estas carencias estructurales.

Resumen de Riesgos

0	4	3	3	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 88 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	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 88 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  88 dias restantes (expira: 2026-07-20T22:53:40.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-21T22:53:41.000Z
- 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

- 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
- 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 301 redirige a https://crisal.dev/
- 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

- 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: La ausencia de esta cabecera impide prevenir ataques de Cross-Site Scripting (XSS) e inyeccion de datos maliciosos.
[HIGH] X-Frame-Options: Falta de proteccion que permite que el sitio sea embebido en otros dominios, facilitando ataques de secuestro de clics o clickjacking.
[HIGH] Strict-Transport-Security: No se ha configurado el mecanismo HSTS, lo que permite que la conexion segura pueda ser degradada a HTTP mediante ataques de intermediario.
[MEDIUM] X-Content-Type-Options: Al no estar presente, el navegador podria intentar interpretar el contenido de forma distinta al tipo MIME declarado, abriendo la puerta a ejecucion de scripts no deseados.
[MEDIUM] Referrer-Policy: La falta de control sobre la informacion de procedencia puede filtrar datos sensibles de la URL a sitios de terceros.
[MEDIUM] Permissions-Policy: No se restringen las capacidades del navegador, permitiendo potencialmente el uso no autorizado de APIs como la camara, el microfono o la geolocalizacion.

[LOW] Server header expuesto: El servidor revela el uso de GitHub.com, proporcionando informacion valiosa sobre la infraestructura tecnologica a posibles atacantes.
[LOW] robots.txt: El archivo no fue encontrado, lo que dificulta la gestion del rastreo por parte de motores de busqueda.
[LOW] sitemap.xml: La ausencia de este mapa del sitio afecta la indexacion y la visibilidad estructurada del contenido web.