EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.crehana.com/org/ch360-formacion/	Checks	9 pruebas
Dominio	www.crehana.com	Hallazgos	49 totales
Fecha	11 de mayo de 2026 a las 22:01	Problemas	9 detectados

B

76/100

puntos de seguridad

RESUMEN EJECUTIVO

El analisis de seguridad realizado ha otorgado una puntuacion de 76/100, lo que se traduce en una calificacion de grado B. Durante la auditoria se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 1 genero una advertencia y 2 presentaron fallos criticos de configuracion. Aunque el sitio web demuestra una implementacion robusta en cuanto a cifrado de datos y redireccion segura, se han detectado carencias importantes en la proteccion contra ataques de inyeccion y en la seguridad de las cookies de sesion. En conclusion, el sitio es funcionalmente seguro para la navegacion basica, pero se considera vulnerable ante vectores de ataque especificos como el secuestro de sesiones y ataques de clickjacking.

Resumen de Riesgos

0	4	4	1	40
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 89 dias
Cabeceras de Seguridad	35	FALLO	Solo 2/6 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	33	FALLO	__creh_country_code: falta HttpOnly; __creh_coun...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 89 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  89 dias restantes (expira: 2026-08-09T07:15:27.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-11T06:15:36.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 35/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: cloudflare — 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=0; 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 301 redirige a https://www.crehana.com/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=0; includeSubDomains
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- MEDIO **HSTS max-age**
  max-age=0 (0 dias) — Recomendado minimo 180 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
- INFO **Tecnologias detectadas**
  Next.js

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 — 33/100

Estado: FALLO

__creh_country_code: falta HttpOnly; __creh_country_code: falta Secure

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: __creh_country_code — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: __creh_country_code — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: __creh_country_code — SameSite**
  SameSite=lax

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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (545 bytes)
- INFO **Reglas robots.txt**
  19 Disallow, 3 Allow
- INFO **sitemap.xml**
  Presente, ? URLs
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- 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

- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — 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 de seguridad impide prevenir ataques de Cross-Site Scripting (XSS) e inyecciones de contenido malicioso.
[HIGH] X-Frame-Options: No se detecto esta cabecera, lo que permite que el sitio sea embebido en iframes externos y facilita ataques de clickjacking.
[HIGH] Cookie __creh_country_code (HttpOnly): La falta de este flag permite que la cookie sea accesible mediante scripts del navegador, aumentando el riesgo de robo de identidad.
[HIGH] Cookie __creh_country_code (Secure): Al carecer de este atributo, la cookie podria ser transmitida a traves de conexiones HTTP no cifradas, comprometiendo la sesion del usuario.
[MEDIUM] Puerto 8080 (HTTP-Alt): El puerto se encuentra abierto, lo que representa una superficie de ataque adicional al exponer servicios web alternativos o proxies.
[MEDIUM] HSTS max-age: La politica de seguridad de transporte estricta tiene una duracion de 0 dias, lo que anula la proteccion persistente contra ataques de degradacion de protocolo.
[MEDIUM] Referrer-Policy: La falta de esta configuracion impide controlar la cantidad de informacion de origen que el navegador envia al navegar hacia otros dominios.
[MEDIUM] Permissions-Policy: No existe una restriccion sobre el uso de APIs del navegador, dejando expuestas funciones como la camara, el microfono o la geolocalizacion.
[LOW] Server header expuesto: El servidor devuelve informacion sobre la tecnologia utilizada (cloudflare), lo cual facilita a potenciales atacantes el reconocimiento del entorno tecnico.