EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://EMILIMA.COM.PE	Checks	9 pruebas
Dominio	emilima.com.pe	Hallazgos	44 totales
Fecha	28 de mayo de 2026 a las 16:31	Problemas	15 detectados

C

64/100

puntos de seguridad

RESUMEN EJECUTIVO

Tras realizar el análisis de seguridad en la plataforma, se ha obtenido una puntuación de 64/100 con una calificación de C. Los resultados de los 9 checks pasivos ejecutados muestran un balance de 4 éxitos, 3 advertencias y 2 fallos críticos de configuración. Aunque el cifrado SSL es correcto, se detectó una ausencia total de cabeceras de seguridad y problemas de contenido mixto en recursos internos. Debido a las múltiples vulnerabilidades de configuración y la exposición de archivos sensibles, se concluye que el sitio es actualmente vulnerable. Es imperativo aplicar medidas correctivas para mitigar riesgos de ataques externos y mejorar la postura defensiva.

Resumen de Riesgos

0	4	10	1	29
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 66 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	60	AVISO	3 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 66 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  66 dias restantes (expira: 2026-08-03T01:18:15.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-05T00:19:46.000Z
- 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: 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
- 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://emilima.com.pe/
- 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
- INFO **Tecnologias detectadas**
  Next.js

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
- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente
- 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 — 60/100

Estado: AVISO

3 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://sgd.emilima.com.pe/mesapartesvirtual.html
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://sgd.emilima.com.pe/denuncias.html
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://sgd.emilima.com.pe/mesapartesvirtual.html

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 — 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: Falta esta cabecera esencial para prevenir ataques de inyección de código como XSS.
[HIGH] X-Frame-Options: No configurado, permitiendo que el sitio sea vulnerable a ataques de clickjacking.
[HIGH] Strict-Transport-Security: HSTS no configurado, lo que impide que el navegador obligue siempre el uso de conexiones HTTPS.
[MEDIUM] Contenido Mixto: Presencia de 3 recursos HTTP vinculados a mesapartesvirtual.html y denuncias.html dentro de la página HTTPS.

[MEDIUM] Archivos Sensibles Expuestos: Acceso público a /readme.html y /README.txt que pueden revelar información técnica.
[MEDIUM] Directorio Administrativo Expuesto: La ruta /administrator/ es accesible públicamente, facilitando ataques de fuerza bruta.
[MEDIUM] X-Content-Type-Options: Falta de cabecera para evitar que el navegador interprete archivos con tipos MIME incorrectos.
[MEDIUM] Puerto 8080 Abierto: El puerto HTTP-Alt se encuentra activo, aumentando la superficie de ataque del servidor.
[MEDIUM] Referrer-Policy y Permissions-Policy: Ausencia de controles sobre la información de referencia y restricciones de APIs del navegador.
[LOW] Server Header Expuesto: Se revela el uso de tecnología Cloudflare, proporcionando información técnica útil para un atacante.