EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.inocar.mil.ec	Checks	9 pruebas
Dominio	www.inocar.mil.ec	Hallazgos	48 totales
Fecha	10 de septiembre de 2026 a las 02:45	Problemas	14 detectados

C

63/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web arrojó una puntuación de 63/100, lo que corresponde a una calificación de grado C. El análisis se basó en 9 checks pasivos, de los cuales 3 resultaron satisfactorios, 1 generó una advertencia y 4 finalizaron en fallo. Se han identificado debilidades críticas relacionadas con software obsoleto, falta de cabeceras de seguridad y presencia de contenido mixto. Debido a la exposición de versiones antiguas y configuraciones de red incompletas, el sitio se considera vulnerable y requiere intervención técnica inmediata.

Resumen de Riesgos

0	2	7	5	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 162 dias
Cabeceras de Seguridad	60	FALLO	Solo 3/6 presentes. Faltan: X-Frame-Options, Ref...
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion HTTPS
Deteccion CMS	100	OK	CMS detectado: Joomla, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 2.9.5 expuesta
Seguridad de Cookies	67	AVISO	2f1f256af82af3aec7589981e962f9af: falta SameSite
Contenido Mixto	20	FALLO	6 recursos HTTP en pagina HTTPS
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	1 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 162 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  162 dias restantes (expira: 2027-02-18T20:37:52.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-08-04T20:37:52.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 60/100

Estado: FALLO

Solo 3/6 presentes. Faltan: X-Frame-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: Apache/2.4.63 (Rocky Linux) OpenSSL/3.5.5 — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.3.33 — Revela framework/lenguaje
- INFO **Content-Security-Policy**
  Presente: default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://cdn....
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; includeSubDomains; preload
- 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.)

Deteccion CMS — 100/100

Estado: OK

CMS detectado: Joomla, PrestaShop

- INFO **WordPress**
  No detectado
- INFO **Joomla**
  Detectado via HTML body
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  Detectado via HTML body
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: Joomla! - Open Source Content Management
- INFO **Tecnologias detectadas**
  Next.js, PHP/8.3.33

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 2.9.5 expuesta

- ALTO **WordPress version**
  Version 2.9.5 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- INFO **Archivo /readme.html**
  No accesible (correcto)
- INFO **Archivo /README.txt**
  No accesible (correcto)

Seguridad de Cookies — 67/100

Estado: AVISO

2f1f256af82af3aec7589981e962f9af: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: 2f1f256af82af3aec7589981e962f9af — HttpOnly**
  HttpOnly activo — No accesible via JavaScript

- INFO **Cookie: 2f1f256af82af3aec7589981e962f9af — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: 2f1f256af82af3aec7589981e962f9af — SameSite**
  Falta SameSite — Vulnerable a CSRF

Contenido Mixto — 20/100

Estado: FALLO

6 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.youtube.com/user/inocarec
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.inocar.mil.ec/tsunamis/eventos.php
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://ecuadorenlaantartida.inocar.mil.ec/
- MEDIO **href (link/stylesheet)**
  ...y 3 mas del mismo tipo

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

1 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)**
  Cerrado — 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] Versión de WordPress expuesta: Se detectó la versión 2.9.5 expuesta públicamente, la cual es extremadamente antigua y permite a atacantes explotar múltiples vulnerabilidades críticas y CVEs conocidos.
[HIGH] X-Frame-Options faltante: La ausencia de esta cabecera permite que el sitio sea cargado en iframes, facilitando ataques de clickjacking para engañar a los usuarios.
[MEDIUM] Contenido mixto detectado: Existen 6 recursos cargados a través de HTTP en una página HTTPS, lo que degrada la seguridad de la conexión y permite ataques de interceptación.
[MEDIUM] Cookie sin atributo SameSite: La cookie de sesión no implementa el atributo SameSite, lo que deja a los usuarios expuestos a ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] Referrer-Policy faltante: El servidor no controla qué información de procedencia se envía a otros sitios, lo que puede derivar en la fuga de datos sensibles en las URLs.
[MEDIUM] Permissions-Policy faltante: No se restringe el acceso del navegador a APIs sensibles como la cámara, el micrófono o la geolocalización, aumentando la superficie de ataque.
[LOW] Cabecera Server expuesta: El servidor revela el uso de Apache/2.4.63 sobre Rocky Linux, proporcionando información valiosa para que un atacante planifique exploits específicos.
[LOW] Cabecera X-Powered-By expuesta: Se muestra el uso de PHP/8.3.33, lo que facilita el reconocimiento de la tecnología del lado del servidor.
[LOW] Meta generator expuesto: La etiqueta meta revela que el sitio utiliza el CMS Joomla, simplificando la fase de reconocimiento en un ataque dirigido.
[LOW] Archivos robots.txt y sitemap.xml no encontrados: La ausencia de estos archivos dificulta la indexación correcta y el control de rastreo por parte de motores de búsqueda.