EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://mail.inocar.mil.ec	Checks	9 pruebas
Dominio	mail.inocar.mil.ec	Hallazgos	45 totales
Fecha	10 de septiembre de 2026 a las 02:49	Problemas	9 detectados

C

72/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el dominio arroja una puntuación de 72/100, lo que corresponde a una calificación de grado C. Durante la evaluación, se ejecutaron 9 checks pasivos que revelaron deficiencias críticas en las políticas de seguridad de red y la gestión de sesiones, obteniendo solo un check fallido pero con múltiples advertencias importantes. Aunque el cifrado de transporte es correcto, la ausencia de cabeceras de protección moderna y la configuración incompleta de cookies comprometen la integridad del sitio. En conclusión, el portal se considera vulnerable ante ataques de inyección de contenido y secuestro de credenciales.

Resumen de Riesgos

0	3	5	1	36
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 103 dias
Cabeceras de Seguridad	15	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion HTTPS
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	50	AVISO	ZM_TEST: falta HttpOnly; ZM_TEST: falta SameSite...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	1 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 103 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  103 dias restantes (expira: 2026-12-21T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-11-21T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 15/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

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

- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- 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.)

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 — 50/100

Estado: AVISO

ZM_TEST: falta HttpOnly; ZM_TEST: falta SameSite; ZM_LOGIN_CSRF: falta SameSite

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- ALTO **Cookie: ZM_TEST — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: ZM_TEST — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: ZM_TEST — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: ZM_LOGIN_CSRF — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: ZM_LOGIN_CSRF — Secure**
  Flag Secure activo — Solo se envia por HTTPS

- MEDIO **Cookie: ZM_LOGIN_CSRF — SameSite**
  Falta SameSite — Vulnerable a CSRF

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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (25 bytes)
- INFO **Reglas robots.txt**
  0 Disallow, 1 Allow
- 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] Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de scripts maliciosos no autorizados y ataques de Cross-Site Scripting (XSS).
[HIGH] Strict-Transport-Security: No se detectó la política HSTS, lo que expone a los usuarios a ataques de degradación de protocolo y robo de datos en tránsito.
[HIGH] Cookie ZM_TEST (HttpOnly): Esta cookie carece del atributo HttpOnly, permitiendo que scripts del lado del cliente accedan a ella y facilitando el robo de sesiones.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite que el navegador intente adivinar el tipo de contenido, aumentando el riesgo de ataques de MIME-sniffing.

[MEDIUM] Referrer-Policy: No se ha definido una política de referer, lo que podría filtrar información sensible de las URLs a dominios externos.
[MEDIUM] Permissions-Policy: El sitio no restringe el acceso a APIs del navegador como la cámara o el micrófono, dejando la puerta abierta a abusos de funcionalidades.
[MEDIUM] Cookies ZM_TEST y ZM_LOGIN_CSRF (SameSite): La falta de este atributo hace que las cookies sean vulnerables a ataques de falsificación de petición en sitios cruzados (CSRF).
[LOW] sitemap.xml: No se encontró el mapa del sitio, lo que dificulta la indexación correcta de la estructura web sin representar un riesgo de seguridad directo.