EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.minal.gob.cu	Checks	9 pruebas
Dominio	www.minal.gob.cu	Hallazgos	44 totales
Fecha	20 de abril de 2026 a las 19:45	Problemas	7 detectados

B

85/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada al portal web ha arrojado una puntuación de 85/100, lo que equivale a una nota B en la escala de cumplimiento. El análisis se basó en 9 checks pasivos, resultando en 7 verificaciones exitosas y 2 fallos críticos en la configuración de seguridad del servidor. Aunque la base de cifrado y la gestión de identidades digitales es robusta, la ausencia de cabeceras de protección expone a los usuarios a riesgos evitables. En su estado actual, el sitio se considera mayoritariamente seguro frente a ataques de red, pero vulnerable a ataques de manipulación de interfaz y navegación. Es fundamental corregir las deficiencias técnicas señaladas para garantizar un entorno de navegación plenamente confiable.

Resumen de Riesgos

0	1	3	3	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 56 dias
Cabeceras de Seguridad	45	FALLO	Solo 2/6 presentes. Faltan: X-Frame-Options, X-C...
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	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	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 56 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  56 dias restantes (expira: 2026-06-15T23:26:19.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-17T23:26:20.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 45/100

Estado: FALLO

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

- BAJO **Server header expuesto**
  Server: openresty — Revela tecnologia del servidor

- INFO **Content-Security-Policy**
  Presente: default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https:; styl...
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- INFO **Strict-Transport-Security**
  Presente: max-age=63072000;includeSubDomains; preload
- 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 — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://www.minal.gob.cu/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=63072000;includeSubDomains; preload
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=63072000 (730 dias)
- INFO **Respuesta HTTPS**
  HTTPS responde con status 403

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 403)
- BAJO **sitemap.xml**
  No encontrado (HTTP 403)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

No se detectaron puertos abiertos

- 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)**
  Cerrado — 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] X-Frame-Options: La falta de esta cabecera permite que el sitio sea embebido en marcos de otras webs, facilitando ataques de clickjacking para engañar a los usuarios.
[MEDIUM] X-Content-Type-Options: Al no estar presente, el navegador puede intentar interpretar archivos con formatos incorrectos, abriendo la puerta a la ejecución de scripts maliciosos.

[MEDIUM] Referrer-Policy: La ausencia de esta directiva implica que no hay control sobre la información de origen que se comparte con terceros al navegar por enlaces externos.
[MEDIUM] Permissions-Policy: El servidor no restringe el acceso del navegador a funciones sensibles como la cámara, el micrófono o la geolocalización mediante políticas de seguridad.
[LOW] Server header expuesto: El servidor revela el uso de la tecnología openresty, proporcionando información valiosa a posibles atacantes para buscar vulnerabilidades específicas.
[LOW] robots.txt: El acceso a este archivo devuelve un error 403, lo que impide una gestión adecuada del rastreo por parte de los motores de búsqueda.
[LOW] sitemap.xml: El archivo de mapa del sitio no es accesible, lo que dificulta la indexación correcta y sugiere una configuración de permisos del servidor demasiado restrictiva o incompleta.