EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://coopriv.com.ar	Checks	9 pruebas
Dominio	coopriv.com.ar	Hallazgos	51 totales
Fecha	7 de agosto de 2026 a las 01:26	Problemas	19 detectados

C

61/100

puntos de seguridad

RESUMEN EJECUTIVO

Tras realizar la auditoría de ciberseguridad al dominio coopriv.com.ar, se ha obtenido una puntuación de 61/100 con una nota final de C. El análisis se basó en 9 checks pasivos, de los cuales 4 resultaron satisfactorios, 2 generaron advertencias y 3 fallaron de forma crítica. Aunque el sitio cuenta con un certificado SSL válido, la exposición de servicios de infraestructura y la falta de cabeceras de seguridad modernas comprometen la integridad del servidor. En su estado actual, el sitio se considera vulnerable debido a configuraciones de red e implementación de software que facilitan vectores de ataque externos.

Resumen de Riesgos

1	5	9	4	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 50 dias
Cabeceras de Seguridad	25	FALLO	Solo 1/6 presentes. Faltan: X-Frame-Options, Str...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	CMS detectado: WordPress
Version CMS Expuesta	20	FALLO	WordPress 6.6.6 expuesta, WordPress 2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	20	FALLO	12 recursos HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	60	AVISO	2 puerto(s) potencialmente riesgoso(s): 21 (FTP)...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 50 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  50 dias restantes (expira: 2026-09-26T10:11:23.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-28T10:11:24.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 25/100

Estado: FALLO

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

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

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.2.30 — Revela framework/lenguaje
- INFO **Content-Security-Policy**
  Presente: upgrade-insecure-requests
- 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://coopriv.com.ar/
- 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

CMS detectado: WordPress

- INFO **WordPress**
  Detectado via HTML body
- 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
- BAJO **Meta generator**
  Expone: WordPress 6.6.6
- INFO **Tecnologias detectadas**
  Next.js, PHP/8.2.30

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.6.6 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 6.6.6 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS

- INFO **Archivo /README.txt**
  No accesible (correcto)
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente

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 — 20/100

Estado: FALLO

12 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://america.micoop.com.ar/login
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://»#»
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://»#»
- MEDIO **href (link/stylesheet)**
  ...y 9 mas del mismo tipo

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (115 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://coopriv.com.ar/wp-sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

2 puerto(s) potencialmente riesgoso(s): 21 (FTP), 3306 (MySQL)

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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
- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — 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

[CRITICAL] Puerto 3306 (MySQL) ABIERTO: La base de datos está expuesta a Internet, lo que permite intentos de conexión remota y ataques de fuerza bruta.
[HIGH] Puerto 21 (FTP) ABIERTO: El protocolo FTP transfiere datos sin cifrar, permitiendo la interceptación de credenciales y archivos en tránsito.
[HIGH] HSTS (Strict-Transport-Security) faltante: El servidor no obliga al uso de conexiones seguras, permitiendo ataques de degradación de HTTPS a HTTP.
[HIGH] WordPress versión 6.6.6 expuesta: La visibilidad pública de la versión exacta del CMS permite a los atacantes buscar exploits específicos y conocidos.
[HIGH] Cabecera X-Frame-Options faltante: La ausencia de esta cabecera hace al sitio vulnerable a ataques de clickjacking mediante el uso de iframes maliciosos.
[MEDIUM] Contenido mixto (12 recursos): Se detectaron múltiples archivos cargándose vía HTTP dentro de la navegación segura, lo que rompe el candado de seguridad del navegador.
[MEDIUM] Cabecera X-Content-Type-Options faltante: La falta de esta protección permite que el navegador intente adivinar el tipo de contenido, facilitando ataques de sniffing.
[MEDIUM] Archivos y rutas administrativas expuestas: El archivo readme.html y el panel wp-login.php son accesibles públicamente, facilitando el reconocimiento del sistema.
[MEDIUM] Cabeceras de seguridad ausentes: Faltan Referrer-Policy y Permissions-Policy para controlar la privacidad y el acceso a funciones del navegador del usuario.
[LOW] Divulgación de tecnología: Las cabeceras exponen el uso de LiteSpeed y la versión PHP/8.2.30, información valiosa para la fase de reconocimiento de un atacante.