EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://agentes.chubut.edu.ar	Checks	9 pruebas
Dominio	agentes.chubut.edu.ar	Hallazgos	45 totales
Fecha	17 de abril de 2026 a las 13:52	Problemas	10 detectados

C

72/100

puntos de seguridad

RESUMEN EJECUTIVO

El analisis de ciberseguridad realizado ha arrojado una puntuacion exacta de 72/100, lo que otorga al sitio una nota de C. Se completaron 9 checks pasivos, obteniendo 6 resultados satisfactorios, 1 advertencia y 2 fallos en categorias criticas de configuracion. Aunque la implementacion del cifrado de datos es correcta, la ausencia total de cabeceras de seguridad representa un riesgo significativo. Por tanto, se concluye que el sitio es vulnerable a ataques de intermediarios y de inyeccion debido a configuraciones de servidor incompletas.

Resumen de Riesgos

0	4	3	3	35
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 71 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	1 cookies, todas con flags correctos
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 71 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  71 dias restantes (expira: 2026-06-27T19:06:25.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-29T19:06:26.000Z
- 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: Apache/2.4.66 (Ubuntu) — 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://agentes.chubut.edu.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

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

1 cookies, todas con flags correctos

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: PHPSESSID — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: PHPSESSID — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: PHPSESSID — SameSite**
  SameSite=strict

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 404)
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- 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] Content-Security-Policy: La ausencia de esta cabecera permite la ejecucion de scripts no autorizados, facilitando ataques de Cross-Site Scripting (XSS).

[HIGH] X-Frame-Options: Al no estar configurada, el sitio puede ser embebido en marcos externos, permitiendo ataques de secuestro de clics o clickjacking.
[HIGH] Strict-Transport-Security: La falta de HSTS impide que el navegador fuerce siempre una conexion segura, dejando la puerta abierta a ataques de degradacion de protocolo.
[MEDIUM] X-Content-Type-Options: El servidor no bloquea el rastreo de tipos MIME, lo que podria permitir que archivos de texto sean interpretados como scripts ejecutables.
[MEDIUM] Referrer-Policy: No existe control sobre la informacion de procedencia enviada en las peticiones, lo que puede exponer rutas internas del portal.
[MEDIUM] Permissions-Policy: El sitio no restringe el acceso a funciones sensibles del navegador como camara, microfono o geolocalizacion mediante cabeceras.
[LOW] Server header expuesto: Se revela la version especifica del software de servidor Apache/2.4.66 y el sistema operativo Ubuntu, facilitando la busqueda de exploits conocidos.
[LOW] Archivo robots.txt ausente: La falta de este archivo impide dar instrucciones claras a los rastreadores sobre que directorios no deben ser indexados.
[LOW] Archivo sitemap.xml ausente: No se detecto un mapa del sitio, lo cual dificulta la auditoria de rutas y el correcto indexado por motores de busqueda.