EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://sso.chubut.edu.ar	Checks	9 pruebas
Dominio	sso.chubut.edu.ar	Hallazgos	46 totales
Fecha	18 de abril de 2026 a las 01:42	Problemas	10 detectados

C

70/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web arroja una puntuación de 70/100 con una calificación de nota C. Se ejecutaron un total de 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 3 generaron advertencias y 1 fue identificado como fallo crítico. La evaluación revela una ausencia total de cabeceras de seguridad esenciales y configuraciones de cookies que comprometen la integridad de las sesiones. No se realizó un pentest activo, por lo que el alcance se limita a la configuración superficial y pública del servidor. Se concluye que el sitio es vulnerable a ataques de suplantación de identidad y secuestro de clics debido a estas omisiones técnicas.

Resumen de Riesgos

0	5	3	2	36
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 70 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	67	AVISO	sistema_de_novedades_de_agentes_session: falta S...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 70 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  70 dias restantes (expira: 2026-06-26T15:22:38.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-28T15:22:39.000Z
- 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://sso.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 — 67/100

Estado: AVISO

sistema_de_novedades_de_agentes_session: falta Secure

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: sistema_de_novedades_de_agentes_session — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: sistema_de_novedades_de_agentes_session — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: sistema_de_novedades_de_agentes_session — SameSite**
  SameSite=lax

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 (24 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- 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: Falta esta cabecera, lo que permite la ejecución de scripts maliciosos y ataques de inyección de contenido XSS.
[HIGH] X-Frame-Options: Al no estar presente, el sitio es susceptible a ataques de Clickjacking, permitiendo que atacantes carguen la web en marcos invisibles.
[HIGH] Strict-Transport-Security: La ausencia de HSTS permite que un atacante intente degradar la conexión de HTTPS a HTTP para interceptar datos.
[HIGH] Cookie sistema_de_novedades_de_agentes_session: Falta el flag Secure, permitiendo que la cookie de sesión se envíe a través de conexiones no cifradas.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el MIME-type sniffing, lo que puede llevar a la ejecución de archivos maliciosos disfrazados.
[MEDIUM] Referrer-Policy: No existe control sobre la información de navegación que se envía a otros sitios al hacer clic en enlaces externos.
[MEDIUM] Permissions-Policy: El sitio no restringe el acceso a APIs sensibles del navegador como la cámara o el micrófono a través de políticas de permisos.
[LOW] Server header expuesto: El servidor revela la versión exacta Apache/2.4.66 (Ubuntu), facilitando a posibles atacantes la búsqueda de exploits específicos.
[LOW] sitemap.xml: El archivo no fue encontrado, lo que dificulta la indexación correcta y el análisis de la estructura del sitio.