EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://bech.chubut.gob.ar/	Checks	9 pruebas
Dominio	bech.chubut.gob.ar	Hallazgos	49 totales
Fecha	7 de abril de 2026 a las 17:12	Problemas	12 detectados

C

64/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web arroja una puntuación de 64/100, lo que equivale a una calificación de grado C. Durante la evaluación, se ejecutaron 9 checks pasivos que resultaron en 3 verificaciones exitosas, 5 advertencias y 1 fallo crítico en la configuración global. A pesar de contar con un certificado SSL válido, la ausencia total de cabeceras de seguridad y deficiencias en la gestión de cookies representan riesgos estructurales significativos. No se realizó un pentest activo, pero los hallazgos detectados de forma pasiva indican que la plataforma es actualmente vulnerable ante ataques de inyección, clickjacking y secuestro de sesiones.

Resumen de Riesgos

0	5	5	2	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 67 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	83	AVISO	XSRF-TOKEN: falta HttpOnly
Contenido Mixto	60	AVISO	1 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 67 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  67 dias restantes (expira: 2026-06-13T18:08:17.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-15T18:08:18.000Z
- 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/2.4.41 (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://bech.chubut.gob.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 — 83/100

Estado: AVISO

XSRF-TOKEN: falta HttpOnly

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- ALTO **Cookie: XSRF-TOKEN — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: XSRF-TOKEN — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: XSRF-TOKEN — SameSite**
  SameSite=lax
- INFO **Cookie: bech_session — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: bech_session — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: bech_session — SameSite**
  SameSite=lax

Contenido Mixto — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (src (script/img/iframe))**
  http://teg.chubut.gov.ar/img/general/mantenimiento.png

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 — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

- INFO **Puerto 21 (FTP)**
  Cerrado — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — 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
- 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 — Previene ataques de Cross-Site Scripting (XSS) y la inyección de contenido malicioso.
[HIGH] X-Frame-Options: Falta — Protege a los usuarios contra ataques de clickjacking que intentan engañarlos para realizar acciones no deseadas.
[HIGH] Strict-Transport-Security: Falta — El servidor no fuerza el uso de HTTPS mediante HSTS, permitiendo posibles ataques de degradación de conexión.
[HIGH] Cookie: XSRF-TOKEN: Falta HttpOnly — Esta cookie es accesible vía scripts del navegador, lo que facilita el robo de sesiones mediante ataques XSS.
[MEDIUM] X-Content-Type-Options: Falta — Evita que el navegador intente adivinar el tipo de contenido, previniendo la ejecución de archivos maliciosos camuflados.
[MEDIUM] Referrer-Policy: Falta — No se controla la información de navegación enviada a otros sitios, lo que compromete la privacidad del usuario.
[MEDIUM] Permissions-Policy: Falta — No se restringen las APIs sensibles del navegador como la cámara, micrófono o geolocalización.
[MEDIUM] Contenido Mixto: Existe un recurso de imagen cargado mediante HTTP en una página protegida por HTTPS, rompiendo la cadena de confianza del cifrado.
[MEDIUM] Puerto 22 (SSH): Se detectó un puerto de acceso remoto abierto, lo que aumenta la superficie de ataque para intentos de intrusión al servidor.
[LOW] Server header expuesto: El servidor Apache/2.4.41 (Ubuntu) revela su versión exacta, facilitando a los atacantes la búsqueda de vulnerabilidades específicas.
[LOW] sitemap.xml: El archivo de mapa del sitio no fue encontrado, lo que dificulta la auditoría de rutas y la indexación controlada.