EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://osepmendoza.com.ar/web/	Checks	9 pruebas
Dominio	osepmendoza.com.ar	Hallazgos	51 totales
Fecha	18 de abril de 2026 a las 06:57	Problemas	19 detectados

D

53/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada sobre el dominio evaluado arroja una puntuación de 53/100, lo que corresponde a una calificación de grado D. Los resultados de los checks pasivos indican deficiencias críticas, con solo 2 pruebas superadas de las 9 ejecutadas, registrándose 5 fallos directos y 2 advertencias. Se han detectado puertos sensibles expuestos a internet, versiones de software desactualizadas y una configuración de cabeceras de seguridad deficiente. Debido a la exposición de servicios internos y la presencia de contenido mixto, se concluye que el sitio es actualmente vulnerable a diversos vectores de ataque.

Resumen de Riesgos

1	6	7	5	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 61 dias
Cabeceras de Seguridad	40	FALLO	Solo 2/6 presentes. Faltan: X-Frame-Options, Str...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 2 expuesta
Seguridad de Cookies	33	FALLO	PHPSESSID: falta HttpOnly; PHPSESSID: falta Same...
Contenido Mixto	20	FALLO	11 recursos HTTP en pagina HTTPS
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	60	AVISO	2 puerto(s) potencialmente riesgoso(s): 21 (FTP)...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 61 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  61 dias restantes (expira: 2026-06-17T23:30:58.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-19T23:30:59.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 40/100

Estado: FALLO

Solo 2/6 presentes. Faltan: X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-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
- INFO **Permissions-Policy**
  Presente: private-state-token-redemption=(self "https://www.google.com" "https://www.gstat...

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://osepmendoza.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, PrestaShop

- INFO **WordPress**
  Detectado via HTML body
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  Detectado via HTML body
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: Site Kit by Google 1.171.0
- INFO **Tecnologias detectadas**
  Next.js, PHP/8.2.30

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 2 expuesta

- ALTO **WordPress version**
  Version 2 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- INFO **Archivo /readme.html**
  No accesible (correcto)

- INFO **Archivo /README.txt**
  No accesible (correcto)

Seguridad de Cookies — 33/100

Estado: FALLO

PHPSESSID: falta HttpOnly; PHPSESSID: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: PHPSESSID — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: PHPSESSID — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: PHPSESSID — SameSite**
  Falta SameSite — Vulnerable a CSRF

Contenido Mixto — 20/100

Estado: FALLO

11 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (src (script/img/iframe))**
  http://osepmendoza.com.ar/web/wp-content/uploads/2020/05/car...
- MEDIO **Recurso HTTP (src (script/img/iframe))**
  http://osepmendoza.com.ar/web/wp-content/uploads/2020/05/tur...
- MEDIO **Recurso HTTP (src (script/img/iframe))**
  http://osepmendoza.com.ar/web/wp-content/uploads/2020/05/ate...
- MEDIO **src (script/img/iframe)**
  ...y 8 mas del mismo tipo

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 — 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): El puerto de la base de datos se encuentra abierto públicamente, permitiendo intentos de acceso externo y ataques de fuerza bruta.
[HIGH] Puerto 21 (FTP): Servicio de transferencia de archivos abierto sin cifrado, lo que facilita la interceptación de credenciales en tránsito.
[HIGH] WordPress versión: Se expone públicamente el uso de WordPress versión 2, lo que permite a atacantes identificar y explotar vulnerabilidades conocidas (CVE) para comprometer el sitio.
[HIGH] HSTS (Strict-Transport-Security): La ausencia de esta cabecera impide que el navegador fuerce conexiones seguras HTTPS, dejando a los usuarios vulnerables a ataques de degradación de protocolo.
[HIGH] X-Frame-Options: Falta esta cabecera de seguridad, lo que permite que el sitio sea embebido en marcos externos y facilita ataques de clickjacking.
[HIGH] Cookie PHPSESSID (HttpOnly): La cookie de sesión carece del atributo HttpOnly, lo que la hace accesible mediante scripts del lado del cliente y eleva el riesgo de robo de sesión por XSS.
[MEDIUM] Contenido Mixto: Se detectaron 11 recursos cargados mediante protocolo HTTP inseguro dentro de una página HTTPS, comprometiendo la integridad de la navegación.
[MEDIUM] Cookie PHPSESSID (SameSite): La falta de este atributo en la configuración de cookies de sesión incrementa la superficie de ataque para vulnerabilidades de tipo CSRF.
[MEDIUM] X-Content-Type-Options: Cabecera ausente, lo que permite que el navegador realice "MIME-type sniffing" y pueda ejecutar archivos maliciosos disfrazados de otros tipos.
[MEDIUM] Referrer-Policy: No se encuentra configurada, lo que impide controlar la cantidad de información que el navegador envía a otros sitios al seguir enlaces.
[LOW] Server header expuesto: El servidor revela el uso de LiteSpeed, proporcionando información valiosa a posibles atacantes para realizar ataques dirigidos.
[LOW] X-Powered-By expuesto: La cabecera revela el uso de PHP/8.2.30, exponiendo la tecnología subyacente del sitio.
[LOW] Meta generator: La etiqueta meta expone el uso de la herramienta Site Kit by Google 1.171.0.
[LOW] robots.txt y sitemap.xml: La ausencia de estos archivos dificulta el control de la indexación por parte de motores de búsqueda y la gestión del tráfico legítimo.