EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.oultonweb.com.ar/portalpacientes/	Checks	9 pruebas
Dominio	www.oultonweb.com.ar	Hallazgos	44 totales
Fecha	12 de mayo de 2026 a las 21:34	Problemas	14 detectados

D

50/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el portal ha arrojado una puntuación de 50/100, lo que equivale a una nota D. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 3 resultaron satisfactorios, 2 generaron advertencias y 3 fueron clasificados como fallos. Se han detectado deficiencias críticas en la configuración de cabeceras de seguridad y en el manejo de sesiones de usuario, lo que compromete la integridad de la plataforma. Concluimos que el sitio es actualmente vulnerable y requiere una intervención técnica inmediata para mitigar riesgos de robo de información.

Resumen de Riesgos

0	5	5	4	30
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	70	AVISO	Certificado expira en 21 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion HTTPS
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	0	FALLO	PHPSESSID: falta HttpOnly; PHPSESSID: falta Secu...
Contenido Mixto	60	AVISO	1 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 70/100

Estado: AVISO

Certificado expira en 21 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- MEDIO **Dias hasta expiracion**
  21 dias restantes (expira: 2026-06-03T04:44:10.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-05T04:44:11.000Z
- 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/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/5.4.16 — Revela framework/lenguaje
- 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.)

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
- INFO **Tecnologias detectadas**
  PHP/5.4.16

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 — 0/100

Estado: FALLO

PHPSESSID: falta HttpOnly; PHPSESSID: falta Secure; PHPSESSID: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: PHPSESSID — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: PHPSESSID — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP

- MEDIO **Cookie: PHPSESSID — SameSite**
  Falta SameSite — Vulnerable a CSRF

Contenido Mixto — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.institutoulton.com.ar

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: Falta la cabecera CSP, lo que permite la ejecución de ataques de inyección de contenido y scripts maliciosos (XSS).
[HIGH] X-Frame-Options: La ausencia de esta cabecera hace que el sitio sea vulnerable a ataques de Clickjacking, permitiendo que atacantes carguen el portal en marcos invisibles para engañar al usuario.
[HIGH] Strict-Transport-Security: No se fuerza la conexión segura mediante HSTS, permitiendo posibles degradaciones de protocolo y ataques de intermediario.
[HIGH] Cookie PHPSESSID (HttpOnly): La cookie de sesión carece del flag HttpOnly, permitiendo que scripts de terceros accedan al identificador de sesión a través del navegador.
[HIGH] Cookie PHPSESSID (Secure): El identificador de sesión no tiene el flag Secure, lo que significa que la cookie podría ser enviada a través de conexiones HTTP no cifradas.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el MIME-type sniffing, lo que puede llevar al navegador a interpretar archivos de forma incorrecta y peligrosa.

[MEDIUM] Referrer-Policy: No existe una política definida para el control de la información de procedencia enviada a otros dominios.
[MEDIUM] Permissions-Policy: No se restringe el acceso a funciones sensibles del navegador como la geolocalización o la cámara.
[MEDIUM] Cookie PHPSESSID (SameSite): La falta de este atributo aumenta significativamente el riesgo de ataques de falsificación de solicitudes entre sitios (CSRF).
[MEDIUM] Contenido Mixto: Se detectó un recurso cargado mediante el protocolo inseguro HTTP dentro del entorno seguro HTTPS, debilitando el cifrado general.
[LOW] Exposición de tecnología: Se revela el uso de Apache/2.4.6 y PHP/5.4.16 a través de las cabeceras Server y X-Powered-By, facilitando ataques dirigidos a versiones específicas.
[LOW] SSL/TLS: El certificado de seguridad actual tiene una fecha de vencimiento próxima de 21 días.
[LOW] Archivos de indexación: No se encontraron los archivos robots.txt ni sitemap.xml, lo que impide una correcta auditoría de las rutas accesibles del sitio.