EscanearVulnerabilidades

Informe de Seguridad Web

URL	http://biblio.unvm.edu.ar/opac_css/	Checks	9 pruebas
Dominio	biblio.unvm.edu.ar	Hallazgos	60 totales
Fecha	19 de abril de 2026 a las 19:32	Problemas	32 detectados

D

47/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis técnico de seguridad realizado al sitio web arroja una puntuación de 47/100, lo que otorga una calificación final de nota D. Se han ejecutado un total de nueve checks pasivos, de los cuales tres resultaron satisfactorios, dos presentaron advertencias y dos fallaron de forma crítica debido a la ausencia de protocolos básicos de cifrado. Los resultados indican que el servidor no implementa medidas de seguridad esenciales para proteger la integridad y privacidad de los datos transmitidos. No se ha realizado un pentest activo en esta evaluación para profundizar en las defensas internas. En conclusión, el sitio web se clasifica como vulnerable y requiere atención inmediata para mitigar riesgos de interceptación de datos.

Resumen de Riesgos

1	17	10	4	28
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	0	ERROR	No se pudo verificar SSL/TLS
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	CMS detectado: WordPress
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	0	FALLO	PhpMyBibli-OPACDB: falta HttpOnly; PhpMyBibli-OP...
Contenido Mixto	50	AVISO	El sitio no usa HTTPS, no aplica chequeo de cont...
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 0/100

Estado: ERROR

No se pudo verificar SSL/TLS

- CRITICO **Conexion SSL**
  No se pudo establecer conexion SSL/TLS

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 — 0/100

Estado: ERROR

No se pudo verificar la redireccion HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS

Deteccion CMS — 100/100

Estado: OK

CMS detectado: WordPress

- INFO **WordPress**
  Detectado via HTML body
- 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**
  Next.js

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

PhpMyBibli-OPACDB: falta HttpOnly; PhpMyBibli-OPACDB: falta Secure; PhpMyBibli-OPACDB: falta SameSite; PHPSESSID: falta HttpOnly; PHPSESSID: falta Secure; PHPSESSID: falta SameSite; PmbOpac-LOGIN: falta HttpOnly; PmbOpac-LOGIN: falta Secure; PmbOpac-LOGIN: falta SameSite; PmbOpac-SESSNAME: falta HttpOnly; PmbOpac-SESSNAME: falta Secure; PmbOpac-SESSNAME: falta SameSite; PmbOpac-SESSID: falta HttpOnly; PmbOpac-SESSID: falta Secure; PmbOpac-SESSID: falta SameSite; PmbOpac-DATABASE: falta HttpOnly; PmbOpac-DATABASE: falta Secure; PmbOpac-DATABASE: falta SameSite

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

- MEDIO **Cookie: PhpMyBibli-OPACDB — SameSite**
  Falta SameSite — Vulnerable a CSRF
- 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
- ALTO **Cookie: PmbOpac-LOGIN — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: PmbOpac-LOGIN — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: PmbOpac-LOGIN — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: PmbOpac-SESSNAME — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: PmbOpac-SESSNAME — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: PmbOpac-SESSNAME — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: PmbOpac-SESSID — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: PmbOpac-SESSID — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: PmbOpac-SESSID — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: PmbOpac-DATABASE — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: PmbOpac-DATABASE — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: PmbOpac-DATABASE — SameSite**
  Falta SameSite — Vulnerable a CSRF

Contenido Mixto — 50/100

Estado: AVISO

El sitio no usa HTTPS, no aplica chequeo de contenido mixto

- ALTO **Protocolo**
  El sitio no usa HTTPS

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (1304 bytes)
- INFO **Reglas robots.txt**
  15 Disallow, 1 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- BAJO **Ruta sensible en robots.txt**
  Referencia a "config" — Puede revelar rutas sensibles a atacantes
- 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

[CRITICAL] Conexion SSL: No se pudo establecer una conexion cifrada SSL/TLS, lo que permite la interceptacion de trafico.
[HIGH] Redireccion HTTP a HTTPS: El sitio permite el acceso por canales no cifrados sin forzar una conexion segura.
[HIGH] Content-Security-Policy: La ausencia de esta cabecera facilita la ejecucion de ataques de inyeccion de contenido y XSS.
[HIGH] X-Frame-Options: Al faltar esta cabecera, el sitio es susceptible a ataques de secuestro de clic o clickjacking.
[HIGH] Strict-Transport-Security: No se aplica la politica HSTS, permitiendo ataques de degradacion de protocolo.
[HIGH] Cookie PhpMyBibli-OPACDB: Carece de flags HttpOnly y Secure, exponiendola a robos mediante scripts y redes no seguras.
[HIGH] Cookie PHPSESSID: La cookie de sesion principal no esta protegida contra acceso por JavaScript ni requiere HTTPS.
[HIGH] Cookie PmbOpac-LOGIN: Informacion de acceso vulnerable por falta de atributos de seguridad en la configuracion de cookies.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite que el navegador adivine el tipo de contenido, facilitando ataques MIME-sniffing.
[MEDIUM] Referrer-Policy: No existe control sobre la informacion de procedencia enviada a otros dominios.
[MEDIUM] Cookies sin SameSite: Multiples cookies de la plataforma carecen de este flag, lo que aumenta el riesgo de ataques CSRF.
[MEDIUM] Configuracion Robots.txt: El archivo bloquea el rastreo total del sitio y expone nombres de directorios internos.
[LOW] Server header expuesto: El servidor revela el uso de Apache/2.4.41 (Ubuntu), facilitando la busqueda de exploits especificos.
[LOW] Sitemap.xml: No se encontro el archivo de mapa del sitio, afectando la indexacion y auditoria de rutas.