EscanearVulnerabilidades

Informe de Seguridad Web

URL	http://movilapp.avicampo.com.co:7380/formaciones/index.php?r=auth/login	Checks	9 pruebas
Dominio	movilapp.avicampo.com.co	Hallazgos	40 totales
Fecha	22 de mayo de 2026 a las 15:35	Problemas	14 detectados

D

44/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web ha resultado en una puntuación de 44/100, lo que equivale a una calificación de grado D. Durante el análisis se ejecutaron un total de 9 checks pasivos, de los cuales 3 resultaron satisfactorios, se emitió 1 advertencia y se identificaron 3 fallos críticos en la configuración. La ausencia total de cifrado HTTPS y la carencia de cabeceras de seguridad fundamentales exponen la plataforma a diversos vectores de ataque. Por lo tanto, se concluye que el sitio es actualmente vulnerable y representa un riesgo para la confidencialidad de la información gestionada.

Resumen de Riesgos

0	6	4	4	26
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

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	50	AVISO	El sitio no usa HTTPS, no aplica chequeo de cont...
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

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/2.4.62 (Win64) OpenSSL/3.1.7 PHP/8.3.14 mod_fcgid/2.3.10-dev — Revela tecnologia del servidor
- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.3.14 — 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/8.3.14

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 — 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 — 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] Protocolo de comunicación inseguro: El sitio opera sobre HTTP sin cifrado, permitiendo la interceptación de credenciales y datos en tránsito.
[HIGH] Ausencia de Content-Security-Policy: La falta de esta cabecera facilita la ejecución de ataques XSS y la inyección de contenido malicioso.
[HIGH] Falta de X-Frame-Options: El sitio es vulnerable a ataques de clickjacking al permitir ser embebido en marcos de sitios externos.
[HIGH] Ausencia de Strict-Transport-Security: No se implementa HSTS, lo que impide forzar conexiones seguras y protegidas contra degradación de protocolo.
[HIGH] Cookie de sesión PHPSESSID sin HttpOnly: La falta de este flag permite que la cookie sea accesible mediante scripts, facilitando el robo de sesión.
[HIGH] Cookie de sesión PHPSESSID sin flag Secure: Al no estar marcada como segura, la identificación de sesión se transmite por canales no cifrados.
[MEDIUM] Falta de X-Content-Type-Options: El navegador podría interpretar archivos de forma incorrecta, permitiendo ataques de sniffing de tipo MIME.
[MEDIUM] Ausencia de Referrer-Policy: No existe control sobre la información de navegación que se comparte con otros dominios.
[MEDIUM] Falta de Permissions-Policy: El sitio no restringe el acceso a funciones sensibles del navegador como la cámara o el micrófono.
[MEDIUM] Cookie PHPSESSID sin SameSite: La ausencia de este atributo incrementa el riesgo de ataques de falsificación de petición en sitios cruzados (CSRF).
[LOW] Exposición de firma del servidor: El encabezado Server revela el uso de Apache/2.4.62, OpenSSL/3.1.7 y PHP/8.3.14, facilitando la búsqueda de exploits específicos.
[LOW] Cabecera X-Powered-By expuesta: Se confirma el uso de PHP/8.3.14, brindando información técnica innecesaria a posibles atacantes.
[LOW] Ausencia de archivos de rastreo: No se han localizado los archivos robots.txt ni sitemap.xml para la gestión de indexación.