EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.umecit.edu.pa	Checks	9 pruebas
Dominio	www.umecit.edu.pa	Hallazgos	51 totales
Fecha	6 de julio de 2026 a las 23:57	Problemas	14 detectados

C

61/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad del portal institucional arroja una puntuación de 61/100, lo que equivale a una nota de C. Se ejecutaron 9 checks pasivos, de los cuales 5 resultaron correctos, 1 presentó advertencias y 3 fallaron con criticidad alta. Se han detectado riesgos importantes relacionados con la obsolescencia del software y la ausencia de protecciones básicas en la configuración del servidor. Debido a la exposición de una versión de CMS extremadamente antigua y la falta de cabeceras de seguridad, el sitio se considera vulnerable a ataques conocidos.

Resumen de Riesgos

0	8	4	2	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 86 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	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 2.9.0 expuesta
Seguridad de Cookies	33	FALLO	_fbp: falta HttpOnly; PHPSESSID: falta HttpOnly;...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 86 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  86 dias restantes (expira: 2026-09-30T13:11:10.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-07-02T13:11:11.000Z
- 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 — 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 302 redirige a https://www.umecit.edu.pa/
- 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 1.182.0
- INFO **Tecnologias detectadas**
  React, Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 2.9.0 expuesta

- ALTO **WordPress version**
  Version 2.9.0 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

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

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- ALTO **Cookie: _fbp — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: _fbp — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: _fbp — SameSite**
  SameSite=lax
- 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 — 100/100

Estado: OK

No se detecto contenido mixto

- INFO **Contenido mixto**
  Todos los recursos se cargan por HTTPS

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (171 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- INFO **Sitemap en robots.txt**
  https://umecit.edu.pa/sitemap_index.xml
- 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] WordPress version: Se detectó la versión 2.9.0 expuesta públicamente, lo cual es crítico porque permite a atacantes explotar múltiples vulnerabilidades documentadas (CVEs) para tomar el control del sitio.
[HIGH] Content-Security-Policy: Cabecera ausente, lo que facilita ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[HIGH] X-Frame-Options: La falta de esta cabecera hace que el sitio sea vulnerable a ataques de clickjacking, permitiendo que sea embebido en marcos invisibles.
[HIGH] Strict-Transport-Security: HSTS no está configurado, lo que impide que el navegador fuerce conexiones HTTPS de forma estricta y segura.
[HIGH] Cookie Security (HttpOnly): Las cookies _fbp y PHPSESSID no tienen el flag HttpOnly, permitiendo que sean robadas mediante scripts de navegador en ataques XSS.
[HIGH] Cookie Security (Secure): La cookie PHPSESSID se envía sin el flag Secure, lo que significa que la sesión podría ser interceptada en conexiones no cifradas.
[MEDIUM] X-Content-Type-Options: Al no estar presente, el navegador puede intentar interpretar el contenido de forma distinta a la declarada, facilitando el sniffing de tipos MIME.
[MEDIUM] Cookie Security (SameSite): La falta de este atributo en la cookie de sesión PHPSESSID deja a los usuarios vulnerables a ataques de Cross-Site Request Forgery (CSRF).
[MEDIUM] Referrer-Policy: No existe una política definida para el control de la información de referencia enviada a sitios externos.
[MEDIUM] Permissions-Policy: No se restringe el acceso a APIs sensibles del navegador como la cámara o el micrófono.
[LOW] Server header expuesto: El servidor revela el uso de Apache, proporcionando información útil a los atacantes para perfilar el entorno técnico.
[LOW] Meta generator: La etiqueta revela el uso de Site Kit by Google 1.182.0, exponiendo detalles sobre la infraestructura interna de plugins.