EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://americancollege.edu.ec/	Checks	9 pruebas
Dominio	americancollege.edu.ec	Hallazgos	49 totales
Fecha	24 de marzo de 2026 a las 19:04	Problemas	15 detectados

C

62/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web arroja una puntuación de 62/100, lo que equivale a una nota de C. Durante la evaluación se ejecutaron un total de 9 checks pasivos, de los cuales 4 resultaron exitosos, 3 generaron advertencias y 2 terminaron en fallo crítico. A pesar de contar con un cifrado de conexión adecuado, la ausencia total de cabeceras de seguridad y la exposición de versiones de software comprometen la integridad del portal. Se concluye que el sitio es vulnerable y requiere intervenciones técnicas inmediatas para mitigar riesgos de explotación conocidos.

Resumen de Riesgos

0	5	6	4	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 46 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 6.9.4 expuesta, WordPress 2 expuesta
Seguridad de Cookies	67	AVISO	lp_session_guest: falta SameSite
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta robots.txt
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 46 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  46 dias restantes (expira: 2026-05-10T06:28:55.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-09T06:28:56.000Z
- 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

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.1.34 — 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.)

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://americancollege.edu.ec/
- 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: WordPress 6.9.4
- INFO **Tecnologias detectadas**
  Next.js, PHP/8.1.34

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.9.4 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 6.9.4 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS

- INFO **Archivo /README.txt**
  No accesible (correcto)
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente

Seguridad de Cookies — 67/100

Estado: AVISO

lp_session_guest: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: lp_session_guest — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: lp_session_guest — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: lp_session_guest — 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 — 60/100

Estado: AVISO

Falta robots.txt

- BAJO **robots.txt**
  No encontrado (HTTP 404)
- INFO **sitemap.xml**
  Presente, 2 URLs
- 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

[ALTA] Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de scripts maliciosos y ataques de inyección de contenido XSS.
[ALTA] X-Frame-Options: Al no estar configurada, el sitio es susceptible a ataques de clickjacking donde un atacante puede camuflar la interfaz.
[ALTA] Strict-Transport-Security: La falta de HSTS impide que el navegador fuerce conexiones HTTPS, permitiendo posibles ataques de degradación de protocolo.
[ALTA] WordPress version: Se detectó la versión 6.9.4 expuesta públicamente, lo cual facilita a atacantes la búsqueda de vulnerabilidades específicas para este software.
[MEDIA] X-Content-Type-Options: El sitio no previene el sniffing de tipos MIME, lo que podría derivar en la ejecución de archivos con contenido malicioso disfrazado.
[MEDIA] Referrer-Policy: No se controla la información de referencia enviada a otros sitios, lo que puede filtrar URLs privadas o datos de navegación.
[MEDIA] Permissions-Policy: No se restringe el acceso a APIs del navegador como cámara o micrófono, dejando la privacidad del usuario sin una capa de control adicional.
[MEDIA] Ruta /wp-login.php: El panel de administración es accesible de forma global, aumentando el riesgo de ataques de fuerza bruta.
[MEDIA] Archivo /readme.html: Este archivo está disponible públicamente y revela información técnica sensible sobre la instalación del CMS.
[MEDIA] Cookie lp_session_guest: La falta del atributo SameSite en las cookies de sesión hace que el sitio sea vulnerable a ataques de falsificación de petición en sitios cruzados o CSRF.
[BAJA] Server header expuesto: El servidor revela el uso de Apache, entregando información útil para la fase de reconocimiento de un atacante.
[BAJA] X-Powered-By expuesto: Se expone la versión de PHP/8.1.34, lo que permite acotar los vectores de ataque según el lenguaje del backend.
[BAJA] Meta generator: La etiqueta en el código fuente confirma el uso de WordPress 6.9.4.
[BAJA] robots.txt: No se encontró el archivo, lo que dificulta la gestión del rastreo por parte de motores de búsqueda.