EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://campusvirtual.areandina.edu.co/user-login/	Checks	9 pruebas
Dominio	campusvirtual.areandina.edu.co	Hallazgos	52 totales
Fecha	19 de mayo de 2026 a las 04:44	Problemas	17 detectados

C

60/100

puntos de seguridad

RESUMEN EJECUTIVO

El analisis de seguridad realizado sobre el sitio web ha arrojado una puntuacion de 60/100, lo que representa una calificacion de grado C. Los resultados se basan en la ejecucion de 9 checks pasivos, de los cuales 4 resultaron correctos, 3 generaron advertencias y 2 fallaron por deficiencias criticas en la configuracion. Aunque la infraestructura posee un certificado SSL vigente, la ausencia total de cabeceras de seguridad y la exposicion de versiones de software incrementan el riesgo de explotacion. Se concluye que el sitio es vulnerable debido a la falta de protecciones basicas contra ataques de inyeccion y secuestro de sesiones.

Resumen de Riesgos

0	5	9	3	35
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 200 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, Drupal, 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	60	AVISO	3 recurso(s) HTTP en pagina HTTPS
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 200 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  200 dias restantes (expira: 2026-12-04T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-12-24T00:00:00.000Z
- 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/8.0.30 — 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://campusvirtual.areandina.edu.co/
- 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, Drupal, PrestaShop

- INFO **WordPress**
  Detectado via HTML body
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  Detectado via HTML body
- 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: All in One SEO (AIOSEO) 4.6.1.1
- INFO **Tecnologias detectadas**
  Next.js, PHP/8.0.30

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 — 60/100

Estado: AVISO

3 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://gmpg.org/xfn/11
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://campusvirtual.areandina.edu.co/account/
- MEDIO **Recurso HTTP (CSS url())**
  http://eduma.thimpress.com/thim-2/wp-content/themes/eduma/im...

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (110 bytes)
- INFO **Reglas robots.txt**
  0 Disallow, 1 Allow
- INFO **Sitemap en robots.txt**
  https://campusvirtual.areandina.edu.co/aliados-estrategicos-back/sitemap.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: La version 6.9.4 es detectable publicamente, lo que facilita a atacantes potenciales la busqueda de exploits especificos.
[HIGH] Content-Security-Policy: La ausencia de esta cabecera impide prevenir ataques de Cross-Site Scripting (XSS) e inyeccion de contenido malicioso.
[HIGH] X-Frame-Options: Falta la proteccion contra ataques de clickjacking, permitiendo que el sitio sea embebido en marcos externos no autorizados.
[HIGH] Strict-Transport-Security: La falta de HSTS no obliga al navegador a utilizar conexiones HTTPS, permitiendo posibles degradaciones de seguridad.
[MEDIUM] X-Content-Type-Options: El servidor no previene el MIME-type sniffing, lo que podria llevar a la ejecucion de archivos con contenido disfrazado.
[MEDIUM] Referrer-Policy: No existe un control sobre la informacion de procedencia enviada cuando un usuario navega hacia enlaces externos.
[MEDIUM] Permissions-Policy: No se restringen las capacidades del navegador como camara o microfono, aumentando la superficie de ataque.
[MEDIUM] Archivo /readme.html: Este archivo es accesible publicamente y revela informacion tecnica detallada sobre la instalacion del CMS.
[MEDIUM] Ruta /wp-login.php: El panel de acceso administrativo esta expuesto, lo que lo hace susceptible a intentos de intrusion por fuerza bruta.
[MEDIUM] Cookie lp_session_guest: La falta del atributo SameSite en esta cookie de sesion la hace vulnerable a ataques de falsificacion de peticion en sitios cruzados (CSRF).
[MEDIUM] Contenido Mixto: Se detectaron 3 recursos cargandose mediante HTTP dentro de una sesion HTTPS, rompiendo la integridad del cifrado.
[LOW] Server header expuesto: El servidor revela el uso de Apache, proporcionando informacion sobre la tecnologia subyacente a posibles atacantes.
[LOW] X-Powered-By expuesto: La cabecera indica el uso de PHP/8.0.30, lo que ayuda a identificar vulnerabilidades especificas del lenguaje.
[LOW] Meta generator: El codigo fuente expone el uso y version del plugin All in One SEO (AIOSEO) 4.6.1.1.