EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.ucb.edu.bo	Checks	9 pruebas
Dominio	www.ucb.edu.bo	Hallazgos	46 totales
Fecha	2 de abril de 2026 a las 15:53	Problemas	15 detectados

C

62/100

puntos de seguridad

RESUMEN EJECUTIVO

El sitio web ucb.edu.bo presenta una puntuacion de seguridad de 62/100, lo que resulta en una calificacion de grado C. El analisis se baso en la ejecucion de 9 checks pasivos, de los cuales 4 resultaron exitosos, 3 generaron advertencias y 2 fallaron criticamente. Aunque el cifrado basico de la conexion es correcto, la ausencia de capas de seguridad modernas y la exposicion de informacion tecnica del servidor comprometen la integridad del sitio. En su estado actual, la plataforma se considera vulnerable ante ataques de suplantacion de identidad, inyeccion de scripts y ataques de degradacion de protocolo.

Resumen de Riesgos

0	5	8	2	31
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 250 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 6.7.5 expuesta, WordPress 2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	60	AVISO	3 recurso(s) HTTP en pagina HTTPS
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 250 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  250 dias restantes (expira: 2026-12-08T13:42:01.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-11-06T13:42:02.000Z
- 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 301 redirige a https://www.ucb.edu.bo/
- 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 6.7.5
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.7.5 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 6.7.5 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 — 100/100

Estado: OK

No se encontraron cookies

- INFO **Cookies detectadas**
  El sitio no establece cookies en la respuesta inicial

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://lpz.ucb.edu.bo/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.ucb.edu.bo/noticias/

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta robots.txt

- INFO **sitemap.xml**
  Presente, ? 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

[HIGH] Content-Security-Policy: Falta esta cabecera esencial que previene ataques de Cross-Site Scripting (XSS) e inyeccion de contenido malicioso.
[HIGH] X-Frame-Options: No se encuentra configurada, lo que deja el sitio vulnerable a ataques de clickjacking mediante marcos invisibles.
[HIGH] Strict-Transport-Security: La ausencia de HSTS permite que un atacante intente degradar la conexion de los usuarios de HTTPS a HTTP.
[HIGH] WordPress version: La version 6.7.5 del CMS se encuentra expuesta publicamente, facilitando la identificacion de vulnerabilidades conocidas (CVEs).
[MEDIUM] X-Content-Type-Options: Falta esta directiva, permitiendo que el navegador intente adivinar el tipo de contenido, lo que puede derivar en la ejecucion de archivos maliciosos.
[MEDIUM] Referrer-Policy: No existe control sobre la informacion de procedencia enviada a otros sitios web cuando se hace clic en un enlace.
[MEDIUM] Permissions-Policy: La falta de esta cabecera impide restringir el acceso del navegador a funciones sensibles como la camara, el microfono o la geolocalizacion.
[MEDIUM] Contenido Mixto: Se detectaron 3 recursos cargados mediante protocolo inseguro HTTP dentro de la pagina protegida por HTTPS.
[MEDIUM] Archivo /readme.html: Este archivo es accesible de forma publica y revela detalles tecnicos sobre la instalacion y version del CMS.
[MEDIUM] Ruta /wp-login.php: El panel de acceso administrativo es publico, lo que aumenta el riesgo de ataques de fuerza bruta contra las credenciales.
[LOW] Server header expuesto: El encabezado Server revela el uso de tecnologia Apache, entregando informacion valiosa para el reconocimiento inicial de un atacante.
[LOW] Meta generator: La etiqueta meta expone especificamente que el sitio utiliza WordPress 6.7.5, ayudando a la automatizacion de ataques.
[LOW] Falta robots.txt: No se encontro el archivo de reglas para buscadores, lo que dificulta la gestion del rastreo y la exclusion de directorios privados.