EscanearVulnerabilidades

Informe de Seguridad Web

URL	http://alumnos.cobaev.edu.mx/	Checks	9 pruebas
Dominio	alumnos.cobaev.edu.mx	Hallazgos	45 totales
Fecha	16 de agosto de 2026 a las 20:53	Problemas	16 detectados

F

36/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al dominio alumnos.cobaev.edu.mx ha resultado en una puntuación crítica de 36/100, lo que otorga al sitio una calificación de nota F. Durante la auditoría se ejecutaron 9 checks pasivos, identificando 4 fallos graves, 1 advertencia y solo 3 controles superados satisfactoriamente. La ausencia de un certificado SSL válido y la falta total de cabeceras de protección exponen la plataforma a múltiples vectores de ataque. En su estado actual, el sitio se considera vulnerable y no apto para el manejo seguro de información institucional o estudiantil.

Resumen de Riesgos

1	7	4	4	29
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	0	FALLO	Certificado SSL no valido
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

SSL/TLS — 0/100

Estado: FALLO

Certificado SSL no valido

- CRITICO **Certificado valido**
  El certificado SSL NO es valido
- INFO **Dias hasta expiracion**
  50 dias restantes (expira: 2026-10-05T14:08:15.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-07-07T14:08:16.000Z
- 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/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.6.40 — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/5.6.40 — 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 — 0/100

Estado: ERROR

No se pudo verificar la redireccion HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS

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/5.6.40

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 Inteligencia Artificial

---RESUMEN EJECUTIVO---
El análisis de seguridad realizado al dominio alumnos.cobaev.edu.mx ha resultado en una puntuación crítica de 36/100, lo que otorga al sitio una calificación de nota F. Durante la auditoría se ejecutaron 9 checks pasivos, identificando 4 fallos graves, 1 advertencia y solo 3 controles superados satisfactoriamente. La ausencia de un certificado SSL válido y la falta total de cabeceras de protección exponen la plataforma a múltiples vectores de ataque. En su estado actual, el sitio se considera vulnerable y no apto para el manejo seguro de información institucional o estudiantil.

---VULNERABILITIES---
[CRITICAL] Certificado SSL no válido: El sitio no cuenta con un certificado de seguridad funcional, lo que impide el cifrado de las comunicaciones.
[HIGH] Fallo en redirección HTTPS: El servidor responde bajo el protocolo inseguro HTTP 200 y no fuerza la conexión cifrada, facilitando la interceptación de tráfico.
[HIGH] Ausencia de Content-Security-Policy: No existe una política de seguridad de contenido, permitiendo la ejecución de scripts maliciosos y ataques XSS.
[HIGH] Ausencia de cabecera X-Frame-Options: El sitio es susceptible a ataques de clickjacking al permitir ser cargado dentro de marcos externos.
[HIGH] Ausencia de Strict-Transport-Security: No se obliga a los navegadores a interactuar exclusivamente mediante HTTPS, facilitando ataques de degradación.
[HIGH] Cookie PHPSESSID sin flag HttpOnly: El identificador de sesión es accesible mediante JavaScript, lo que permite el robo de sesiones en caso de XSS.
[HIGH] Cookie PHPSESSID sin flag Secure: La información de sesión se envía a través de canales no cifrados, exponiéndola en redes públicas.
[MEDIUM] Cookie PHPSESSID sin flag SameSite: La falta de este atributo incrementa el riesgo de ataques de falsificación de solicitudes en sitios cruzados (CSRF).
[MEDIUM] Ausencia de X-Content-Type-Options: El sitio es vulnerable al sniffing de tipos MIME por parte del navegador.
[MEDIUM] Ausencia de Referrer-Policy y Permissions-Policy: No se restringe la información de procedencia ni el acceso a APIs sensibles del navegador.
[LOW] Exposición de tecnología en cabecera Server: El servidor revela el uso de Apache/2.4.6 (CentOS) y PHP/5.6.40, lo cual ayuda a un atacante a buscar exploits específicos.
[LOW] Cabecera X-Powered-By expuesta: Se confirma el uso de una versión obsoleta de PHP (5.6.40) que ya no recibe parches de seguridad.
[LOW] Ausencia de archivos de control: No se detectaron robots.txt ni sitemap.xml, dificultando la gestión adecuada de la indexación web.