

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://iemontecristo.edusac2.info/webportal.php
Dominio iemontecristo.edusac2.info
Fecha 8 de julio de 2026 a las 03:11

Checks 9 pruebas
Hallazgos 42 totales
Problemas 11 detectados

C

61/100

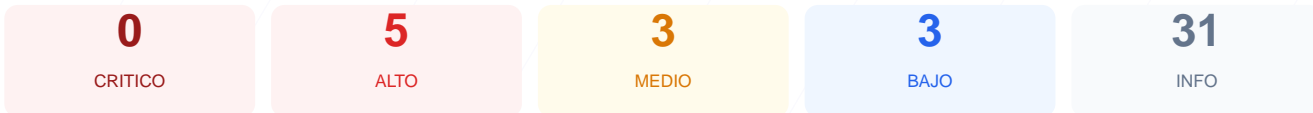
puntos de seguridad



RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada al portal web arroja una puntuación de 61/100, lo que equivale a una nota de grado C. Se ejecutaron un total de 9 checks pasivos, de los cuales 6 resultaron satisfactorios y 3 presentaron fallos críticos de configuración, sin haberse realizado un pentest activo. A pesar de contar con un cifrado SSL vigente, la plataforma carece de las protecciones fundamentales contra ataques de inyección y suplantación. Se concluye que el sitio es vulnerable debido a una configuración de servidor deficiente que expone a los usuarios a riesgos de interceptación de datos y ataques de clickjacking.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 77 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a 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	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 77 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
77 dias restantes (expira: 2026-09-22T21:54:28.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-06-24T21:54:29.000Z
- 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 — 0/100

Estado: **FALLO**

No hay redireccion HTTP a HTTPS

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

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

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 — 100/100

Estado: **OK**

No se encontraron cookies

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

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 — 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 autentificacion 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: La ausencia de esta cabecera permite la ejecución de scripts maliciosos y ataques de inyección de contenido XSS.
- [HIGH] X-Frame-Options: El sitio no está protegido contra clickjacking, permitiendo que atacantes carguen la web en marcos externos para engañar al usuario.
- [HIGH] Strict-Transport-Security: La falta de HSTS impide que el navegador obligue siempre el uso de conexiones cifradas, facilitando ataques de degradación de SSL.
- [HIGH] Redirección HTTP a HTTPS: El servidor responde a través de conexiones no seguras (puerto 80) sin forzar el cifrado, dejando los datos expuestos en tránsito.
- [MEDIUM] X-Content-Type-Options: Al no estar configurada, el navegador podría interpretar archivos de forma incorrecta, facilitando ataques de tipo MIME-sniffing.
- [MEDIUM] Referrer-Policy: No existe control sobre la información de navegación que se comparte con otros dominios al seguir enlaces externos.

[MEDIUM] Permissions-Policy: No se han restringido las APIs del navegador, dejando abierta la posibilidad de acceso no autorizado a componentes como cámara o micrófono.

[LOW] Server header expuesto: La cabecera revela el uso de Apache, proporcionando información técnica valiosa para que un atacante busque vulnerabilidades específicas.

[LOW] Ausencia de robots.txt y sitemap.xml: La falta de estos archivos dificulta la correcta gestión de indexación por parte de motores de búsqueda.