

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://portal.aliadosacr.com/	Checks	9 pruebas
Dominio	portal.aliadosacr.com	Hallazgos	43 totales
Fecha	6 de octubre de 2026 a las 03:21	Problemas	13 detectados

C

72/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre portal.aliadosacr.com arroja una puntuación de 72/100, lo que equivale a una nota de C. Durante la auditoría se ejecutaron 9 checks pasivos, resultando en 6 verificaciones exitosas, 1 advertencia y 2 fallos críticos. Aunque el sitio web cuenta con un cifrado SSL adecuado, presenta una carencia total de cabeceras de seguridad esenciales para la protección del usuario. Debido a estas omisiones de configuración, el sitio se considera vulnerable a ataques de inyección y suplantación. Es imperativo aplicar las correcciones técnicas detalladas para mejorar la postura de seguridad actual.

Resumen de Riesgos

0 CRITICO	4 ALTO	8 MEDIO	1 BAJO	30 INFO
--------------	-----------	------------	-----------	------------

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 31 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
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	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 31 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
31 dias restantes (expira: 2026-11-06T10:29:58.000Z)
- INFO Fecha de emision
Emitido desde: 2026-08-08T10:29:59.000Z
- 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: nginx/1.18.0 (Ubuntu) — 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://portal.aliadosacr.com/
- 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

- INFO

WordPress
Detectado via HTML body
- 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

- MEDIO

Archivo /readme.html
Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO

Archivo /README.txt
Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO

Ruta /wp-login.php
Panel de login accesible publicamente
- MEDIO

Ruta /administrator/
Panel de login accesible publicamente
- MEDIO

Ruta /user/login
Panel de login accesible publicamente

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

INFO

security.txt

Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 100/100

Estado: OK

2 puerto(s) abierto(s), todos esperados

- 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)
- Abierto (esperado) — Servidor web
- INFO

Puerto 443 (HTTPS)
- Abierto (esperado) — 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: La ausencia de esta cabecera permite la ejecución de scripts maliciosos y ataques de inyección de contenido XSS.

[HIGH] X-Frame-Options: No está configurada, lo que deja el sitio desprotegido frente a ataques de clickjacking que pueden engañar a los usuarios.

[HIGH] Strict-Transport-Security: El servidor no fuerza el uso de HTTPS mediante HSTS, permitiendo posibles degradaciones de conexión a HTTP.

[MEDIUM] X-Content-Type-Options: Al faltar esta cabecera, el navegador podría interpretar archivos de forma incorrecta mediante MIME-type sniffing.

[MEDIUM] Referrer-Policy: No se controla la información de procedencia que el navegador envía a terceros, comprometiendo la privacidad de la navegación.

[MEDIUM] Permissions-Policy: No se han definido restricciones sobre el uso de funciones del navegador como la cámara, el micrófono o la geolocalización.

[MEDIUM] Archivos de información expuestos: Los archivos /readme.html y /README.txt son accesibles, pudiendo revelar detalles técnicos internos del CMS.

[MEDIUM] Rutas administrativas expuestas: El acceso público a /wp-login.php y /administrator/ facilita intentos de intrusión por fuerza bruta.

[LOW] Server header expuesto: La cabecera revela el uso de nginx/1.18.0 sobre Ubuntu, lo que ayuda a un atacante a buscar exploits específicos.

[LOW] Ausencia de archivos de indexación: La falta de robots.txt y sitemap.xml dificulta la gestión del rastreo y la visibilidad controlada del sitio.