

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://creditoacr.com	Checks	9 pruebas
Dominio	creditoacr.com	Hallazgos	50 totales
Fecha	6 de octubre de 2026 a las 03:17	Problemas	17 detectados

D

56/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado al dominio creditoacr.com ha resultado en una puntuación de 56/100, lo que corresponde a una calificación de grado D. Durante la auditoría se ejecutaron 9 checks pasivos, identificando 4 resultados satisfactorios, 2 advertencias y 3 fallos críticos en la infraestructura web. Los hallazgos revelan deficiencias significativas en la configuración de cabeceras de seguridad, protección de cookies y gestión de versiones del CMS. Debido a la exposición de componentes desactualizados y la ausencia de políticas de defensa en profundidad, el sitio se considera vulnerable ante ataques dirigidos y automatizados. Es imperativo abordar las vulnerabilidades detectadas para mitigar riesgos de interceptación de datos y compromiso del servidor.

Resumen de Riesgos

0	7	6	4	33
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 185 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 5.2.7 expuesta, WordPress 2.7 expuesta
Seguridad de Cookies	0	FALLO	pw_general_ad_search_favorit_cookie: falta HttpO...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 185 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
185 dias restantes (expira: 2027-04-08T23:59:59.000Z)
- INFO Fecha de emision
Emitido desde: 2026-09-23T00:00:00.000Z
- 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/2.4.18 (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://creditoacr.com:443/
- 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 5.2.7
- INFO

Tecnologias detectadas
Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 5.2.7 expuesta, WordPress 2.7 expuesta

- ALTO

WordPress version
Version 5.2.7 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 — 0/100

Estado: FALLO

pw_general_ad_search_favorit_cookie: falta HttpOnly; pw_general_ad_search_favorit_cookie: falta Secure; pw_general_ad_search_favorit_cookie: falta SameSite

-  **INFO** **Cookies detectadas**
1 cookie(s) encontrada(s)
-  **ALTO** **Cookie: pw_general_ad_search_favorit_cookie — HttpOnly**
Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
-  **ALTO** **Cookie: pw_general_ad_search_favorit_cookie — Secure**
Falta flag Secure — Cookie se envia en conexiones HTTP
-  **MEDIO** **Cookie: pw_general_ad_search_favorit_cookie — SameSite**
Falta SameSite — Vulnerable a CSRF

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 — 60/100

Estado: AVISO

Falta sitemap.xml

-  **INFO** **robots.txt**
Presente (67 bytes)
-  **INFO** **Reglas robots.txt**
1 Disallow, 1 Allow
-  **BAJO** **Ruta sensible en robots.txt**
Referencia a "admin" — Puede revelar rutas sensibles a atacantes
-  **BAJO** **sitemap.xml**
No encontrado (HTTP 404)
-  **BAJO** **security.txt**
No encontrado — Recomendado para politica de divulgacion

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 (CSP): Ausencia de política de seguridad de contenido, permitiendo la ejecución de scripts maliciosos y ataques XSS.
- [HIGH] X-Frame-Options: Falta de cabecera contra Clickjacking, lo que permite que el sitio sea embebido en marcos externos fraudulentos.
- [HIGH] Strict-Transport-Security (HSTS): No se fuerza el uso de HTTPS a nivel de navegador, exponiendo a los usuarios a ataques de degradación de red.
- [HIGH] WordPress version: Exposición pública de las versiones 5.2.7 y 2.7, las cuales poseen múltiples vulnerabilidades conocidas (CVEs).
- [HIGH] Cookie Security (HttpOnly/Secure): Las cookies carecen de flags de seguridad, permitiendo su robo mediante scripts o transmisiones no cifradas.
- [MEDIUM] X-Content-Type-Options: Ausencia de protección contra MIME-type sniffing, lo que podría derivar en la ejecución de archivos maliciosos.
- [MEDIUM] SameSite Cookie: Falta del atributo SameSite, dejando el sitio vulnerable a ataques de falsificación de petición en sitios cruzados (CSRF).
- [MEDIUM] Referrer-Policy y Permissions-Policy: Falta de control sobre la información de navegación compartida y las capacidades de hardware del navegador.
- [MEDIUM] Rutas sensibles expuestas: El panel de administración wp-login.php y el archivo readme.html son accesibles, revelando información técnica a atacantes.
- [LOW] Server header: El servidor revela detalles específicos de la tecnología utilizada (Apache/2.4.18 en Ubuntu).
- [LOW] Robots.txt y Sitemap: El archivo robots.txt menciona rutas administrativas y no se localizó el archivo sitemap.xml.