EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.ibercajagestion.com	Checks	9 pruebas
Dominio	www.ibercajagestion.com	Hallazgos	63 totales
Fecha	13 de mayo de 2026 a las 11:52	Problemas	20 detectados

B

76/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio ibercajagestion.com arroja una puntuación de 76/100 con una calificación de nota B. Durante la auditoría se ejecutaron 9 checks pasivos, resultando en 6 verificaciones satisfactorias y 3 fallos de seguridad críticos. Aunque la plataforma cuenta con un cifrado SSL robusto y una gestión de redirecciones adecuada, se han detectado debilidades severas en la configuración de puertos y el manejo de sesiones. La exposición de servicios internos y la falta de cabeceras de protección incrementan significativamente la superficie de ataque. En su estado actual, el sitio se considera vulnerable debido a fallos estructurales en la infraestructura del servidor.

Resumen de Riesgos

3	10	6	1	43
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 308 dias
Cabeceras de Seguridad	50	FALLO	Solo 3/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
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	39	FALLO	ApplicationGatewayAffinityCORS: falta HttpOnly; ...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	20	FALLO	5 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 308 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  308 dias restantes (expira: 2027-03-16T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-18T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 50/100

Estado: FALLO

Solo 3/6 presentes. Faltan: Content-Security-Policy, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: unknown — Revela tecnologia del servidor

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000
- INFO **X-Content-Type-Options**
  Presente: nosniff
- MEDIO **Referrer-Policy**
  Falta — Controla la informacion de referer enviada
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://www.ibercajagestion.com/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 dias)
- 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 — 39/100

Estado: FALLO

ApplicationGatewayAffinityCORS: falta HttpOnly; ApplicationGatewayAffinity: falta HttpOnly; ApplicationGatewayAffinity: falta Secure; ApplicationGatewayAffinity: falta SameSite; IBSESSID: falta HttpOnly; IBSESSID: falta Secure; IBSESSID: falta SameSite; PHPSESSID: falta HttpOnly; PHPSESSID: falta Secure; PHPSESSID: falta SameSite; incap_ses_690_2949907: falta HttpOnly

- INFO **Cookies detectadas**
  6 cookie(s) encontrada(s)
- ALTO **Cookie: ApplicationGatewayAffinityCORS — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: ApplicationGatewayAffinityCORS — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: ApplicationGatewayAffinityCORS — SameSite**
  SameSite=none
- ALTO **Cookie: ApplicationGatewayAffinity — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: ApplicationGatewayAffinity — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: ApplicationGatewayAffinity — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: IBSESSID — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: IBSESSID — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: IBSESSID — SameSite**
  Falta SameSite — Vulnerable a CSRF
- 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
- INFO **Cookie: visid_incap_2949907 — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: visid_incap_2949907 — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: visid_incap_2949907 — SameSite**
  SameSite=none
- ALTO **Cookie: incap_ses_690_2949907 — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: incap_ses_690_2949907 — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: incap_ses_690_2949907 — SameSite**
  SameSite=none

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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (146 bytes)

- INFO **Reglas robots.txt**
  1 Disallow, 4 Allow
- INFO **Sitemap en robots.txt**
  https://identidadcorporativa.ibercaja.es/sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 20/100

Estado: FALLO

5 puertos riesgosos abiertos

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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
- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — Base de datos MySQL expuesta
- CRITICO **Puerto 3389 (RDP)**
  ABIERTO — Escritorio remoto Windows
- INFO **Puerto 5432 (PostgreSQL)**
  Cerrado — Base de datos PostgreSQL expuesta
- CRITICO **Puerto 6379 (Redis)**
  ABIERTO — Cache Redis sin autenticacion por defecto
- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
  Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[CRITICAL] Puerto 3306 (MySQL) abierto: La base de datos es accesible desde internet, lo que permite ataques de fuerza bruta y riesgo de exfiltración de información sensible.
[CRITICAL] Puerto 3389 (RDP) abierto: El protocolo de escritorio remoto de Windows está expuesto, siendo un vector principal para ataques de secuestro de sistemas (Ransomware).
[CRITICAL] Puerto 6379 (Redis) abierto: El servicio de caché Redis se encuentra expuesto y podría permitir el acceso a datos temporales de la aplicación sin autenticación.
[HIGH] Gestión de Cookies insegura: Las cookies IBSESSID, PHPSESSID y ApplicationGatewayAffinity carecen de los flags HttpOnly y Secure, permitiendo el robo de sesiones mediante scripts maliciosos.
[HIGH] Content-Security-Policy (CSP) faltante: La ausencia de esta política facilita la ejecución de ataques de inyección de contenido y Cross-Site Scripting (XSS).
[HIGH] Puerto 21 (FTP) abierto: El servicio de transferencia de archivos no cifrado está activo, exponiendo credenciales y datos durante su tránsito.
[MEDIUM] Referrer-Policy y Permissions-Policy faltantes: El navegador no recibe instrucciones para limitar la fuga de información técnica o restringir el uso de APIs sensibles como la cámara o el micrófono.
[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La presencia de un servidor web alternativo desprotegido aumenta los puntos de entrada potenciales para un atacante.
[LOW] Cabecera de servidor expuesta: El campo Server revela información sobre la tecnología subyacente, facilitando la búsqueda de exploits específicos.