EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://paneles.gestiondecuenta.com/login	Checks	9 pruebas
Dominio	paneles.gestiondecuenta.com	Hallazgos	47 totales
Fecha	15 de julio de 2026 a las 07:23	Problemas	8 detectados

B

85/100

puntos de seguridad

RESUMEN EJECUTIVO

El analisis de seguridad realizado al sitio web ha arrojado una puntuacion de 85/100, lo que equivale a una nota de B. Durante la evaluacion se ejecutaron un total de 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 2 generaron advertencias y 1 fue clasificado como fallo. El sitio presenta una base solida en cuanto a cifrado y configuracion de red, pero carece de protecciones esenciales contra ataques de inyeccion y gestion de sesiones. En su estado actual, el sitio se considera moderadamente seguro, aunque requiere intervenciones tecnicas inmediatas para mitigar riesgos de seguridad conocidos.

Resumen de Riesgos

0	1	6	1	39
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 137 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	67	AVISO	PHPSESSID: falta SameSite
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 137 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  137 dias restantes (expira: 2026-11-29T11:41:37.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-10-28T11:41:38.000Z
- 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: HTTPd — 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=2629750; includeSubdomains;
- 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://paneles.gestiondecuenta.com/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=2629750; includeSubdomains;
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- MEDIO **HSTS max-age**
  max-age=2629750 (30 dias) — Recomendado minimo 180 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

- 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
- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 67/100

Estado: AVISO

PHPSESSID: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: PHPSESSID — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: PHPSESSID — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: PHPSESSID — 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 (186 bytes)
- INFO **Reglas robots.txt**
  6 Disallow, 0 Allow
- 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: Falta esta cabecera esencial que previene ataques de Cross-Site Scripting (XSS) e inyeccion de contenido malicioso.
[MEDIUM] Cookie PHPSESSID: La ausencia del atributo SameSite hace que la sesion del usuario sea vulnerable a ataques de Cross-Site Request Forgery (CSRF).
[MEDIUM] Archivo /readme.html: Este archivo es accesible publicamente y puede revelar informacion tecnica sobre la infraestructura o el sistema subyacente.
[MEDIUM] Archivo /README.txt: La exposicion de este archivo permite a un atacante obtener detalles sobre la configuracion o versiones del software utilizado.
[MEDIUM] HSTS max-age: El tiempo de persistencia configurado es de solo 30 dias, cuando el estandar de seguridad recomendado es de al menos 180 dias.
[MEDIUM] Referrer-Policy: La falta de esta cabecera impide controlar que informacion de origen se envia a otros sitios web al navegar.
[MEDIUM] Permissions-Policy: No se han restringido las APIs del navegador, permitiendo potencialmente el acceso no autorizado a funciones como la camara o el microfono.
[LOW] Server header expuesto: La cabecera revela el uso de HTTPd, proporcionando informacion util a atacantes para buscar vulnerabilidades especificas.
[LOW] Sitemap: No se detecto el archivo sitemap.xml, lo que dificulta la auditoria de la estructura completa del sitio.