EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://app.gvcgaesco.es/app-web/es/#/login	Checks	9 pruebas
Dominio	app.gvcgaesco.es	Hallazgos	39 totales
Fecha	5 de junio de 2026 a las 12:45	Problemas	9 detectados

C

72/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre la plataforma ha arrojado una puntuación de 72/100, lo que equivale a una calificación de grado C. Se ejecutaron un total de 9 comprobaciones pasivas, de las cuales 6 resultaron satisfactorias y 2 presentaron fallos críticos en la configuración de seguridad. Aunque el cifrado de datos es robusto, la ausencia total de cabeceras de seguridad esenciales compromete la integridad del sitio. En su estado actual, el sitio se considera vulnerable a ataques de intermediarios y de inyección de contenido. Es imperativo corregir las deficiencias técnicas para alcanzar un nivel de protección adecuado para un entorno de autenticación.

Resumen de Riesgos

0	3	3	3	30
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 48 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion 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	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 48 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  48 dias restantes (expira: 2026-07-23T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-06-26T00:00:00.000Z
- 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/2.4.58 (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.)

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

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 no autorizados, facilitando ataques de Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options: Al no estar implementada, el sitio es susceptible a ataques de clickjacking donde un atacante puede camuflar la interfaz.
[HIGH] Strict-Transport-Security: La falta de HSTS no obliga al navegador a usar conexiones seguras, permitiendo posibles degradaciones de protocolo por parte de atacantes.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el MIME-type sniffing, lo que podría llevar al navegador a interpretar archivos de forma maliciosa.
[MEDIUM] Referrer-Policy: No existe control sobre la información de referencia enviada a otros dominios, lo que podría exponer datos sensibles de la URL.
[MEDIUM] Permissions-Policy: El sitio no restringe el acceso a APIs del navegador como la cámara o el micrófono, aumentando la superficie de ataque.
[LOW] Server header expuesto: El servidor revela la versión específica Apache/2.4.58 (Ubuntu), facilitando a los atacantes la búsqueda de exploits conocidos para esa versión.
[LOW] Ausencia de robots.txt y sitemap.xml: El servidor responde con errores 404 para estos archivos, lo que dificulta la gestión del rastreo y la indexación controlada.