

# Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://coffeegreen.com.co  
Dominio coffeegreen.com.co  
Fecha 8 de mayo de 2026 a las 15:44

Checks 9 pruebas  
Hallazgos 49 totales  
Problemas 13 detectados

# D

## 58/100

puntos de seguridad



### RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio coffeegreen.com.co ha resultado en una puntuación de 58/100, lo que equivale a una nota D. Esta evaluación se basa en la ejecución de 9 checks pasivos, de los cuales 5 resultaron exitosos, 2 generaron advertencias y 2 terminaron en fallo crítico. Se han detectado deficiencias graves en la implementación de cabeceras de seguridad y en la gestión de sesiones seguras, a pesar de contar con un certificado SSL válido. Debido a la ausencia de mecanismos de defensa básicos contra ataques web comunes, se concluye que el sitio es actualmente vulnerable.

### Resumen de Riesgos



### Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 89 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a 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	50	AVISO	XSRF-TOKEN: falta HttpOnly; XSRF-TOKEN: falta Se...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

### SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 89 dias

- INFO **Certificado valido**  
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**  
89 dias restantes (expira: 2026-08-05T22:43:43.000Z)
- INFO **Fecha de emision**  
Emitido desde: 2026-05-07T22:43:44.000Z
- 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 — 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 — 0/100

---

Estado: **FALLO**

No hay redireccion HTTP a HTTPS

- **ALTO** **HTTP !' HTTPS redireccion**  
HTTP 302 — No redirige a HTTPS
- **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**

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 — 50/100

---

Estado: **AVISO**

XSRF-TOKEN: falta HttpOnly; XSRF-TOKEN: falta Secure; coffeegreen\_session: falta Secure

- INFO **Cookies detectadas**  
2 cookie(s) encontrada(s)
- ALTO **Cookie: XSRF-TOKEN — HttpOnly**  
Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: XSRF-TOKEN — Secure**  
Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: XSRF-TOKEN — SameSite**  
SameSite=lax
- INFO **Cookie: coffeegreen\_session — HttpOnly**  
HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: coffeegreen\_session — Secure**  
Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: coffeegreen\_session — SameSite**  
SameSite=lax

## 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 (26 bytes)
- INFO **Reglas robots.txt**  
1 Disallow, 0 Allow
- BAJO **sitemap.xml**  
No encontrado (HTTP 404)
- BAJO **security.txt**  
No encontrado — Recomendado para politica de divulgacion

## Puertos Abiertos — 100/100

---

Estado: OK

No se detectaron puertos abiertos

- 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)**  
Cerrado — Servidor web
- INFO **Puerto 443 (HTTPS)**  
Cerrado — 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 ataques de inyección de contenido y Cross-Site Scripting (XSS).

[HIGH] X-Frame-Options: Al no estar configurada, el sitio es susceptible a ataques de clickjacking, donde un atacante puede engañar al usuario para que realice acciones no deseadas.

[HIGH] Strict-Transport-Security: La falta de HSTS impide que el navegador obligue siempre el uso de conexiones seguras HTTPS.

[HIGH] Redirección HTTP a HTTPS: El sitio no redirige automáticamente el tráfico inseguro al protocolo seguro, facilitando la interceptación de datos.

[HIGH] Cookie XSRF-TOKEN: Carece de los atributos HttpOnly y Secure, lo que permite su robo mediante scripts maliciosos o en redes no cifradas.

[HIGH] Cookie coffeegreen\_session: No incluye el flag Secure, permitiendo que la sesión se transmita por canales de texto plano.

[MEDIUM] X-Content-Type-Options: La falta de esta cabecera expone al sitio a ataques de MIME-type sniffing.

[MEDIUM] Referrer-Policy: No existe control sobre la información de origen que se envía a otros dominios al navegar.

[MEDIUM] Permissions-Policy: No se restringen las APIs del navegador, dejando expuestas funciones como cámara o micrófono.

[LOW] Server header expuesto: El servidor revela el uso de tecnología Apache, proporcionando información útil para un atacante en fase de reconocimiento.

[LOW] Sitemap: No se encontró el archivo sitemap.xml, lo que afecta la visibilidad de la estructura del sitio.