

# Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://cookie-gamma.vercel.app/  
Dominio cookie-gamma.vercel.app  
Fecha 11 de mayo de 2026 a las 12:16

Checks 9 pruebas  
Hallazgos 44 totales  
Problemas 8 detectados

# B

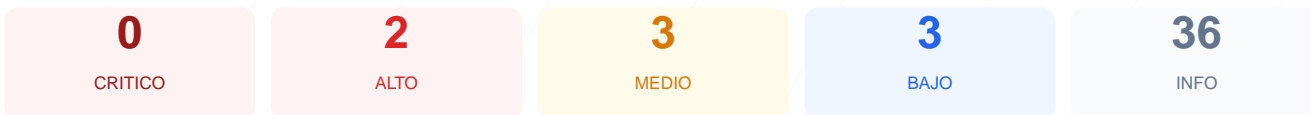
## 80/100

puntos de seguridad

### RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web ha arrojado una puntuación de 80/100 con una nota final de B. El análisis se basó en 9 checks pasivos, de los cuales 7 resultaron exitosos y 2 fallidos, centrados principalmente en la configuración de cabeceras y archivos de metadatos. El portal demuestra una implementación robusta en cuanto a cifrado de datos y transporte seguro, cumpliendo con los estándares actuales de SSL/TLS. No obstante, la ausencia de políticas de seguridad en el servidor lo clasifica como vulnerable ante ataques dirigidos al navegador del usuario final. En su estado actual, el sitio es técnicamente seguro en su comunicación, pero requiere ajustes urgentes para mitigar riesgos de inyección y manipulación.

### Resumen de Riesgos



### Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 77 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 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	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 77 dias

- INFO **Certificado valido**  
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**  
77 dias restantes (expira: 2026-07-27T02:04:42.000Z)
- INFO **Fecha de emision**  
Emitido desde: 2026-04-28T02:04:43.000Z
- INFO **Puerto 443**  
Conexion HTTPS establecida correctamente en puerto 443

### Cabeceras de Seguridad — 20/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**  
Server: Vercel — 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
- **INFO** **Strict-Transport-Security**  
Presente: max-age=63072000; includeSubDomains; preload
- **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 — 100/100

---

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- **INFO** **HTTP !' HTTPS redireccion**  
HTTP 308 redirige a https://cookie-gamma.vercel.app/
- **INFO** **HSTS (Strict-Transport-Security)**  
HSTS activo: max-age=63072000; includeSubDomains; preload
- **BAJO** **HSTS includeSubDomains**  
HSTS cubre subdominios
- **INFO** **HSTS max-age**  
max-age=63072000 (730 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 — 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: Falta esta cabecera crítica, lo que permite la ejecución de ataques XSS y la inyección de contenido malicioso de terceros.

[HIGH] X-Frame-Options: Al no estar presente, el sitio es vulnerable a clickjacking, permitiendo que atacantes carguen la web en marcos invisibles para engañar al usuario.

[MEDIUM] X-Content-Type-Options: La ausencia de esta configuración permite el sniffing de tipos MIME, lo que podría derivar en la ejecución de scripts camuflados como otros archivos.

[MEDIUM] Referrer-Policy: No se controla la información de procedencia enviada en las peticiones, lo que puede exponer rutas internas a sitios externos.

[MEDIUM] Permissions-Policy: No se restringe el acceso a APIs sensibles del navegador como la cámara o el micrófono, aumentando la superficie de ataque.

[LOW] Server header expuesto: Se detectó el encabezado Server: Vercel, lo cual revela la infraestructura subyacente y facilita el reconocimiento a posibles atacantes.

[LOW] robots.txt: Este archivo no fue localizado, lo que impide una gestión adecuada del rastreo y visibilidad de directorios por parte de buscadores.

[LOW] sitemap.xml: La falta de este archivo dificulta la auditoría de la estructura del sitio y la correcta indexación de sus recursos legítimos.