

Escanear Vulnerabilidades

Informe de Seguridad Web

URL: https://elparking.com/
Dominio: elparking.com
Fecha: 13 de mayo de 2026 a las 12:44

Checks: 9 pruebas
Hallazgos: 56 totales
Problemas: 7 detectados

B

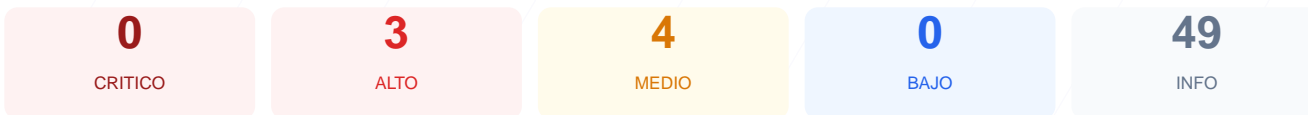
88/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web elparking.com arroja una puntuación de 88/100, lo que equivale a una calificación de grado B. Durante el análisis, se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios y 3 generaron advertencias técnicas que requieren atención inmediata. Los principales hallazgos se concentran en la configuración de cabeceras de seguridad y la gestión de cookies de sesión generadas por balanceadores de carga. Aunque la base de seguridad es sólida y el cifrado es excelente, la presencia de configuraciones incompletas en las cookies indica que el sitio es parcialmente vulnerable a ataques de interceptación y robo de sesiones. En conclusión, el sitio presenta un nivel de seguridad aceptable, pero requiere ajustes técnicos para mitigar riesgos específicos de seguridad web.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 129 dias
Cabeceras de Seguridad	75	AVISO	4/6 presentes. Faltan: Referrer-Policy, Permissi...
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	AWSALBTG: falta HttpOnly; AWSALBTG: falta Secure...
Contenido Mixto	60	AVISO	1 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 129 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
129 dias restantes (expira: 2026-09-19T11:40:26.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-03-05T11:40:26.000Z
- INFO **Puerto 443**
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 75/100

Estado: AVISO

4/6 presentes. Faltan: Referrer-Policy, Permissions-Policy

- INFO **Content-Security-Policy**
Presente: default-src 'self'; child-src https://www.google.com/recaptcha/ https://staticxx...
- INFO **X-Frame-Options**
Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
Presente: max-age=31536000; includeSubDomains
- INFO **X-Content-Type-Options**
Presente: nosniiff
- 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://elparking.com/
- INFO **HSTS (Strict-Transport-Security)**
HSTS activo: max-age=31536000; includeSubDomains
- BAJO **HSTS includeSubDomains**
HSTS 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 — 67/100

Estado: AVISO

AWSALBTG: falta HttpOnly; AWSALBTG: falta Secure; AWSALBTG: falta SameSite; AWSALBTGCORS: falta HttpOnly

- INFO** **Cookies detectadas**
4 cookie(s) encontrada(s)
- ALTO** **Cookie: AWSALBTG — HttpOnly**
Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO** **Cookie: AWSALBTG — Secure**
Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO** **Cookie: AWSALBTG — SameSite**
Falta SameSite — Vulnerable a CSRF
- ALTO** **Cookie: AWSALBTGCORS — HttpOnly**
Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO** **Cookie: AWSALBTGCORS — Secure**
Flag Secure activo — Solo se envia por HTTPS
- INFO** **Cookie: AWSALBTGCORS — SameSite**
SameSite=none
- INFO** **Cookie: PHPSESSID — HttpOnly**
HttpOnly activo — No accesible via JavaScript
- INFO** **Cookie: PHPSESSID — Secure**
Flag Secure activo — Solo se envia por HTTPS
- INFO** **Cookie: PHPSESSID — SameSite**
SameSite=lax
- INFO** **Cookie: _csrf — HttpOnly**
HttpOnly activo — No accesible via JavaScript
- INFO** **Cookie: _csrf — Secure**
Flag Secure activo — Solo se envia por HTTPS
- INFO** **Cookie: _csrf — SameSite**
SameSite=lax

Contenido Mixto — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO** **Recurso HTTP (href (link/stylesheet))**
<http://www.facebook.com/elparkingapp>

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO** **robots.txt**
Presente (82 bytes)
- INFO** **Reglas robots.txt**
1 Disallow, 0 Allow
- INFO** **Sitemap en robots.txt**
<https://elparking.com/sitemap.xml>
- 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 — Envío 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 autenticación 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

[MEDIUM] Referrer-Policy: Falta la cabecera que controla cuánta información de referencia se envía al navegar desde el sitio, lo que puede exponer URLs privadas.

[MEDIUM] Permissions-Policy: Ausencia de cabecera para restringir el acceso del navegador a funciones sensibles como cámara, micrófono o geolocalización.

[HIGH] Cookie AWSALBTG (HttpOnly): Falta el flag HttpOnly, permitiendo que la cookie sea accesible vía scripts (JavaScript), lo que eleva el riesgo de robo de sesión ante un ataque XSS.

[HIGH] Cookie AWSALBTG (Secure): Falta el flag Secure, lo que permite que esta cookie sea enviada a través de conexiones HTTP no cifradas, exponiéndola a interceptaciones.

[MEDIUM] Cookie AWSALBTG (SameSite): La falta de este atributo hace que la cookie sea vulnerable a ataques de falsificación de petición en sitios cruzados (CSRF).

[HIGH] Cookie AWSALBTGCORS (HttpOnly): Al igual que la versión estándar, esta cookie de soporte para recursos compartidos carece de protección contra acceso por script.

[MEDIUM] Contenido Mixto (Recurso HTTP): Se detectó un enlace a Facebook utilizando el protocolo inseguro HTTP en lugar de HTTPS, lo que degrada la integridad de la página segura.