EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://apuestasroyal.com	Checks	9 pruebas
Dominio	apuestasroyal.com	Hallazgos	44 totales
Fecha	15 de julio de 2026 a las 23:07	Problemas	10 detectados

C

64/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio ha arrojado una puntuación exacta de 64/100, lo que corresponde a una nota de C. Durante la evaluación, se ejecutaron 9 checks pasivos, resultando en 5 verificaciones correctas, 2 advertencias y 2 fallos críticos de configuración. La infraestructura presenta debilidades importantes en la implementación de cabeceras de seguridad y en el forzado de conexiones cifradas. En consecuencia, el sitio se considera vulnerable debido a que carece de protecciones fundamentales contra ataques de interceptación y de inyección de contenido.

Resumen de Riesgos

0	4	4	2	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 33 dias
Cabeceras de Seguridad	25	FALLO	Solo 2/6 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	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 33 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  33 dias restantes (expira: 2026-08-17T12:25:34.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-19T11:25:39.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 25/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, Strict-Transport-Security, X-Content-Type-Options, Permissions-Policy

- BAJO **Server header expuesto**
  Server: cloudflare — Revela tecnologia del servidor

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- MEDIO **X-Content-Type-Options**
  Falta — Evita MIME-type sniffing
- INFO **Referrer-Policy**
  Presente: same-origin
- 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 403 — No redirige a HTTPS
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 403

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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (1836 bytes)
- INFO **Reglas robots.txt**
  9 Disallow, 1 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- BAJO **sitemap.xml**
  No encontrado (HTTP 403)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- 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
- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — 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, lo que permite ataques de cross-site scripting (XSS) y la inyección de contenido malicioso.
[HIGH] Strict-Transport-Security: La ausencia de HSTS impide que el navegador obligue el uso de conexiones seguras, facilitando ataques de tipo Man-in-the-Middle.

[HIGH] Redirección HTTPS: El servidor no redirige el tráfico de forma automática de HTTP a HTTPS, devolviendo un error 403 y dejando la conexión inicial desprotegida.
[MEDIUM] X-Content-Type-Options: Al faltar esta configuración, el sitio es susceptible a ataques de sniffing de tipos MIME para ejecutar archivos con formatos falsos.
[MEDIUM] Permissions-Policy: No se definen restricciones para las APIs del navegador, permitiendo potencialmente que scripts accedan a funciones como la cámara o el micrófono.
[MEDIUM] Puerto 8080 (HTTP-Alt): Este puerto se encuentra abierto y expuesto, lo que aumenta la superficie de ataque al ofrecer un servicio web alternativo.
[MEDIUM] Bloqueo en Robots.txt: El archivo bloquea el rastreo de todo el sitio mediante la directiva Disallow: /, lo cual puede ser un error de configuración o una medida de ocultación ineficaz.
[LOW] Server header expuesto: Se detecta la cabecera Server: cloudflare, lo cual revela información sobre la infraestructura tecnológica utilizada.
[LOW] sitemap.xml: El archivo no fue encontrado o devuelve un error 403, dificultando la auditoría de rutas legítimas del sitio.